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. These AD FS Proxy servers, also known as Web Application Proxies (WAP), are replaced through the BIG-IP system's support for the MS-ADFSPIP protocol in version 13.1+. This simplifies the environment by reducing the number of servers necessary.

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, APM, AFM	Microsoft AD FS **2.0**: BIG-IP v11.0 - 13.1 Microsoft AD FS **2012 (3.0)**: BIG-IP v11.4.1 - 13.1 Microsoft AD FS **2016 (4.0)**: BIG-IP v11.4.1 - 13.1
Microsoft Active Directory Federation Services	2.0, 2012 (3.0), 2016 (4.0)
MS-ADFSPIP support for AD FS Proxy (WAP) Replacement	BIG-IP v13.1 and later
iApp Template version	f5.microsoft_adfs.v1.0.0 and f5.microsoft_adfs.v1.2.0rc9
Deployment Guide version	2.7 (see *Document Revision History on page 41*)
Last updated	04-26-2019

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*

If you are looking for older versions of this or other deployment guides, check the Deployment Guide Archive tab at: *https://f5.com/solutions/deployment-guides/archive-608*

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

Contents

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. For AD FS 2012 and 2016 (3.0 and 4.0), you must be on BIG-IP v11.4.1 or later. We recommend version 13.0 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 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.
- *iApp version f5.microsoft_adfs.v1.0.0 only*: If your AD FS clients are using certificate authentication or device registration, there are additional BIG-IP configuration objects you need to create after running the iApp template. See *Configuring the BIG-IP system to support client certificate authentication and device registration (iApp version f5.microsoft_adfs.v1.0.0 or manual configuration only) on page 21.* You do not need to add these objects if you are using f5.microsoft_adfs.v1.1.0rc1 or later.
- If your implementation requires you to support Forms SSO for your application when you are using claims-based auth in AD FS, see *Optional: Supporting Forms SSO for applications the use claims-based auth in AD FS on page 23*.

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.

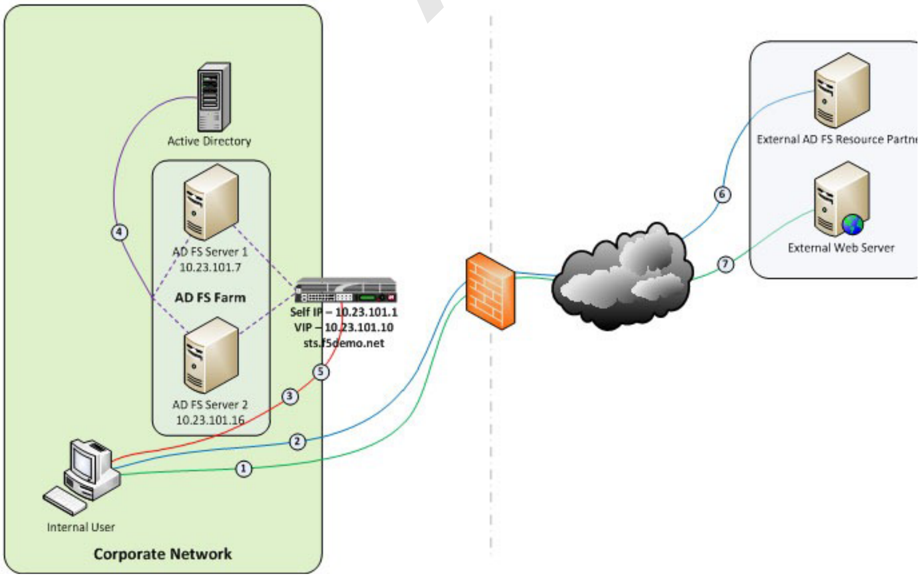

Figure 1: *Logical configuration diagram: Load Balancing AD FS*

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.

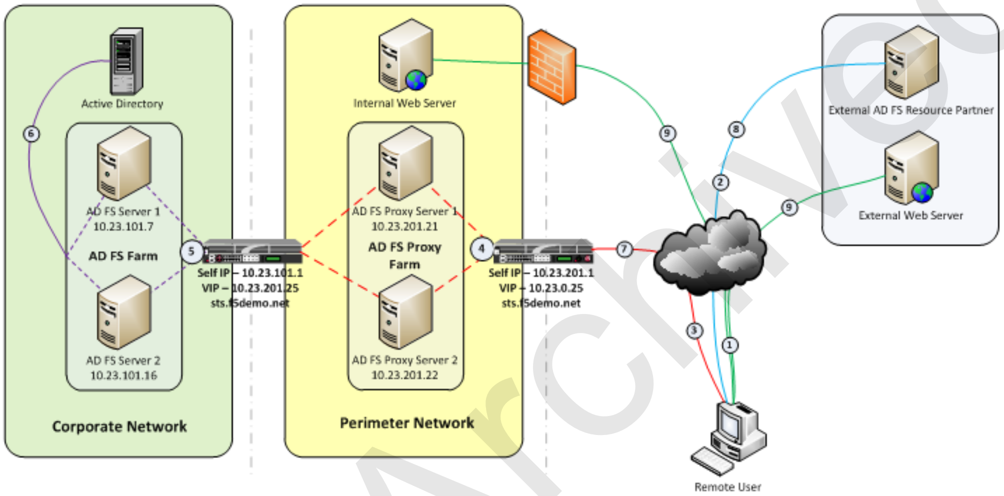

Figure 2: *Logical configuration diagram: Load Balancing AD FS proxy servers*

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. These AD FS Proxy servers, also known as Web Application Proxies (WAP), are replaced through the BIG-IP system's support for the MS-ADFSPIP protocol in version 13.1+. This simplifies the environment by reducing the number of servers necessary."

