Deployment Guide



# Deploying the BIG-IP LTM and APM with Citrix XenApp or XenDesktop

Welcome to the F5 deployment guide for Citrix® XenApp® with BIG-IP v11.2 and later. This guide shows how to configure the BIG-IP Local Traffic Manager (LTM) and Access Policy Manager (APM) for delivering a complete remote access and intelligent traffic management solution that ensures application availability, improves performance and provides a flexible layer of security for Citrix XenApp and XenDesktop deployments.

This document also contains guidance on configuring the BIG-IP system for Citrix StoreFront, as well as using the BIG-IP APM for two factor authentication with RSA SecurID.

This guide and associated iApp template replaces the previous guides and iApps for Citrix XenApp and LTM, Citrix XenDesktop and LTM, and both XenApp and XenDesktop with BIG-IP APM.

### Products and versions

| Product | Versions |
|---|---|
| BIG-IP LTM and APM | 11.2, 11.2 HF-1, 11.3, 11.4, 11.4.1 |
| Citrix XenApp | 6.5[1] |
| Citrix XenDesktop | 7.1, 7.0, 5.6 and 5.5[1] |
| Citrix StoreFront | 1.0, 1.1, 1.2, 2.0, and 2.1 |
| iApp Template version | f5.citrix_vdiv1.1.0rc6 RELEASE CANDIDATE |
| Deployment Guide revision | RC-6 (see *Document Revision History on page 55*) |

[1] The iApp template can be used with XenApp and XenDesktop 4.0 and later with no modifications

**Important:** *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/iapp-xenapp-xendesktop-dg-RC-6.pdf*

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

# Contents

## Why F5

While Citrix XenApp and XenDesktop products provide users with the ability to deliver applications "on-demand to any user, anywhere," the F5 BIG-IP system secures and scales the environment, and can act as a replacement for Citrix Web Interface servers.

In a Citrix environment, the BIG-IP LTM provides intelligent traffic management and high-availability by monitoring and managing connections to the Citrix Web Interface and the Citrix XML Broker components. In addition, the built-in performance optimization capabilities of the LTM provide faster operations to facilitate a better end-user experience. The LTM also keeps persistence records for certain connections to always be directed to the same server for a specified period of time, to ensure that the workflow in the CItrix environment is fully preserved.

Additionally, the BIG-IP system can securely proxy Citrix ICA traffic, using TCP optimization profiles which increase overall network performance for your application. You also have the option to configure the BIG-IP APM with smart card authentication or with two factor authentication using RSA SecurID.

The classic deployment of Citrix XenApp and XenDesktop allows organizations to centralize applications; this guide describes configuring access and delivering applications as needed with the BIG-IP system.

## What is F5 iApp?

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

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

## Prerequisites and configuration notes

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

- This guide was written for Citrix XenApp version 6.5, and XenDesktop version 7.1, 7.0, 5.6 and 5.5. If you are using a previous version, see the deployment guide index on F5.com.
- The iApp template referenced in this guide is a RELEASE CANDIDATE, and available on DevCentral. This means it has been created and tested by F5 Solution Engineers, but has not yet completed full regression testing. Once regression testing is complete, it will be available as an ESD release on downloads.f5.com.
- This document is written with the assumption that you are familiar with both F5 devices and Citrix XenApp or XenDesktop products. For more information on configuring these devices, consult the appropriate documentation.
- For this deployment guide, the BIG-IP system ***must*** be running version 11.2 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. This guide does not apply to previous versions.
- The majority of this document provides guidance for the iApp for your Citrix deployment. For users familiar with the BIG-IP system, there are manual configuration tables at the end of this guide. Because of the complexity of the configuration, we strongly recommend using the iApp template.
- You can optionally configure the BIG-IP APM with smart card authentication or with two-factor authentication using RSA SecurID.
  - If deploying two factor authentication using SecurID, you must upload your SecurID access agent configuration file to the BIG-IP system using iFile prior to running the iApp. If you have not uploaded your SecurID configuation file, go to System>>File Management: iFile List, and then click Import.
  - If deploying smart card authentication, be sure to see *Appendix A: Citrix server changes required to support smart card authentication on page 32.* Note we currently do not support smart card authentication with StoreFront; only Web Interface server 5.4 is supported.

- Citrix Session configuration must be set to Direct mode (see Figure 1). For specific information on configuring the Citrix Session mode, see the Citrix documentation.

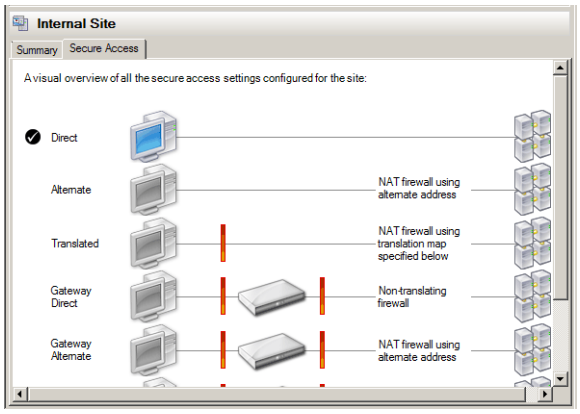



**Figure 1:** *Citrix Session configuration*

## Deployment Scenarios

This section describes the three main scenarios described in this document.

### Using the BIG-IP LTM

This configuration example describes the typical configuration of the BIG-IP LTM system to monitor and manage the critical components of a Citrix XenApp or XenDesktop environment, namely the Web Interface servers and the XML Broker servers.

In this implementation, traffic to the Citrix Web Interface servers and the Citrix XML Broker servers is managed by the F5 BIG-IP LTM system, and when necessary, ensures that each client connects to the same member of the farm across multiple sessions using persistence on the BIG-IP LTM. The F5 BIG-IP LTM system is also setup to monitor the Citrix Web Interface servers and Citrix XML Broker servers to ensure availability and automatically mark down servers that are not operating correctly. The ability to terminate SSL sessions in order to offload this processing from the Citrix devices is also available with a simple addition of the Client SSL profile to the web interface virtual server referred to in this guide.