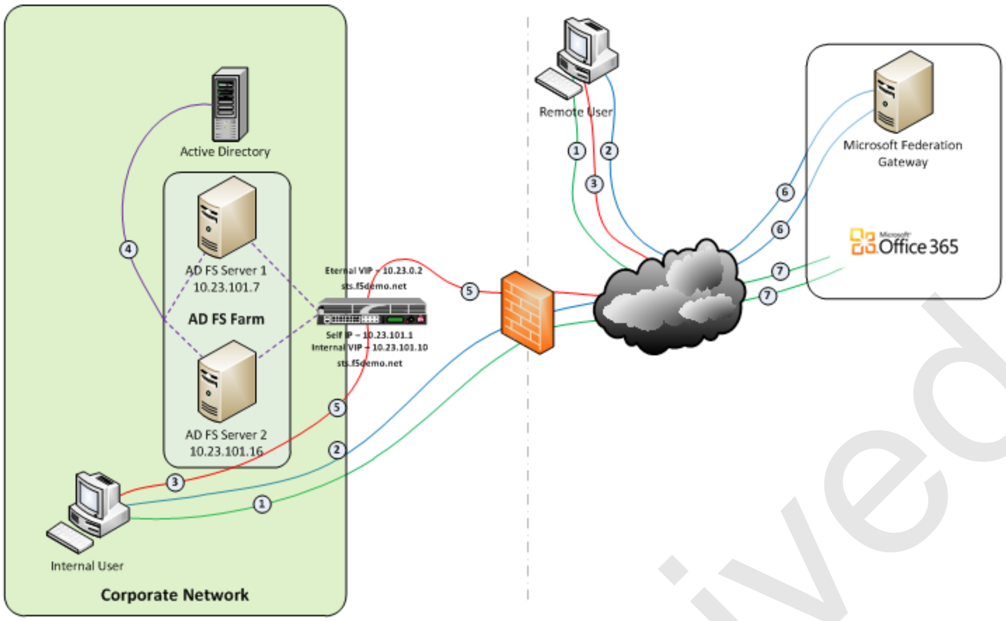

Figure 3: *Logical configuration diagram: Using BIG-IP APM*

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 iApp template for Microsoft AD FS

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

Downloading and importing the new iApp

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

To download and import the iApp

1. Open a web browser and go to *downloads.f5.com*.
2. Click **Find a Download**.
3. In the **BIG-IP** F5 Product Family section, click **iApp Templates**.
4. On the Product Version and Container page, click **iApp-Templates**.
5. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
6. Extract (unzip) the **f5.microsoft_adfs.v<latest version>.tmpl** file. We recommend using the latest template, **f5.microsoft_adfs.v1.2.0rc3**, available in the **RELEASE_CANDIDATES** directory.
   The last non-release candidate version (v1.0.0) is available in the root directory of the iApp package.
7. Log on to the BIG-IP system web-based Configuration utility.
8. On the Main tab, expand **iApp**, and then click **Templates**.
9. Click the **Import** button on the right side of the screen.
10. Click a check in the **Overwrite Existing Templates** box.
11. Click the **Browse** button, and then browse to the location you saved the iApp file.
12. Click the **Upload** button. The iApp is now available for use.

Upgrading an Application Service from previous version of the iApp template

If you configured your BIG-IP system using a previous version of the f5.microsoft_adfs iApp template, we strongly recommend you upgrade the iApp template to the most recent version.

When you upgrade to the current template version, the iApp retains all of your settings for use in the new template. In some new versions, you may notice additional questions, or existing questions asked in different ways, but your initial settings are always saved.

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

1. From the Main tab of the BIG-IP Configuration utility, expand **iApp** and then click **Application Services**.
2. Click the name of your existing f5.microsoft_adfs application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. At the top of the page, in the **Template** row, click the **Change** button to the right of the list.
5. From the **Template** list, select **f5.microsoft_adfs.<latest version>**.
6. Review the questions in the new template, making any necessary modifications. Use the iApp walkthrough section of this guide for information on specific questions.
7. Click **Finished**.

Getting Started with the iApp for Microsoft Active Directory Federation Services

To begin the 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 **AD-FS-iapp_.**
5. From the **Template** list, select **f5.microsoft_adfs.v<latest version>**. The Microsoft AD FS 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 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 AD FS are you deploying?***
   Choose which version of Microsoft Active Directory Federation Services you are using. The selection you make here determines some of the options that appear later in this template.

   - **AD FS 2.0**
     Select this option if you are deploying this iApp template for AD FS 2.0.

- **AD FS 2012 (3.0)**
  Select this option if you are deploying this iApp template for AD FS 2012. Previously this was referred to as AD FS 3.0.
- **AD FS 2016 (4.0)**
  Select this option if you are deploying this iApp template for AD FS 4.0. Previously this was referred to as AD FS 4.0.

4. ***Which AD FS server role is BIG-IP being deployed in front of?***
   Choose the Active Directory Federation Services role in front of which this BIG-IP is being deployed. You can choose AD FS or AD FS Proxy to protect your AD FS servers.
   - **AD FS**
     Select this option deploying AD FS only, and not the AD FS Proxy. In this case, the BIG-IP system can securely pre-authenticate AD FS requests, eliminating the need for AD FS Proxy.
   - **AD FS Proxy**
     Select this option if you are deploying this iApp template for AD FS Proxy. If you choose this option, the BIG-IP APM options do not appear.

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.

2. ***Which VLANs transport client traffic?*** 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. The VLAN objects must already be configured on this BIG-IP system before you can select them.

   If there are VLANs on the BIG-IP system that should not transport client traffic, select the VLAN(s) and use the remove arrows (>>) to move the VLAN(s) to the Options box.

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 AD FS 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.

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

   - **Virtual server IP and AD FS servers are on the same subnet**
     If the BIG-IP virtual servers and AD FS 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 AD FS 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 AD FS 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 next 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 you expect.

          a. *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. *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 server is reached, new requests fail.*

   - **Virtual servers and AD FS 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 AD FS servers?*
        If you chose different subnets, this question appears asking whether the AD FS 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 AD FS 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.

          a. *How many connections to you expect to each AD FS 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 AD FS 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.

  a. *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 server is reached, new requests fail.*

Access Policy Manager (BIG-IP APM)

The section in this scenario asks about 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 B: Configuring DNS and NTP on the BIG-IP system on page 38* for instructions.