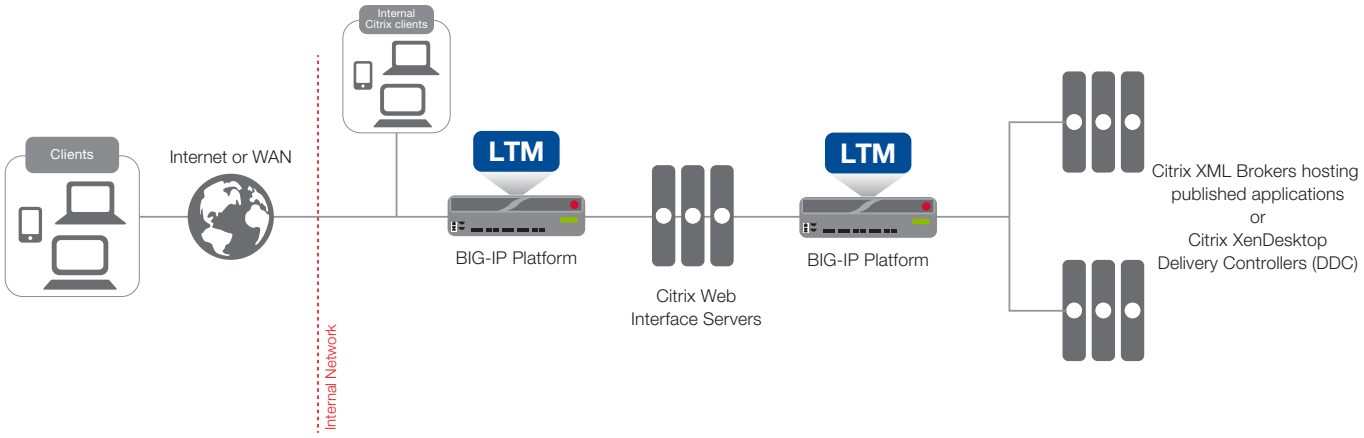



**Figure 2:** *Logical configuration example*

## Using the BIG-IP APM with Dynamic Webtops to replace Web Interface servers

In this scenario, the BIG-IP APM Dynamic Presentation Webtop functionality is used to replace the Citrix Web Interface tier. With BIG-IP APM, a front-end virtual server is created to provide security, compliance and control. The iApp template configures the APM using Secure ICA Proxy mode. In secure ICA proxy mode, no F5 BIG-IP APM client is required for network access. The BIG-IP system uses SSL on the public (non-secure) network and ICA to the servers on local (secure) network.

Through the setup of a secure proxy that traverses APM, remote access for user sessions originating from desktops or mobile devices is possible. Secure proxy mode has many benefits to both users and administrators. For administrations, APM user authentication is tied directly to Citrix's Active Directory store allowing for compliance and administrative control. For users, TCP optimization and application delivery, plus the need for only the Citrix client, creates a fast and efficient experience.

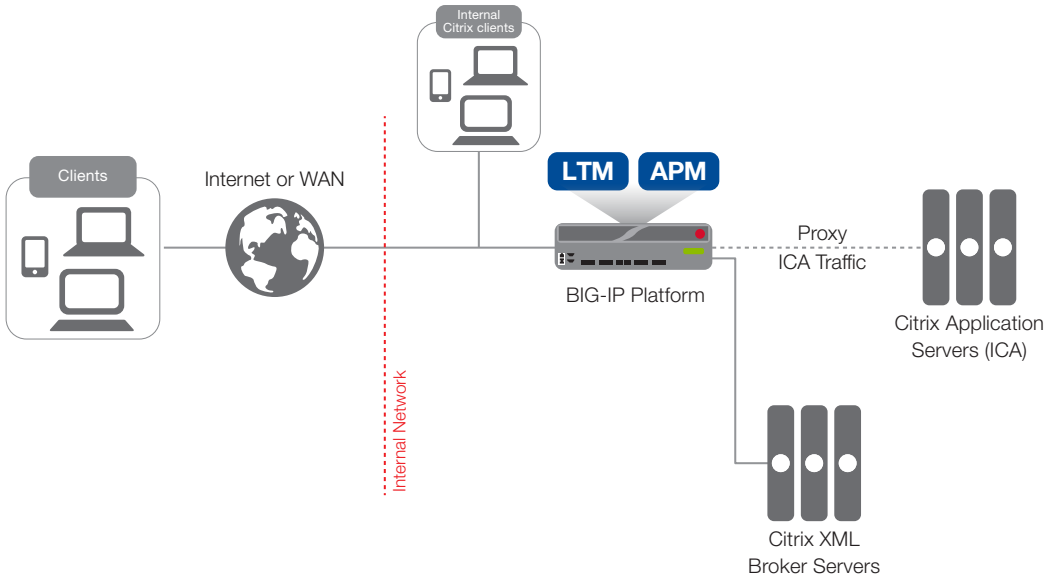



**Figure 3:** *Using the BIG-IP APM to replace the Web Interface servers*

## Using the BIG-IP APM and Web Interface servers

This final scenario is very similar to the previous one. However, in this example, the BIG-IP APM, while still proxying ICA traffic and authenticating users, is not replacing the Web Interface devices.

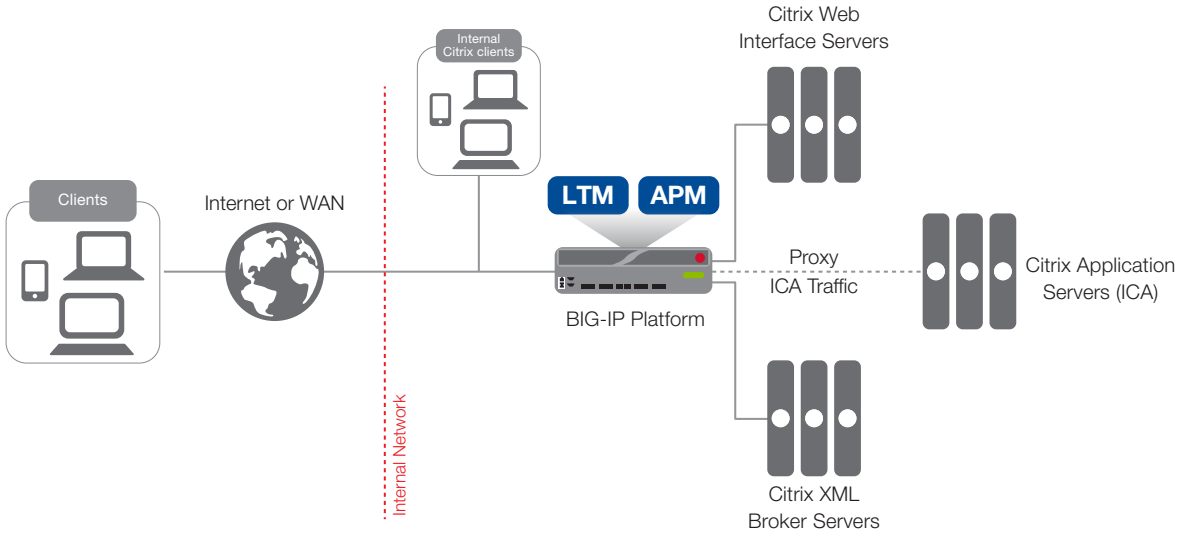



**Figure 4:** *Using the BIG-IP APM with Web Interface servers*

## Downloading and importing the new iApp template

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

**To download and import the iApp**

1. Open a web browser and go to: *https://devcentral.f5.com/wiki/iApp.Citrix-VDI-v1-1-0.ashx*.
2. Download the Citrix XenApp/XenDesktop iApp to a location accessible from your BIG-IP system.
3. Extract (unzip) the **f5.citrix_vdi.v1.1.0rc6** file (or a newer version if applicable).
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

## Configuring the BIG-IP iApp for Citrix XenApp or XenDesktop

Use the following guidance to help you configure the BIG-IP system for XenApp or XenDesktop using the BIG-IP iApp template.

### Getting Started with the iApp

To begin the iApp Template, use the following procedure.

**To start the iApp template**

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 **Citrix-XenApp-.**
5. From the **Template** list, select **f5.citrix_vdi.v1.1.0rc6** (or a newer version if applicable). The Citrix template opens.