➡ ***Note:*** *This entire section does not appear if you selected to deploy the BIG-IP system for the AD FS Proxy server role. Continue with Advanced Firewall Manager (BIG-IP AFM) on page 13.*

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 AD FS.

   - **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. Continue with *Advanced Firewall Manager (BIG-IP AFM) on page 13.*

   - **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 AD FS.

     a. *Which Access Profile do you want to use?*
     Choose whether you want the iApp template to create a new Access Profile for your BIG-IP APM implementation, or if you want to use an existing Access Policy you created outside the template. Unless you have created a custom Access Profile specifically for this implementation, we recommend allowing the iApp to create a new profile.

     - *Select the profile you created*
       If you manually created an Access Profile for this implementation, select it from the list.

     - **Use the iApp to create a new Access Profile**
       Select this option if you want the iApp to create a new Access Profile. You must answer the following questions.

       a. *Do you want the iApp to configure Forms SSO?*
       Choose whether you want the system to configure Forms SSO for this deployment. If you select Yes, the iApp creates a Forms (Client-Initiated) SSO and associated objects for the ADFS endpoint(/adfs/ls) used commonly with SharePoint, CRM and other claims-based authentication configured applications.

       - **No, do not configure Forms SSO for AD FS (/adfs/ls endpoint)**
         Select this option if you do not want to configure Forms SSO. Continue with the next question.

- **Yes, configure Forms SSO for AD FS (/adfs/ls endpoint)**
  Select this option if you want to configure Forms SSO. The system creates an APM Forms (Client-Initiated) SSO object, and the associated configuration objects.

b. *Which AAA Server object do you want to use?*
The APM AAA Server contains information on your Active Directory deployment. The iApp template can create a new AAA Server for AD FS deployments, or you can use a custom AAA Server object you created for this implementation.

- *Select an existing AAA Server object*
  If you created an AAA Server for this implementation, select it from the list.

  ⓘ ***Important*** *The AAA Server object you created must be configured to use a pool of Domain Controllers.*

- **Use the iApp to create a new AAA Server**
  Select this option if you want the iApp template to create a new AAA Server for this implementation.

  a. *Which Active Directory server IP address 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.

  b. *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.

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

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

  c. *Create a new monitor for the Active Directory servers?*
  Choose whether you want the iApp to create a new LDAP or ICMP monitor, or if you want to select an existing monitor you created for the AD servers. For more accurate monitoring, we recommend using an LDAP monitor.

    - *Select an existing monitor for the Active Directory pool*
      If you 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, select it from the list. If you want to create a health monitor manually, 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.

    - **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:

      a. *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.

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

      c. *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.

d. *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.

e. *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.

f. *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.

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

d. *Do you want to configure support for Azure MFA (via Azure MFA Servers)?*
Select whether you want to configure Azure Multi-Factor Authentication (MFA) servers as a part of this deployment. This refers to integration with the on-premise Azure MFA servers as described in:
https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-get-started-server

- **No, do not configure support for Azure MFA**
  Select this option if you do not want to configure support for Azure MFA at this time. Continue with step e.
- **Yes, configure support for Azure MFA**
  Select this option if you want to include support for Azure MFA. The iApp adds the necessary objects to the APM policy. APM will connect via RADIUS to Azure MFA servers. See the Microsoft documentation referenced above for information on how to setup the Azure MFA service/servers. You must answer the following questions.

  a. *Which MFA (RADIUS) AAA Object would you like to use?*
  Choose whether you want the iApp to create new RADIUS AAA object for this implementation, or if you have already created on from the list. Only existing RADIUS AAA objects that are configured to use a pool show up in the list (you can create a pool with only a single server if necessary).

  - *Select an existing RADIUS AAA server object*
    If you created a custom RADIUS AAA server object, select it from the list.
  - **Create a new Azure MFA RADIUS Server**
    Select this option if you want the iApp to create a new AAA server object. You must answer the following questions.

    a. *Which Azure MFA servers would you like to use?*
    Type the IP address of each of your Azure MFA servers. Click **Add** to include more servers.

    b. *What port is the Azure MFA Servers listening on for RADIUS connections?*
    Type the port that your Azure MFA servers are listening on for RADIUS connections. The default is 1812.

    c. *What port are the Azure MFA servers listening on for RADIUS accounting?*
    Type the port that your Azure MFA servers are listening on for RADIUS accounting. The default is 1813.

    d. *What is the RADIUS secret configured on the Azure MFA servers for this connection?*
    Type the RADIUS secret configured on your MFA servers.

e. *Create a new monitor for Azure MFA (RADIUS) servers?*
Choose whether you want the iApp to create a simple ICMP monitor for the MFA servers you entered in step a, or if you do not want the system to monitor the MFA servers.

- **Yes, create a simple ICMP monitor**
  Select this option if you want the iApp to create a simple ICMP ping monitor for the MFA servers.
- **No, do not monitor MFA (RADIUS) servers**
  Select this option if you do not want the system to monitor the MFA servers.

e. *Which log settings would you like to use to log APM events?*
Select the APM logging profile you want to use for the Access Policy created for this deployment. The iApp does not create an APM logging profile, you must manually create one outside the iApp or select Do not specify a logging profile for the APM profile.

- *Select an existing logging profile*
  If you already created an APM logging profile, select it from the list. If you want to create a profile manually, but have not already done so, you must exit the template and create the object before it becomes available from the list.
- **Do not specify a logging profile for the APM profile**
  Select this option if you do not want to specify an APM logging profile.

Advanced Firewall Manager (BIG-IP AFM)

This section gathers information about BIG-IP Advanced Firewall Manager if you want to use it to protect the AD FS deployment. For 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 AD FS deployment. If you choose to use BIG-IP AFM, you can restrict access to the AD FS 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 *SSL Encryption on page 15*.
- *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 AD FS 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 AD FS 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 AD FS virtual server by IP address or network address.

    a. *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 AD FS 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 AD FS 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.*

- **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 AD FS 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 AD FS 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.

e. *Which Denial-of-Service profile do you want to use?* Advanced
If you created a Denial-of-Service profile for this implementation, select it from the list. The Denial-of-Service (DoS) profile can enable Layer 7 application DoS protection of HTTP traffic and Layer 7 DoS protection for SIP and DNS traffic. The iApp template does not create a DoS profile, if you want to use this functionality, you must create a custom DoS Profile outside the template.