### Advanced options

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

1. ***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.

## General

This section of the iApp template asks general questions about the deployment and iApp options.

1. ***Do you want to see inline help?***
   Select whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Show inline help text**.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to show inline help for most questions in the template.
   - **No, do not show inline help text**
     Select this option if you do not want to see inline help. 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, parent profiles, and settings are all set automatically. The F5 recommended settings come as a result of extensive testing with Citrix 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 Citrix application service. This option provides more flexibility for advanced users.

     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 this icon.

3. ***Use APM or Edge Gateway to securely proxy application (ICA) traffic and authenticate users into your Citrix environment?***
   Select whether you are using BIG-IP APM or Edge Gateway to securely proxy application traffic and authenticate users.
   - **Yes, proxy ICA traffic and authenticate users with the BIG-IP**
     If you select Yes, you must have BIG-IP APM or Edge Gateway fully licensed and provisioned on this BIG-IP system. Later in the iApp, you have the option of configuring this BIG-IP system to proxy ICA traffic and authenticate users and then send traffic directly to the Xen servers, or send traffic to a separate BIG-IP system running LTM.
   - **No, do not proxy ICA traffic and authenticate users with the BIG-IP**
     If you select No, the iApp configures the BIG-IP system for intelligent traffic direction and high availability for the Web Interface and XML Broker servers. Later in the iApp you have the option of directing all ICA traffic through this BIG-IP system for security, logging, or network topology purposes.

4. ***What is the Active Directory NetBIOS name used for your Xen servers?***
   Type the Active Directory Domain name in NetBIOS format. This is the Windows domain that is used to authenticate Citrix user accounts.

## BIG-IP Access Policy Manager

If you chose to proxy ICA traffic and authenticate users with the BIG-IP system, in this section you configure the BIG-IP APM options. If you do not see this section, continue with *Virtual Server for Web Interface Servers on page 10.*

1. ***Should the BIG-IP APM support smart card authentication for Citrix access?***
   The BIG-IP APM supports clients authenticating to the Citrix Web Interface servers using smart cards. Select whether your Citrix clients will use smart cards to access the Citrix implementation. Smart card authentication is not supported when using StoreFront; only Web Interface server 5.4 is supported.

***Important***

*Be sure to see Appendix A: Citrix server changes required to support smart card authentication on page 32 for important guidance on configuring your Citrix and Active Directory devices.*

- **No, BIG-IP APM should not support smart card authentication**
  Select this option if you do not require the BIG-IP system to support smart card authentication. Continue with #2.
  If you are deploying the template in Basic mode, continue with #2a.
- **Yes, BIG-IP APM should support smart card authentication**
  Select this option if you want the BIG-IP system to support smart card authentication to the Citrix deployment. Note that with this implementation users must enter their PIN twice; once as they authenticate to the Web Interface server, and once as the Citrix application or desktop is launched.

  a. *Does the smart card UPN match the domain name of your Citrix environment?*
  Choose whether the User Principal Name, located in the smart card client certificates Subject Alternative Name field, will match the domain name of your Citrix Active directory domain.

  - **Yes, the UPNs are the same**
    Select this option if the smart card UPN matches the domain name of the Citrix environment. The iApp does not create an BIG-IP APM Active Directory AAA Server in this case.
  - **No, the UPNs are different**
    Select this option if the UPNs are not the same. In this case, the iApp creates an Active Directory AAA Server profile object which is used to query and determine the correct UPN to use.

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

  c. *Which service account (in SPN format) can be used for Kerberos authentication?*
  Specify a service account in SPN (Service Principal Name) format which can be used to enable Kerberos Protocol Transition and Constrained Delegation from the BIG-IP to Web Interface resources.

  The following is an example user account using SPN format: **host/user@domain.com**

  Where the Service is **host** and the Service Name is **user@domain.com**.

  d. *What is the password associated with that account?*
  Specify the password for the service account you entered in the previous question.

  Credentials are stored in plaintext on your BIG-IP system.

  If you specified the smart card UPN matched your Citrix Active Directory domain name, this completes this section; continue with *Virtual Server for Web Interface Servers on page 10*. Otherwise, continue with #2.

2. ***How do you want to provide AAA services for your deployment?***
*This question only appears if you selected Advanced configuration mode, however Basic mode starts with #2a.*

The AAA Server contains the authentication mechanism for the BIG-IP APM Access Policy.

Select whether you want to the template to create a new BIG-IP APM AAA Server object, or if you have already created an AAA object for XenApp or XenDesktop on the BIG-IP system.

- **Use an existing AAA Server object** Advanced
  Select this option if you have already created an AAA Server object for this deployment. If you want to create your own AAA Server, but have not already done so, you must exit the template and create the object before it becomes available from the list.

  a. *Which AAA Server object do you want to use?*
  Select the AAA Server you created for this implementation from the list. Continue with #3.

- **Create a new AAA Server object**
  Select this option (the default) to have the template create a new Active Directory AAA Server object for the Citrix environment.

  a. *What is the Active Directory FQDN for your Xen users?*
  Type the Active Directory domain name for your XenApp or XenDesktop implementation in FQDN (fully qualified domain name) format.

  b. *Which Active Directory servers in your domain can this BIG-IP system contact?*
  Type both the FQDN and IP address of all Active Directory servers in your domain that this BIG-IP system can contact. Make sure this BIG-IP system and the Active Directory servers have routes to one another and that firewalls allow traffic between the two. Click **Add** to include additional servers.

  c. *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.

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

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

    *These credentials are stored in plaintext on your BIG-IP system.*

  d. *How do you want to handle health monitoring for this pool?*
  You can choose the type of health monitor you want to use for the pool of Active Directory servers. Specify whether you want the template to create a new LDAP monitor or a new ICMP monitor, or if you select an existing monitor.

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

    i). *Which monitor do you want to use?*
    From the list, select the LDAP or External monitor you created to perform health checks for the Active Directory pool created by the template. Only monitors that have a Type value of LDAP or External appear in this list. Continue with #3.

  - **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 #3.
  - **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:

    i). *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.

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

    iii). *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 'Citrix Users' and is in the domain 'citrix.company.com', the LDAP tree would be: ou=Citrix Users, dc=Citrix, dc=company, dc=com.

iv). *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.

v). *How many seconds between Active Directory health checks?* **Advanced**
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.

vi). *Which port is used for Active Directory communication?* **Advanced**
Specify the port being used for communication with your Active Directory implementation. The default port when using the TLS security protocol, or no security, is port 389. The default port used when using the SSL security protocol is 636. The port that appears by default changes depending on your answer to the secure protocol question above.

3. ***Do you want the BIG-IP system to proxy RSA SecurID for two-factor authentication?***
The BIG-IP APM supports two-factor authentication using RSA SecurID. Select whether you want the template to configure two-factor authentication using RSA SecurID.

- **No, do not configure the BIG-IP system for two-factor authentication**
Select this option do not require two-factor authentication at this time. You can always reconfigure the template at a later time to add two-factor authentication. Continue with the next section.
- **Yes, configure the BIG-IP system for two-factor authentication**
Select this option if you want to configure two-factor authentication on the BIG-IP system.