- **Do not use a DoS profile**
  Select this option if you do not want use a DoS profile at this time. You can always re-enter the template at a later date to add this profile. Continue with the next question.
- *Select an existing DoS profile from the list*
  If you have already created a DoS profile for this implementation, select it from the list. Only policies that already exist on the system appear in the list. Specific instructions for creating a DoS profile is outside the scope of this iApp and deployment guide.

Application Security Manager (ASM)

This section gathers information about BIG-IP Application Security Manager if you want to use it to help protect your deployment. This section only appears if you have fully licensed and provisioned BIG-IP ASM. Contact your F5 sales representative for details.

Important _In order to use BIG-IP ASM, you must have manually created a BIG-IP LTM Policy that includes ASM and applicable Rules. Creating an LTM policy is outside the scope of this guide. For specific information, see the Help tab or BIG-IP documentation._

1. _Do you want to deploy BIG-IP Application Security Manager?_
   Choose whether you want to use BIG-IP ASM to help secure this AD FS deployment. If you choose to use BIG-IP ASM, you must have a BIG-IP LTM policy with ASM enabled.

   - **No, 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. Continue with the next section.
   - _Select an existing LTM policy with ASM enabled from the list_
     If you already created a BIG-IP LTM policy with ASM enabled for this implementation, select it from the list. Only LTM Policy objects with ASM enabled appear in the list. If you do not have any applicable policies, the only option you see is No, do not use Application Security Manager.

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?_
   This question does not appear if you are using BIG-IP APM. If using APM, start this section with the "Which Client SSL Profile do you want to use?" question.

   Choose how you want the system to handle encrypted traffic from AD FS clients.

   - **Encrypted traffic is forwarded without decryption (SSL pass-through)**
     Select this method if you want the highest performance, or if your environment does not allow SSL decryption. In this case, the BIG-IP system sends encrypted traffic to the servers without unencrypting it.

     If you select this method, the system creates a Performance (Layer 4) virtual server. Continue with _High Availability on page 16._
   - **Terminate SSL from clients, re-encrypt to servers (SSL Bridging)**
     Select 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.

     a. _Which Client SSL profile do you want to use?_
        Choose 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

          a. _Which SSL certificate do you want to use?_
             Select the SSL certificate you imported for this implementation.

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

c. *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.

d. *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, the recommended Server SSL profile uses the serverssl parent. 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*.

High Availability

This section gathers information about your AD FS deployment that is 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 AD FS 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 AD FS servers.

2. ***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 AD FS 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.

3. ***Which FQDNs will clients use to access the AD FS?***
   Type each fully qualified domain name clients will use to access the AD FS 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 AD FS Apps in AD FS 2013, or if you have Office Web Apps accessed through the AD FS virtual server, you must also add those FQDN(s).

4. ***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 AD FS servers to log the value of this header. For more information on configuring logging see *Appendix C: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 39*. If you are using AD FS 2012 or 2016 (3.0 or 4.0), be sure to see the Important note in that section.

- **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.

5. *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 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 AD FS 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.

   - **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 AD FS server pool. We recommend the default, **Least Connections (member)**.

     b. *Should the BIG-IP system 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.

     c. *Use a Slow Ramp time for newly added servers?* **Advanced**
        Choose whether you want to use a Slow Ramp time. With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added AD FS 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 AD FS servers), as the BIG-IP system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

        - **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.

d. *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 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 manuals 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.

     a. *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.

e. *Which servers should be included in this pool?*
   Specify the IP address(es) of your AD FS 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.

6. *Do you want to configure support for client certificate authentication?*
   Choose whether you want the iApp to configure the BIG-IP LTM to support client certificate authentication. If you select Yes, the iApp creates the objects needed for certificate authentication. This uses port 49443 by default, which is based on Microsoft's alternate port configuration. You can change this port in the subsequent question if you select Yes.

   - **No, do not create the configuration**
     Select this option if you do not need the iApp to create support for certificate authentication.

   - **Yes, configure support for client certificate authentication**
     Select this option to have the iApp create the objects for supporting certificate authentication.

     a. *What port do you want to use for client certificate authentication?* Advanced
        Type the port you want to use for client certificate authentication, if different than Microsoft's default of 49443.

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 AD FS 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.

   - *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 20.*

   - **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 HTTP URI should be sent to the servers?*
        The HTTP URI is used to specify the resource on the AD FS server to query for each pool member to determine availability

of that AD FS server. The default URI string (**/adfs/fs/federationserverservice.asmx**) can be customized to request a specific federation endpoint/URI to determine server availability depending on your specific needs.

The most typical reason for modifying the URI is if you are load balancing to AD FS proxy servers instead of directly to AD FS servers, as with proxy servers the default URI may not be available.
If you are using AD FS proxy servers, we recommend using the following URI:
/FederationMetadata/2007-06/FederationMetadata.xml.

c. *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.

d. *Should the health monitor require credentials?*
Choose whether you want the system to attempt to authenticate to the AD FS servers 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.

  a. *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.

  b. *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.

  a. *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.*

  b. *What is the associated password?*
  Type the password for the account.

Client Optimization

This section gathers information on the type of client optimization you want the system to perform.

1. *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 AD FS servers, select it from the list.

Server Optimization

This section gathers information on the type of server optimization you want the system to perform.

1. ***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 AD FS servers, select it from the list.

iRules

In this section, you can add custom iRules to the AD FS 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 AD FS virtual server?*** Advanced
   Select if have preexisting iRules you want to add to your AD FS implementation.