> ***Important***
>
> *You must have an existing SecurID AAA Server object on the BIG-IP APM to use this option. This AAA Server must include your SecurID Configuration file. You must also configure the BIG-IP system as a standard authoritative agent on the RSA Authentication server. For specific information on configuring the RSA server, consult the appropriate RSA documentation.*
>
> *If you do not have an existing SecurID AAA Server object, you can either exit this iApp template, configure the AAA Server object, and then start over; or select "No" now, and then reconfigure the iApp after you have created the SecurID AAA Server object.*

a. *Which AAA Server object do you want to use for SecurID?*
Select the SecurID AAA Server object you created on the BIG-IP APM.

b. *What do you want to call the form field for the RSA SecurID token?*
As mentioned, the logon page produced by the iApp includes additional field to collect the password generated from RSA. You can specify a unique name to use for this field, or leave the default, Passcode.

## Virtual Server for Web Interface Servers

The next section of the template asks questions about the BIG-IP virtual server for the Citrix Web Interface devices. A virtual server is a traffic management object on the BIG-IP system that is represented by an IP address and a service port.

The first questions you see depend on whether you chose to proxy ICA traffic and authenticate users with the BIG-IP system.

If you chose ***not*** to proxy ICA traffic and authenticate users with the BIG-IP system, start with either #3 (if using Advanced), or #4 if using Basic (F5 recommended), on page 12.

1. ***Should this BIG-IP system load balance Citrix traffic or send it to another BIG-IP system?***
*This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system.*

Because you are using the BIG-IP APM to proxy ICA traffic and authenticate users, you can choose whether you want the BIG-IP system you are currently configuring to handle the load balancing duties, or if you want to send the Citrix traffic to a separate BIG-IP system for load balancing.

- **Load balance Citrix traffic on this BIG-IP system**
  Select this option to load balance Citrix services on the BIG-IP system you are currently configuring. In the next sections, you specify information about the Citrix servers.
- **Send Citrix traffic to a separate BIG-IP system**
  Select this option if you are sending the Citrix traffic to a separate BIG-IP system for load balancing. In the next sections, you specify information about the Citrix deployment on the other BIG-IP system.

2. ***Do you want to replace Citrix Web Interface servers with the BIG-IP system?***
   *This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system.*

   You can use the BIG-IP system to eliminate the need for the Citrix Web Interface servers altogether. The BIG-IP system uses a Dynamic Presentation Webtop to present Citrix published applications.

   - **No, do not replace the Citrix Web Interface servers**
     Select this option if you do not want to use the BIG-IP system to replace the Web Interface servers from your environment.

     a. *Do you need to add a custom PNAgent URI?*
        Choose whether you need to add a non-default PNAgent URI to the configuration. If you are using StoreFront, or using a PNAgent URI other than **/Citrix/Pnagent/config.xml**, you must choose Yes, and add the URI in the next question.

        - **No, use the default URI only**
          Select this option if you are only using the default PNAgent URI in your implementation.
        - **Yes, add a custom PNAgent URI**
          Select this option if you have a custom URI in your Citrix environment. The BIG-IP system adds this URI to a Data Group object which is referenced by an iRule to allow dynamic configuration.

          i). *What custom URI do you want to add?*
              Type the custom PNAgent URI supported by your Citrix FQDN. Web Interface servers use /Citrix/PNAgent/config.xml as the default PNAgent URI. StoreFront uses this URI if legacy PNAgent support is enabled, otherwise Citrix clients use /Citrix/<storename>/PNAgent/config.xml.

   - **Yes, replace Citrix Web Interface servers with the BIG-IP system**
     Select this option if you want the BIG-IP system to replace the need for Citrix Web Interface servers. In this case, BIG-IP APM Dynamic Presentation Webtop functionality is used to replace the Citrix Web Interface tier (see *Using the BIG-IP APM with Dynamic Webtops to replace Web Interface servers on page 5* more information).

     For this scenario to work properly, the BIG-IP system must have connectivity to a Citrix XML Broker server, or a BIG-IP virtual server that load balances a pool of XML Broker servers.

3. ***Is traffic coming directly from clients or from a BIG-IP system running APM or Edge Gateway?*** Advanced
   *This question only appears if you chose Advanced and not to proxy ICA traffic and authenticate users with the BIG-IP system.*

   Specify whether Citrix traffic is coming directly from clients, or if it is coming via another BIG-IP system running APM or Edge Gateway. The template asks this question to offer an additional layer of security if traffic is coming from another BIG-IP system.

   - **Traffic is coming directly from clients**
     Select this option if traffic is coming directly from clients. Continue with #4.
   - **Traffic is coming from another BIG-IP system**
     Select this option if you are using a separate BIG-IP system running APM or Edge Gateway, and sending the traffic to this system for load balancing.

     a. *Should this BIG-IP system drop all traffic not coming from the other BIG-IP system?*
        Specify whether you want this BIG-IP system to drop all traffic not coming from the remote BIG-IP system running APM or Edge Gateway. This option enables an additional layer of security for your Citrix deployment.

- **No, allow traffic from any location**
  Select this option if you want to allow traffic from any location. In this scenario, the local BIG-IP system can accept Web Interface traffic directly from users. Continue with #4.

  If you choose to only allow traffic from the other BIG-IP system, you must specify the IP address(es) of the other BIG-IP system from which this BIG-IP system will receive traffic.

- **Yes, only allow traffic from another BIG-IP system**
  Select this option to secure the Web Interface traffic and prevent users from directly making connections to the local BIG-IP system.

  i). *What are the IP address of the BIG-IP system that is sending traffic?*
  Specify all IP addresses used by the BIG-IP system that will be sending traffic to this BIG-IP system. Click the Add button to include additional addresses.

b. *Is the other BIG-IP system replacing the Web Interface servers?*
Because you specified traffic is coming from another BIG-IP system, the iApp needs to know if you configured the other system to replace the Web Interface servers.

- **No, the other BIG-IP system is NOT replacing Web Interface servers**
  Select this option if you did not configure (or do not plan to configure) the other BIG-IP system to replace Citrix Web Interface servers. Continue with #4.

- **Yes, the other BIG-IP system is replacing Web Interface servers**
  Select this option if you configured (or plan to configure) the other BIG-IP system to replace Citrix Web Interface servers. Continue with *Web Interface servers on page 16.*

4. ***Is incoming Web Interface traffic encrypted (HTTPS) or unencrypted (HTTP)?***
*This question only appears if you chose not to proxy ICA traffic and authenticate users with the BIG-IP system.*

Specify whether incoming Web Interface traffic is encrypted or unencrypted.

- **Web Interface traffic is encrypted (HTTPS)**
  Select this option if traffic coming into this BIG-IP system is using HTTPS. We recommend using encryption to prevent transporting user credentials in cleartext.

- **Web Interface traffic is unencrypted (HTTP)**
  Select this option if traffic coming to this BIG-IP system is using HTTP. We recommend using encryption to prevent transporting user credentials in cleartext.
  The most common use case for this option is if you are using a separate BIG-IP APM device to handle the initial connection, and then send traffic from that system to this BIG-IP system using HTTP.

5. ***What IP address will clients use to access the Web Interface servers or the F5 Webtop?***
Specify the IP address the system should use for the BIG-IP virtual server. Remote and local clients resolve to this IP address to enter this Citrix environment via the BIG-IP system. The IP address you specify is used for either the BIG-IP Dynamic Presentation Webtop (if using BIG-IP APM) or the Citrix Web Interface virtual server.

6. ***Did you deploy Citrix StoreFront?***
*This question appears if you chose not to proxy ICA traffic and authenticate users with the BIG-IP system, or if you chose to proxy ICA traffic and authenticate users, but chose not to replace the Web Interface servers.*

Select The BIG-IP system supports Citrix StoreFront software, version 1.0, 1.1, 1.2, 2.0, and 2.1.

- **Yes, my Citrix environment uses StoreFront 1.0, 1.1, or 1.2**
  Select this option if you have replaced the standard Web Interface servers with StoreFront version 1.0, 1.1, or 1.2.

  a. *What is the custom URI on StoreFront for XenApp or XenDesktop?*
  Specify the URI you created on the StoreFront servers for XenApp or XenDesktop.

- **Yes, my Citrix environment uses StoreFront 2.0 or 2.1**
  Select this option if you have replaced the standard Web Interface servers with StoreFront version 2.0 or 2.1.

a. *What is the custom URI on StoreFront for XenApp or XenDesktop?*
Specify the URI you created on the StoreFront servers for XenApp or XenDesktop.

- **No, my Citrix environment does not use StoreFront**
Select this option if you are not using StoreFront, and are using standard Web Interface servers.

a. *Are you deploying Citrix XenApp or XenDesktop?*
Specify whether you deploying this iApp template for Citrix XenApp, XenDesktop, or both.

- **Deploying XenApp**
Select this option if you are deploying the iApp template for XenApp only.

i). *Does the Web Interface use a default or custom URI?*
Specify whether your Web Interface deployment uses the default URI or a custom URI for XenApp. Use the default URI if you have not modified websites created during XenApp or XenDesktop Web Interface server installations, or have created additional XenApp or XenDesktop websites after the initial installation of the Citrix Web Interface servers.

- **The Web Interface uses a default URI**
Select this option if the Web Interface uses the default URI. The default URI for XenApp is **/Citrix/XenApp/**.
- **The Web Interface uses a custom URI**
Select this option if you configured a custom URI for the XenApp Web Interface servers.

1). *What is the custom URI you configured?*
Specify the custom URI you configured for XenApp.

- **Deploying XenDesktop**
Select this option if you are deploying the iApp template for XenDesktop only.

i). *Does the Web Interface use a default or custom URI?*
Specify whether your Web Interface deployment uses the default URI or a custom URI for XenDesktop.

- **The Web Interface uses a default URI**
Select this option if the Web Interface uses the default URI. The default URI for XenDesktop is **/Citrix/XenDesktopweb/**.
- **The Web Interface uses a custom URI**
Select this option if you configured a custom URI for the XenDesktop Web Interface servers.

1). *What is the custom URI you configured?*
*Specify the custom URI you configured for XenDesktop.*

- **Deploying both XenApp and XenDesktop**
Select this option if you are deploying this iApp template for both XenApp and XenDesktop. If using both applications, you can create a separate instance of the iApp for each application, or use one URI for both applications.

i). *What is the custom URI on StoreFront for XenApp or XenDesktop?*
Specify the custom URI you configured on the Web Interface server to use for both XenApp and XenDesktop.

7. ***Which port do you want to use for this HTTP virtual server?***
***Which port do you want to use for this HTTPS virtual server?*** Advanced
*One of these questions appears only if you chose not to proxy ICA traffic and authenticate users with the BIG-IP system. This question uses HTTP or HTTPS, depending on how you answered the incoming traffic question.*

Specify the port you want to use for the BIG-IP virtual server, depending on whether your clients will use HTTP or HTTPS. The text box displays default port for HTTP (80) or HTTPS (443); change the port if necessary.

If you are using HTTP, continue with #13 on page 15.

8. ***Which certificate do you want to use for authentication?***
*This question appears unless you specified incoming Web Interface traffic is unencrypted.*

Select the SSL certificate you imported onto the BIG-IP system for client-side SSL processing for the Citrix implementation.

If you have not yet imported a trusted certificate, you must import one before it appears in the list. You can either: complete the template using the default certificate and key, import the trusted certificate and key, and then use the Reconfigure option to re-enter the template, and select them from the list; or exit the template to import the certificate and key, and then start the configuration over from the beginning.

> ⚠ ***Warning***
>
> *The default certificate and key on the BIG-IP system is not secure and should never be used in production environments. The trusted certificate must be valid for all fully qualified domain names used to access the application. For more information on importing certificates and keys, see the BIG-IP documentation.*

9. ***Which key do you want to use for encryption?***
   *This question appears unless you specified incoming Web Interface traffic is unencrypted.*

   Select the key associated with the certificate you imported.

10. ***Do you need to use an intermediate certificate?***
    *This question appears unless you specified incoming Web Interface traffic is unencrypted.*

    Select whether you need to use an intermediate certificate.

    Intermediate certificates or intermediate certificate chains are used to help systems which depend on SSL certificates for peer identification. The chain certificate is 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. See *http://support.f5.com/kb/en-us/solutions/public/13000/300/sol13302.html* for help on creating an intermediate certificate chain.

    The intermediate certificate must already be present on the BIG-IP system to select it from the list. See #8 for information about importing certificates.

    - **No, I do not need to use an intermediate certificate**
      If you choose to use an intermediate certificate, the certificate question appears. Select the appropriate certificate from the list.
    - **Yes, I need to use an intermediate certificate**
      Select this option if you need to use an intermediate certificate.

      a. *Which intermediate do you want to use?*
         Select the appropriate intermediate certificate from the list.

11. ***Do you want to redirect inbound HTTP traffic to HTTPS?*** **Advanced**
    *This question appears depending on your answers to previous questions.*

    Select whether you want the BIG-IP system to redirect users who attempt to access this virtual server using HTTP to HTTPS. We recommend selecting to redirect users as it enables a more seamless user experience.

    - **No, do not redirect users to HTTPS**
      Select this option if you do not want the BIG-IP system to automatically redirect users to HTTPS.
    - **Yes, redirect users to HTTPS**
      Select this option if you want the BIG-IP system to automatically redirect users to HTTPS.

      a. *From which port should HTTP traffic be redirected?*
         Specify the HTTP port (typically port 80), from which you want the traffic redirected to HTTPS.

12. ***Do you want to re-encrypt Web Interface traffic?***
    *This question appears unless you specified incoming Web Interface traffic is unencrypted or you selected to replace the Web Interface servers.*

    Specify if you want the BIG-IP system to re-encrypt the Web Interface traffic after processing it (SSL bridging) or leave the traffic unencrypted (SSL offload).

- **No, do not re-encrypt the Web Interface traffic**
  Select this option for the BIG-IP system to not re-encrypt traffic to the Web Interface servers (SSL offload).
- **Yes, re-recrypt the Web Interface traffic**
  Select this option for the BIG-IP system to re-encrypt traffic to the Web Interface servers (SSL bridging).