   ⚠ *Warning* *While iRules can provide additional functionality not present in the iApp, improper use or misconfiguration of an iRule can result in unwanted application behavior and poor performance of your BIG-IP system. We recommended you verify the impact of an iRule prior to deployment in a production environment.*

   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 AD FS 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.

Finished

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

Configuring the BIG-IP system to support client certificate authentication and device registration (iApp version f5.microsoft_adfs.v1.0.0 or manual configuration only)

Version 1.0.0 of the iApp template does not create the configuration objects for clients using certificate authentication or device registration. If your clients are using certificate authentication or device registration and you are using f5.microsoft_adfs.v1.0.0, you must configure these objects manually.

If your clients are not using certificate authentication or device registration, or you are using f5.microsoft_adfs.v1.1.0rc1, you **do not** need to create these objects, the iApp creates them automatically.

If you are using iApp version f5.microsoft_adfs.v1.2.0rc1, the iApp now asks a question asking if you want to support certificate authentication and device registration.

If you are manually configuring the BIG-IP system, and need to support client certificate authentication and device registration, you must create these objects.

Use the following tables for guidance on configuring the load balancing pool and virtual server.

Pools (*Main tab > Local Traffic > Pools*)	
Name	Type a unique name
Health Monitor	**TCP**
Load Balancing Method	**Least Connections (Member)**
Address	Type the IP Address of an AD FS server or AD FS Proxy Server
Service Port	**49443** Click **Add** to repeat Address and Port for all AD FS nodes

Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)	
Name	Type a unique name.
Type	**Performance (Layer 4)**
Destination Address	Type the same IP address of the virtual server you specified for the AD FS or AD FS Proxy virtual server. If you used the iApp template, this is the IP address you entered for the question "What IP address do you want to use for the virtual server?"
Service Port	**49443**
Protocol Profile (client)	**fastL4**
Default Pool	Select the pool you created above

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Microsoft AD FS service you just created. To see the list of all the configuration objects created to support the AD FS 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 AD FS 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 AD FS 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 AD FS 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 AD FS 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.

Optional: Supporting Forms SSO for applications the use claims-based auth in AD FS

You do not need to perform these steps if you are using iApp version f5.microsoft_adfs.v1.2.0rc1 or later.

If your implementation requires you to support Forms SSO for your application when you are using claims-based auth in AD FS, you need to create the additional SSO and iRule objects on the BIG-IP system, and then re-enter the iApp template to select the iRule object you created. The following example describes how to enable Forms SSO for Microsoft SharePoint or Dynamics CRM.

If you are using f5.microsoft_adfs.v1.2.0rc1, the iApp now asks a question about Forms SSO support.

➡ ***Note:*** *The form parameter names for your application may vary from the values used in this example*

Creating the SSO Configuration object

The first task is to create a new Forms - Client Initiated SSO Configuration object on the BIG-IP APM.

To create the new SSO Configuration

1. From the BIG-IP Configuration utility, click **Access Policy > SSO Configurations > Forms - Client Initiated > Create**.
2. In the **SSO Configuration Name** field, type a unique name.
3. In the left navigation pane, click **Form Settings**.
4. Click **Create**.
5. In the **Form Name** field, type a unique a name.
6. In the left navigation pane, click **Form Parameters**.
7. Click **Create**.
8. From the **Form Name** list, type **UserName**.
   IMPORTANT: *DO NOT* just select 'username' from the list, type **UserName** case sensitive. Be cautious about the autocomplete which may try to change the entry to username.
9. From the **Form Parameter Value** list, type **%{session.sso.token.last.username}@domain.com**. Note: **domain.com** could also be %{session.ad.last.actualdomain} to match the domain associated with the APM logon page.
10. Click **OK**.
11. Click **Create**.
12. From the **Form Parameter Name** list, type **Password**. Again, ***you must type this name*** and NOT select password.
13. From the **Form Parameter Value** list, select **%{session.sso.token.last.password}**.
14. From the **Secure** list, select **Yes**.
15. Click **OK**.
16. In the left navigation pane, click **Form Detection**.
17. In the **Request URI** field, type **/adfs/ls**. Do NOT click Ok.
18. In the left navigation pane, click **Form Identification**.
19. From the **Identify Form by** list, select **ID Attribute**.
20. In the **Form ID** field, type **loginForm**.
21. In the left navigation pane, click **Logon Detection**.
22. From the **Detect Login by** list, select **Presence of Cookie**.
23. In the **Cookie Name** field, type **MSISAuth**.
24. Leave all the rest of the settings at the default levels, and then click **OK**.

Creating the iRule

The next step is to create an iRule for selecting the SSO object you just created. This URI is used by SharePoint and Dynamics CRM. IMPORTANT: You must change line 4 in the iRule (highlighted in red) to match the path and name of the SSO object you just created.

To create the iRule

1. Click **Local Traffic > iRules** and then click **Create**.
2. In the **Name** field, type a unique name.
3. In the **Definition** section, copy and paste the following code, omitting the line numbers. Make sure to change the path and name to match the SSO object you just created.

```
1  when ACCESS_ACL_ALLOWED {
2      set req_uri [HTTP::uri]
3      if { $req_uri starts_with "/adfs/ls" } {
4              set ssoconfig /Common/ADFS_Form_CRM_2.0
5              WEBSSO::select $ssoconfig
6              unset ssoconfig
7      }
8      unset req_uri
9  }
```

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 AD FS configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your AD FS 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.

Troubleshooting

Use this section to find any known issues and common troubleshooting steps.

➤ *The BIG-IP APM Access Policy session remains active after a user signs out of an AD FS federated application*

After a user signs out of an AD FS federation application, the APM session remains active until the session **Inactivity Timeout** expires.

Important *If you are using App version v1.2.0rc1 and later, and selected to use Forms SSO in the iApp template, you do not need to create this iRule for the /adfs/ls endpoint. This iRule is now created by the iApp in the forms selection SSO iRule.*

To resolve this issue, use the following procedure to create an iRule and attach it to the configuration using the iApp template. This ensures the APM session is removed when a user signs out.

Note: This iRule redirects the user to the APM logout page. To start a new session, the user must send a new request to the federated application.