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

- **Same subnet for BIG-IP virtual servers and Web Interface servers**
  If the BIG-IP virtual servers and Web Interface 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 Web Interface server?*
  Select whether you expect more or fewer than 64,000 concurrent connections to each Web Interface 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 Web Interface 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.
  - **More than 64,000 concurrent connections**
    Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

    i). *Which IP addresses do you want to use for the SNAT pool?*
    Specify one otherwise unused IP address for every 64,000 concurrent connections, or fraction thereof. Click **Add** for additional rows.

    > ***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 Web Interface server is reached, new requests fail.*

- **Different subnet for BIG-IP virtual servers and Web Interface servers**
  If the BIG-IP virtual servers and Web Interface servers are on different subnets, the following question appears asking how routing is configured.

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

  - **Web Interface servers do NOT use BIG-IP as the default gateway**
    If the Web Interface servers do not use the BIG-IP system as their default gateway, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

    i). *How many connections to you expect to each Web Interface server?*
    Select whether you expect more or fewer than 64,000 concurrent connections to each Web Interface 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 Web Interface 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.

- **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 every 64,000 connections you expect.

  1). *Which IP addresses do you want to use for the SNAT pool?*
  Specify one otherwise unused IP address for every 64,000 concurrent connections, or fraction thereof. Click **Add** for additional rows.

▸ **Web Interface servers use BIG-IP as the default gateway**
If the Web Interface servers use the BIG-IP system as their default gateway, the concurrent user question does not appear.

14. ***How do you want to optimize network connections?*** Advanced
Select how you want the BIG-IP system to optimize network connections. This setting is used to determine the type optimizations the BIG-IP system uses in the TCP profile.

▸ **Use F5's recommended optimizations for WAN clients**
Select this option if most clients are connecting to the Citrix environment over the WAN. The system applies F5's recommended WAN-optimized TCP profile.

▸ **Use F5's recommended optimizations for LAN clients**
Select this option if most clients are connecting to the Citrix environment over the LAN. The system applies F5's recommended LAN-optimized TCP profile.

▸ **Select an existing network optimization profile**
Select this option if you created a custom TCP profile and want to attach it to the Web Interface virtual server.

a. *Which network optimization profile do you want to use?*
Select the TCP profile you created from the list.

15. ***Do you want to add any iRules to the Web Interface virtual server?*** Advanced
Select if have preexisting iRules you want to add to this implementation. While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.
For more information on iRules, see *https://devcentral.f5.com/HotTopics/iRules/tabid/1082202/Default.aspx.*

> ***Important***
>
> *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 want to add iRules, from the **Options** box, select the iRule(s) you want to include, and then click the Add (**<<**) button.

## Web Interface servers

In this section, you add the Web Interface servers and configure the load balancing pool. Even if you chose to replace the Web Interface servers with the BIG-IP system, the first question still appears.

1. ***What DNS name will clients use to reach the Citrix Web Interface servers?***
Specify the public DNS name for the Citrix Web Interface servers. This is the name that resolves (or will resolve) to the BIG-IP virtual server address you specified for the Web Interface servers in the previous section.

If you selected to use APM or Edge Gateway to proxy ICA traffic and authenticate users and to replace the Web Interface servers with the BIG-IP system, this section ends here; continue with *Virtual Server for XML Broker Servers on page 18.*

2. ***What is the IP address of the Web Interface virtual server on the BIG-IP system to which you are sending traffic?***
*This question only appears if you chose to send Citrix traffic to a separate BIG-IP system, and chose not to replace Web Interface servers.*

   Specify the BIG-IP virtual server IP address for the Web Interface servers on the remote BIG-IP system. If you are not using a remote BIG-IP system, this can be the IP address of a single Web Interface server.

   a. *Which port does the Web Interface virtual server use on that system?* **Advanced**
   Specify the port for the encrypted or unencrypted traffic. The default is 80 for HTTP and 443 for HTTPS.

   Continue with *Virtual Server for XML Broker Servers on page 18.*

3. ***Do you want to create a new pool or use an existing one?***
Select whether you want the system to create a new pool for the Web Interface servers, or if you have already created a Web Interface pool on this BIG-IP system.

   - **Use an existing pool**
   Select this option if you have already configured a pool for the Web Interface servers. If you want to create a pool, but have not already done so, you can either exit the template now and then restart the configuration after creating the pool, or complete and save the template with a new pool, and then re-enter the template after creating the pool, and select it from the list.

      a. *Which pool do you want to use?*
      Select the pool you previously created for the Web Interface servers.
      Continue with *Virtual Server for XML Broker Servers on page 18.*

   - **Create a new pool**
   Select this option for the system to create a new pool for the Web Interface servers. The following questions appear, depending on which configuration mode you selected.

      a. *Which TCP port have you configured for Web Interface HTTP traffic?*
      Which TCP port have you configured for Web Interface HTTPS traffic?
      This question uses HTTP or HTTPS, depending on how you answered previous questions.

      Specify the TCP port you configured for Web Interface traffic. The default is 80 for HTTP and 443 for HTTPS.

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

      c. *Use a Slow Ramp time for newly added servers?* **Advanced**
      Select 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 Xen 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 Citrix), 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.

            i). *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 enable Priority Group Activation?* **Advanced**
      Select whether you want to use Priority Group Activation.
      Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP

system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP then sends traffic to the group of servers with the next highest priority, and so on. See the BIG-IP documentation for more details.

- **Do not use Priority Group Activation**
  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 Web Interface server in the Priority box described in #4.

  *i). What is the minimum number of active members for each priority group?*
  Specify a minimum number of available members in a priority group before sending traffic to the next group.

4. ***What are the IP addresses of your Web Interface servers?***
   Specify the IP Address and Port for each Web Interface server. 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 in the pool.

   You should use the default port of 80 for the Web Interface servers, unless you have changed them in the Citrix configuration.

5. ***Do you want to create a new health monitor or use an existing one?***
   Select whether you want the system to create a new health monitor for the Web Interface servers, or if you have already created a Web Interface health monitor on this BIG-IP system.

   - **Use an existing health monitor**
     Select this option if you have already configured a health monitor for the Web Interface servers. If you want to create a monitor, but have not already done so, you can either exit the template now and then restart the configuration after creating the monitor, or complete and save the template with a new monitor and then re-enter the template after creating the monitor, and select it from the list.

     *a. Which monitor do you want to use?*
     Select the health monitor you previously created for the Web Interface servers.

   - **Create a new health monitor**
     Select this option for the system to create a new health monitor for the Web Interface servers. This monitor queries Citrix Web Interface servers for the specific domain name service name and URL that you provided previously in the template. The server member is only considered healthy if it responds properly.

     *a. How many seconds should pass between health checks?*
     Specify how often the system checks the health of the servers. We recommend the default of 30 seconds.