1. On the Main tab, expand **Local Traffic** and then click **iRules**.
2. Click **Create**.
3. In the **Name** box, type a unique name for this iRule.
4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers. In line 2, **/adfs/ls** corresponds to the URI from the SAML Logout Endpoint Trusted URL you configured in the application's Relying Party Trust in AD FS.

```
1  when HTTP_REQUEST {
2      if { [string tolower [HTTP::uri]] contains "/adfs/ls/?wa=wsignout1.0" } {
3          ACCESS::session remove
4          HTTP::respond 302 Location "https://[HTTP::host]/vdesk/hangup.php3"
5      }
6  }
```

5. Click the **Finished** button.
6. Re-enter the iApp template (on the Main tab, click **iApp** > **Application Services** > [name of your AD FS application service] and then from the Menu bar, click **Reconfigure**).
7. From the *Which configuration mode do you want to use?* question, select **Advanced - configure advanced options**.
8. 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 box.
9. Click the **Update** button.

➤ *When using LTM to load balance AD FS (no AD FS proxy replacement), AD FS Proxy (WAP or another BIG-IP APM replacing WAP) cannot establish and maintain trust to the AD FS servers and/or clients are failing client certificate authentication.*

The most likely cause is use of SSL bridging, which breaks the client certificate authentication between the proxy/client and AD FS server. To avoid this issue, from the 'How should the BIG-IP system handle SSL traffic?' question, select **SSL pass-through**.

➤ *After establishing or reestablishing AD FS trust my users get HTTP error "404 Not Found" when accessing AD FS.*

The new trust may take a moment to take effect. If you wait a minute or so and the problem persists, you can restart the adfs_proxy service on the BIG-IP system from the CLI by typing the following command:
`bigstart restart adfs_proxy`.

- *The trust certificate has expired and must be reestablished.*

  The BIG-IP will reestablish trust automatically, but cannot if it or the Primary AD FS server is offline. To manually reestablish trust after expiration (or for any other reason), go to the virtual server acting as AD FS proxy (the name will end with _adfs_vs_443), find the "AD FS Proxy" section, note it is enabled, evaluate the certificate expiration date, and click the reestablish trust button. Credentials must be specified in the domain\username or username@domain.com (UPN) format.

- *When trying to establish trust the request is rejected*.

  This is usually caused by the AD FS service not functioning on the primary AD FS server. The primary server is required to establish trust.

- *When trying to establish trust, you receive the following error: "Failed to establish ADFS trust relationship"…."Can't connect to AD FS."*

  The BIG-IP is unable to communicate with the primary AD FS server. The primary server is required to establish trust. This error will occur if you attempt to establish trust from a standby device. Trust must be established from the active device in the HA group.

Appendix A: Manual Configuration tables

The following tables contain a list of BIG-IP 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: SSL Bridging

Use this table if you are configuring the system for SSL Bridging (you must configure bridging if using APM). If using SSL Pass-through, see *Configuring the BIG-IP LTM for load balancing AD FS or AD FS proxy servers: SSL Pass-through on page 29*.

Health Monitors (*Main tab > Local Traffic > Monitors*)		
If using AD FS 2.0, choose one of the first two monitors. If using AD FS 2012 or 2016 (3.0 or 4.0), 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 2012 or 2016 (3.0 or 4.0): External Monitor		
Name	Type a unique name	
Type	**External**	
Interval	**30** (recommended)	
External Program	See *Importing the script file for AD FS 2012 or 2016 (3.0 or 4.0) health monitor on page 28*	
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	Type a unique name
	Parent Profile	**http**
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**
Client SSL *(Profiles > SSL)*	Name	Type a unique name
	Parent Profile	**clientssl**
	Certificate and Key	Select the Certificate and Key you imported from the associated list

[1] *Replace red text with your FQDN*

Profiles continued		
Server SSL *(Profiles > Other)*	Name	Type a unique name
	Parent Profile	**serverssl**
	Server Name <only 2012>	Type the FQDN clients will use to access the AD FS deployment (If using AD FS 2012 (3.0), this must be the same value as the monitor HOST variable)

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
Protocol Profile (server)	Select the LAN optimized TCP profile you created
HTTP Profile	Select the HTTP profile you created
SSL Profile (Client)	Select the Client SSL profile you created
SSL Profile (Server)	If you created a Server SSL profile, select it from the list
Source Address Translation[2]	**Auto Map[2]**
Default Pool	Select the pool you created

[2] *In version 11.0-11.2.x, this field is **SNAT Pool**. 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.*

Important: If your clients are using certificate authentication or device registration, see *Configuring the BIG-IP system to support client certificate authentication (iApp version f5.microsoft_adfs.v1.0.0 or manual configuration only) on page 21.*

Importing the script file for AD FS 2012 or 2016 (3.0 or 4.0) 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 LTM for load balancing AD FS or AD FS proxy servers: SSL Pass-through

Use this table if you are configuring the system for SSL Bridging (you must configure bridging if using APM).

Health Monitors (*Main tab > Local Traffic > Monitors*)

If using AD FS 2.0, choose one of the first two monitors. If using AD FS 2012 or 2016 (3.0 or 4.0), 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 2012 or 2016 (3.0 or 4.0): External Monitor

Name	Type a unique name
Type	**External**
Interval	**30** (recommended)
External Program	See *Importing the script file for AD FS 2012 or 2016 (3.0 or 4.0) health monitor on page 28*
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*)

Fast L4 *(Profiles > Services)*	Name	Type a unique name
	Parent Profile	**fastL4**

Virtual Servers (*Main tab > Local Traffic > Virtual Servers*)

Name	Type a unique name.
Type	**Performance (Layer 4)**
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
Source Address Translation[2]	**Auto Map**[2]
Default Pool	Select the pool you created above

[1] *Replace red text with your FQDN*

[2] *In version 11.0-11.2.x, this field is* ***SNAT Pool****. 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.*