## Virtual Server for XML Broker Servers

The next section of the template asks questions about the BIG-IP virtual server for the Citrix XML Broker devices.
*This section does not appear if you chose to proxy ICA traffic and authenticate users with the BIG-IP system and to replace the Citrix Web Interface servers.*

1. ***How many unique XML Broker farms are you using?*** Advanced
   *This question only appears if you chose Advanced, to replace the Web Interface servers with the BIG-IP system, and to proxy ICA traffic and authenticate users with the BIG-IP system.*

   Select how many distinct XML Broker farms are a part of your Citrix implementation. The iApp supports up to five XML Broker farms.

2. ***What IP address do you want to use for the XML Broker virtual server?***
   Specify the BIG-IP virtual server IP address for the XML Broker devices. This must be an IP address your Web Interface servers can access. Use this address as the Web Interface server *server farm* address.

   a. *What IP address do you want to use for the second XML Broker farm virtual server?*
   *What IP address do you want to use for the third XML Broker farm virtual server?*

*What IP address do you want to use for the fourth XML Broker farm virtual server?*
*What IP address do you want to use for the fifth XML Broker farm virtual server?* **Advanced**
If you selected two or more XML Broker server farms in #1, specify a unique IP address for the virtual server for each of the farms you specified. You can use private internal IP addresses known to only this system if both client and XML Broker traffic is handled on this BIG-IP system.

3. ***Will the XML Broker traffic arrive encrypted unencrypted?***
Select whether the traffic will arrive to the BIG-IP virtual server encrypted or unencrypted. Using encryption is recommended when transporting user credentials in cleartext.

- **XML Broker traffic is encrypted (HTTPS)**
Select this option if you want the BIG-IP system to accept encrypted XML Broker server traffic.

  a. *Which port do you want to use for this HTTPS virtual server?*
  Specify the port for this XML Broker virtual server. The default port is 443 for encrypted XML Broker server traffic (HTTPS). You must use same port you configured for your Citrix Web Interface server farm.

  b. *Which certificate do you want the BIG-IP XML Broker virtual server to use for authentication?*
  Select the certificate you imported for the XML Broker servers from the list.

  If you have not yet imported a certificate, you can leave the default selections and reconfigure this iApp after obtaining the certificates. The deployment will not function correctly until you have selected the correct certificates here.

  c. *Which key do you want this BIG-IP system to use for encryption?*
  Select the associated key from the list.

- **XML Broker traffic is unencrypted (HTTP)**
Select this option if you want the BIG-IP system to accept unencrypted XML Broker server traffic.

  a. *Which port do you want to use for this HTTP virtual server?*
  Specify the port for this XML Broker virtual server should use. The default port is 8080 for older Citrix implementations sending unencrypted XML Broker server traffic (HTTP), and port 80 for newer implementations. This must be the same port you configured for your Citrix Web Interface server farm.

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

- **Same subnet for BIG-IP virtual servers and the XML Broker servers**
If the BIG-IP virtual servers and XML Broker 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 XML Broker server?*
  Select whether you expect more or fewer than 64,000 concurrent connections to each XML Broker 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 XML Broker 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.

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

    i). *Which IP addresses do you want to use for the SNAT pool?*
    Specify one otherwise unused IP address for every 64,000 concurrent connections, or fraction thereof. Click **Add** for additional rows.

**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 XML Broker server is reached, new requests fail.*

- **Different subnet for BIG-IP virtual servers and XML Broker servers**
  If the BIG-IP virtual servers and XML Broker servers are on different subnets, the following question appears asking how routing is configured.

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

  - **XML Broker servers do NOT use BIG-IP as the default gateway**
    If the XML Broker servers do not use the BIG-IP system as their default gateway, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

    i). *How many connections to you expect to each XML Broker server?*
    Select whether you expect more or fewer than 64,000 concurrent connections to each XML Broker 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 XML Broker 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.
    - **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.

      1). *Which IP addresses do you want to use for the SNAT pool?*
      *Specify one otherwise unused IP address for every 64,000 concurrent connections, or fraction thereof. Click* **Add** *for additional rows.*

  - **XML Broker servers use BIG-IP as the default gateway**
    Select this option if thhe XML Broker servers use the BIG-IP system as their default gateway. If they do, the concurrent user question does not appear.

5. ***Which VLANs should accept XML Broker traffic?*** Advanced
   Select whether you want the BIG-IP system to accept XML Broker traffic on all VLANs, or if you want to choose to accept or deny traffic on specific VLANs.

   - **XML Broker traffic is allowed from all VLANs**
     Select this option if you do not want to restrict XML Broker traffic from specific VLANs.
   - **XML Broker traffic is allowed from only specific VLANs**
     Select this option if you want this virtual server to only accept traffic from the VLANs you specify.

     a. *Which VLANs should be allowed?*
     From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move them to the **Selected** box.

   - **XML Broker traffic is allowed from all VLANs**
     Select this option if you want this virtual server to deny traffic from the VLANs you specify.

a. *Which VLANs should be denied?*
From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move them to the **Selected** box.

6. ***Do you want to add any iRules to the XML Broker virtual server?*** **Advanced**
Select if have preexisting iRules you want to add to this implementation. While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.
For more information on iRules, see *https://devcentral.f5.com/HotTopics/iRules/tabid/1082202/Default.aspx.*

> ***Important***
>
> *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 want to add iRules, from the **Options** box, select the iRule(s) you want to include, and then click the Add (**<<**) button.

## XML Broker Servers

In this section, you add the XML Broker servers and configure the load balancing pool.

1. ***Are your XML Brokers and Web Interface servers using the same server farm?***
*This question does not appear if you chose to replace the Web Interface servers.*

Specify whether your XML Brokers are using the same server farm as your Web Interface servers.

- **Yes, use the same pool for both services**
Select this option if you are using the same server farm for both the Web Interface servers and the XML Broker servers. In this case, the BIG-IP system uses the same IP addresses you entered for the Web Interface servers for the XML Broker pool.
Continue with *ICA Traffic on page 24.*
- **No, create a new pool for the XML Broker servers**
Select this option if you are using a separate server farm for the XML Broker servers, and want the iApp to create a new pool for the XML Broker devices.
Continue with #4.
- **No, select an existing pool of XML Broker servers**
Select this option if you have already created a pool of XML Broker servers.

  If you choose an existing pool, be aware that the iApp cannot attach a new health monitor to a pool created outside the template, so you are not able to use the sophisticated health monitor that this iApp is able to create for the XML Broker servers.

  a. *Which pool of XML Broker servers do you want to use?*
  Select the pool of XML Broker servers you previously created on this BIG-IP system.

  Continue with the next section.

2. ***What is the IP address of the BIG-IP system where you are sending XML Broker server requests?***
*This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system, to send Citrix traffic to a separate BIG-IP system, and to replace Web Interface servers.*

Specify the BIG-IP virtual server IP address for the XML Broker on the remote BIG-IP system. If you are not using a remote BIG-IP system, this can be the IP address of a single XML Broker server.

b. *Does the XML Broker traffic need to be encrypted or unencrypted to the BIG-IP system to which you will be forwarding traffic?*

Specify whether the XML Broker traffic you are sending to the remote BIG-IP system should be encrypted or unencrypted.

c. *Which port do you want to use?*
Specify the port for the encrypted or unencrypted traffic.