Manually 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 iApp template 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 B: Configuring DNS and NTP on the BIG-IP system on page 38* 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	
Forms based SSO Configuration (optional: if you are using the /adfs/ls endpoint you must create this to allow for SSO based on SAML)		
SSO Configurations By Type	**Forms-Client Initiated**	
SSO Configuration Name	Type a unique name. We use **form_based_sso_adfs**	
*In the left pane of the box, click **Form Settings**, and then click **Create**.*		
Form Name	Type a unique name. We use **adfs_ls_endpoint_form**	
*In the left pane of the box, click **Form Parameters**, and then click **Create***		
Form Parameters	**Form Name**	Type **UserName.** IMPORTANT: This name is case sensitive, do NOT just select 'username' from the list. Be cautious as autocomplete may try to change this to username.
	Form Parameter Value	**%{session.sso.token.last.username}@domain.com.** Note: domain.com could also be %{session.ad.last.actualdomain} to match the domain associated with the APM logon page**.**
	Click **Ok**, and then click **Create** again in the Forms Parameters box.	
	Form Parameter Name	Type **Password.** IMPORTANT: This name is case sensitive, do NOT just select 'password'
	Form Parameter Value	**%{session.sso.token.last.password}**
	Secure	**Yes** Click **Ok**.
Form Detection	In the left page of the Create New Form Definition box, click **Form Detection**.	
	Detect Form by	Select **URI**
	Request URI	Type **/adfs/ls**. Do NOT click OK at this point.
Form Identification	In the left page of the Create New Form Definition box, click **Form Identification**.	
	Identify Form by	Select **ID Attribute**
	Form ID	Type **loginForm**
Logon Detection	In the left page of the Create New Form Definition box, click **Logon Detection**.	
	Detect Logon by	Select **Presence of Cookie**
	Cookie Name	Type **MSISAuth**. Leave the other settings at the defaults and then click **OK**.

iRules (*Main tab > Local Traffic > iRules*)	
AD FS pip iRule. See AD FS pip iRule on page 31	
Name	Type a unique name
Definition	Use the Definition in *AD FS pip iRule on page 31*
Forms SSO iRule. ***If you are using Forms SSO for the /adfs/ls endpoints, you must create this iRule****. See Forms SSO selection iRule on page 32*	
Name	Type a unique name
Definition	Use the Definition in *Forms SSO selection iRule on page 32*
Optional: *This optional iRule disables APM for MS Federation Gateway. See Optional iRule to disable APM for MS Federation Gateway on page 33*	
Name	Type a unique name
Definition	Use the Definition in *Optional iRule to disable APM for MS Federation Gateway on page 33*
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	Select the AD FS pip and Forms SSO iRules if applicable. If you created the iRule to disable APM for MS Federation Gateway, select the iRule and Enable it.

AD FS pip iRule

This iRule adds the required headers for AD FS advanced rule functionality. For more information, see *https://technet.microsoft.com/en-us/library/dn592182.aspx*.

```
when CLIENT_ACCEPTED {
    set client_ip [IP::remote_addr]
}
when HTTP_REQUEST {
      # Add headers required for certain rules on ADFS backend servers
    HTTP::header insert X-MS-Proxy [HTTP::host]
    HTTP::header insert X-MS-Forwarded-Client-IP $client_ip
    HTTP::header insert X-MS-Endpoint-Absolute-Path [HTTP::uri]
    HTTP::header insert X-MS-Target-Role "PrimaryComputer"
    HTTP::header insert X-MS-ADFS-Proxy-Client-IP $client_ip
}
```

Forms SSO selection iRule

This iRule selects the appropriate APM SSO object, and handles URI logout as well.

You must change line 9 to match your Forms SSO object name and path.

```
1   when CLIENT_ACCEPTED {
2       event HTTP_RESPONSE disable
3         set no_referer_flag false
4   }
5   # Set SSO for /adfs/ls endpoint
6   when ACCESS_ACL_ALLOWED {
7       set req_uri [HTTP::uri]
8       if { $req_uri starts_with "/adfs/ls" } {
9               set ssoconfig <path and name of Forms SSO object>
10              WEBSSO::select $ssoconfig
11              unset ssoconfig
12      }
13      unset req_uri
14  }
15  # Delete session when application redirects back to ADFS for sign out
16  when HTTP_REQUEST {
17      if { [string tolower [HTTP::uri]] contains "/adfs/ls/?wa=wsignout1.0" } {
18           if { [HTTP::header exists "Referer"] } {
19              ACCESS::session remove
20                     HTTP::redirect [HTTP::header value "Referer"]
21           } else {
22               event HTTP_RESPONSE enable
23               set no_referer_flag true
24           }
25      }
26  }
27  # If no referer header, we will just allow client through to ADFS sign out page and then kill the APM session
28  when HTTP_RESPONSE {
29      if { $no_referer_flag } {
30          ACCESS::session remove
31      }
32  }
```

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.

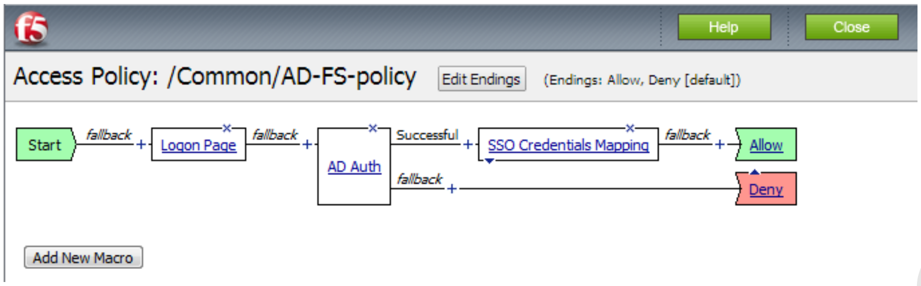

Figure 4: *Logical configuration diagram: Using BIG-IP APM*

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
   }
}
```

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

This section describes how to manually configure BIG-IP AFM, F5's Network Firewall module, to secure your AD FS 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 **AD-FS-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 **AD-FS-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 **AD-FS-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 36*, 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 AD FS 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 AD FS virtual server

If you want to restrict access to your AD FS 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 virtual server:

To assign the IP intelligence policy to the AD FS virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your AD FS 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 display. 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 AD FS 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 34)*.
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 AD FS virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.

2. Click the name of your AD FS 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.

This completes the BIG-IP AFM configuration.

Appendix B: 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.

Appendix C: 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.

ⓘ ***Important*** *The guidance in this section applies to AD FS 2.0 only. AD FS 2012 and 2016 (3.0 and 4.0) do not use the full IIS role, but do use http.sys. It is still possible to use the X-Forwarded-For header with some advanced configuration. For details, see https://migration-blog.com/2015/11/26/adfs-how-to-enable-trace-debugging-and-advanced-access-logging/. Note that this website is not hosted by F5, the link may change without notice. F5 does not guarantee the accuracy of this information.*

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 AD FS 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.

Document Revision History

Version	Description	Date
1.0	New version of this deployment guide for the AD FS iApp template	09-09-2015
1.1	Added the section *Optional: Supporting Forms SSO for applications the use claims-based auth in AD FS on page 23*	02-24-2016
1.2	- Added support for BIG-IP v12.1 - Added a note clarifying the HTTP URI, and what to use when using AD FS proxy servers to *b. What HTTP URI should be sent to the servers? on page 18.*	05-18-2016
1.3	Added the new section *Configuring the BIG-IP system to support client certificate authentication and device registration (iApp version f5.microsoft_adfs.v1.0.0 or manual configuration only) on page 21.*	08-02-2016
1.4	Added the new section *Troubleshooting on page 25,* with an entry regarding APM Access Policy sessions remaining active after users sign out of an AD FS federated application.	08-30-2016
1.5	Updated this guide for iApp version f5.microsoft_adfs.v1.1.0rc1 on downloads.f5.com. There are no visible changes to the iApp presentation. v1.1.0rc1 contains the following features: - Added the BIG-IP configuration objects to the iApp configuration to support client certificate authentication and device registration. - Added support for versions 12.1 and 12.1.1.	10-18-2016
1.6	Modified the section *Optional: Supporting Forms SSO for applications the use claims-based auth in AD FS on page 23* to note you can used the guidance for other applications and not just SharePoint and Dynamics CRM. Added a reference to this section from the Prerequisites.	10-31-2016
1.7	Updated this deployment guide for f5.microsoft_adfs.v1.2.0rc1 on downloads.f5.com in the RELEASE_CANDIDATE directory. This version of the iApp contained the following changes: - Added support for AD FS version 4.0. - Added the capability to select an existing APM profile. - The iApp now asks a question for support of port 49443 certificate authentication objects. - If using BIG-IP APM, the iApp now handles ADFSPIP header creation using an iRule. - Added Forms SSO and iRule objects for /adfs/ls endpoints. - Added Logout URI handling via the Forms SSO iRule.	02-08-2017
1.8	- Added support for BIG-IP v13.0	02-22-2017
1.9	Updated this deployment guide for f5.microsoft_adfs.v1.2.0rc2 on downloads.f5.com in the RELEASE_CANDIDATE directory. This version of the iApp contained the following changes: - Fixed an issue related to selecting a pre-existing health monitor. - Removed an unnecessary source address persistence profile from the virtual server created by the iApp. Removed this profile from the manual configuration tables.	03-29-2017
2.0	- Corrected the iRule in the Troubleshooting entry: *The BIG-IP APM Access Policy session remains active after a user signs out of an AD FS federated application on page 25.*	05-03-2017
2.1	- Updated this deployment guide for f5.microsoft_adfs.v1.2.0rc3 on downloads.f5.com in the RELEASE_CANDIDATE directory. This version of the iApp added support for Azure multi-factor authentication (MFA) in the APM policy. - Added information about using the X-Forwarded-For header with AD FS 3.0 and 4.0 to *Appendix C: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 39.*	07-11-2017
2.2	- Updated this deployment guide for f5.microsoft_adfs.v1.2.0rc5 on downloads.f5.com in the RELEASE_CANDIDATE directory. This version contains the following changes (no visible changes to this guide or the iApp presentation): - The iApp template now deletes all objects associated with the iApp template then the application service is deleted. Previously, if running a prior iApp version using BIG-IP v13.1 (only), two objects were created outside of the partition created by the iApp and were not deleted. - In 13.1 and later only: The iApp now alerts the user to errors when running the "establish-adfs-trust" utility, such as with incorrect credentials.	10-12-2017

Version	Description	Date
2.3	Updated this guide for iApp template version f5.microsoft_adfs.v1.2.0rc6 which includes the following changes: - Added support for BIG-IP v13.1. - Updated the iApp with new BIG-IP AFM IP Intelligence threat categories to support BIG-IP v13.1. - Added support for route domain 0 from non-Common partitions.	11-09-2017
2.4	Updated this guide for iApp template version f5.microsoft_adfs.v1.2.0rc7 which includes the following changes: - Added support for including an existing ASM policy in the iApp configuration. - Added support for including an existing DOS policy in the iApp configuration. - Added an inline help message in the iApp with the recommended health monitor Send String if using AD FS Proxy. - Modified the labels in the iApp to more accurately reflect AD FS versions (for example, AD FS 4.0 is now AD FS 2016) - Added support for using a custom port for client certificate authentication.	03-22-2018
2.5	Updated this guide for iApp template version f5.microsoft_adfs.v1.2.0rc8 which includes the following changes: - Fixed an issue where the iApp could not read ::vs_pool__cert_auth_trusted_ca variable and would fail.	07-26-2018
2.6	Updated this guide for iApp template version f5.microsoft_adfs.v1.2.0rc9 which includes the following changes: - Corrected an issue that caused TCL iApps using client-ssl profiles to break when the iApp was reconfigured. This issue only affected iApps running on BIG-IP 14.1.	01-31-2019
2.7	- Added information the the Troubleshooting section to on page 26 to indicate that trust must be established from the active device in an HA group.	04-26-2019