Continue with *Finished on page 26.*

3. ***Do you want to create a new XML Broker pool?***
*This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system and to replace Web Interface servers.*

- **Select an existing pool of XML Broker servers**
Select this option if you have already created a pool of XML Broker servers.

  If you choose an existing pool, be aware that the iApp cannot attach a new health monitor to a pool created outside the template, so you are not able to use the sophisticated health monitor that this iApp is able to create for the XML Broker servers.

  a. *Which pool of XML Broker servers do you want to use?*
  Select the pool of XML Broker servers you previously created on this BIG-IP system.

  Continue with *Finished on page 26.*

- **Create a new pool for the XML Broker servers**
Select this option if you want the iApp to create a new pool for the XML Broker devices.

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

5. ***Use a Slow Ramp time for newly added servers?*** **Advanced**
Select 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 Xen 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 Citrix), 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.

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

- **Do not use Priority Group Activation**
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 Web Interface server in the Priority box described in #4.

a. *What is the minimum number of active members in a 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.

7. ***What are the IP addresses of your XML Broker servers?***
Specify the IP Address for each XML Broker server. If you are using Advanced mode, you must also specify a port (see the following note). 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 in the pool.

*You should use the default port of 80 for the XML Broker servers unless you have changed them in the Citrix configuration. If you have upgraded from a previous Citrix version, your XML Broker servers may be using port 8080.*

8. ***Do you want to create a new health monitor or use an existing one?***
Select whether you want the system to create a new health monitor for the XML Broker servers, or if you have already created a XML Broker health monitor on this BIG-IP system.

- **Use an existing health monitor**
Select this option if you have already configured a health monitor for the XML Broker servers. If you want to create a monitor, but have not already done so, you can either exit the template now and then restart the configuration after creating the monitor, or complete and save the template with a new monitor and then re-enter the template after creating the monitor, and select it from the list.

  a. *Which monitor do you want to use?*
  Select the health monitor you previously created for the XML Broker servers.

- **Create a new health monitor**
Select this option for the system to create a new health monitor for the XML Broker servers. The health monitor created by the template is one of the most powerful features of this deployment. The health monitors check the nodes (IP address and port they are listening on) by logging in to the Citrix servers with appropriate credentials and attempting to retrieve a specific application. If the check succeeds, the LTM marks the node UP and forwards the traffic. If not, it marks it down so no new requests are sent to that device.

  ***Warning***

  *You must enter the following information very carefully. The template creates a complex monitor Send String that automatically calculates values such as Content Length. It is very difficult to manually change the monitor after the template has created it.*

  a. *How many seconds should pass between health checks?*
  Specify how often the system checks the health of the servers. We recommend the default of 30 seconds.

  b. *What user name should the monitor use?*
  Type the user name for a Citrix account to use in the health monitor.

  ***Note***

  *We recommend you create a Xen user account specifically for use in this monitor. This user could be restricted to only the application specified in the monitor. This Citrix service account should be set to never expire. A deleted or locked account will cause the BIG-IP system to mark the servers down.*

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

  *These credentials are stored in plain text on your BIG-IP system.*

  d. *What published application should the BIG-IP system expect in the monitor response?*

Specify the name of an application the monitor attempts to retrieve. If you leave the published application field blank, the monitor marks the server UP if any response is received from the server.

***Warning***

*The published application name is case sensitive and must exactly match the resource you have configured on your Xen servers. It is important to use a published resource that will always be available since all XML Broker members will be marked down if chosen published application is removed or becomes unavailable.*

## ICA Traffic

In this section, you have the option of configuring the BIG-IP system for ICA traffic.

*This section does not appear if you chose to proxy ICA traffic and authenticate users with the BIG-IP system.*

1. ***How will traffic travel between the clients and the ICA servers?***
   Select how ICA traffic will travel between the clients and the ICA servers.

   - **ICA traffic does not pass through this BIG-IP system**
     Select this option if your ICA traffic does not pass through the BIG-IP system. The Citrix clients must have a route to the Citrix ICA servers.
   - **The BIG-IP system acts as a gateway (router) to the ICA server network**
     Select this option if you plan on routing ICA traffic through the BIG-IP system. At least one self IP address for this BIG-IP system must be on a VLAN that you configure to permit the ICA traffic, and your routing infrastructure must be configured to use that BIG-IP self IP address as the gateway to the ICA server subnet.

     a. *Which TCP port does your ICA traffic use?*
     Select which TCP port your ICA traffic uses. Select 2598 if all Citrix clients support session reliability, otherwise select 1494. Clients fall back to 1494 when session reliability (2598) is unavailable.

     b. *What ports are assigned to Multi-Stream ICA? (not required)*
     Multi-Stream ICA uses multiple TCP connections to carry the ICA traffic between the client and the server. If you are using Multi-Stream ICA and require Multi-Stream ICA support on the BIG-IP system, you can (but are not required to) enter up to three additional TCP ports. These ports are defined as CGP port1, CGP port2, and CGP port3 within each Xen server computer and user policy. The BIG-IP system creates additional virtual servers on the ports you specify.

     Type the port number in the box. Click Add to include additional ports, up to three additional ports.

     c. *What is the Network address of your ICA server subnet?*
     Specify the network address space on which the Citrix application servers reside. The BIG-IP system forwards the requests to the specified network. If the Citrix application server network is not directly connected to this BIG-IP system, then a route to the next hop must be provided in this BIG-IP system's routing table. To add a route, on the Main tab, expand **Network** and then click **Routes**. Click the **Create** button and enter the appropriate information. For more information, see the BIG-IP documentation.

     d. *What is the netmask for your ICA server subnet?*
     Specify the associated subnet mask.

     e. *Which VLANs should accept ICA traffic?*
     Select whether you want the BIG-IP system to accept ICA traffic on all VLANs, or if you want to choose to accept or deny traffic on specific VLANs.

     - **ICA traffic is allowed from all VLANs**
       Select this option if you do not want to restrict ICA traffic from specific VLANs.
     - **ICA traffic is allowed from only specific VLANs**
       Select this option if you want this virtual server to only accept traffic from the VLANs you specify.

       i). *Which VLANs should be allowed?*
       From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move

them to the **Selected** box.

- **ICA traffic is allowed from all VLANs**
  Select this option if you want this virtual server to deny traffic from the VLANs you specify.

  *i). Which VLANs should be denied?*
  From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move them to the **Selected** box.

  Continue with #2.

- **The BIG-IP system replicates ICA IP addresses using Route Domains**
  Select this option if you want the BIG-IP system to use route domains to replicate ICA IP addresses. BIG-IP route domains provide the capability to segment network traffic and define separate routing paths for different network objects and applications.

  Using BIG-IP route domains, you can keep your ICA Application Servers in secure, internal networks but still give them routable IP addresses. This BIG-IP system replicates each of the IP addresses of your ICA servers as virtual servers in a public-facing route domain, so traffic that the clients initiate will pass through this BIG-IP system.

  ***Important***

  *You must have at least two existing Route Domains on the BIG-IP system to select this option. Configuring Route Domains is not a part of the iApp template. To configure Route Domains, expand Network and then click Route Domains. Click the Create button. If you do not have existing Route Domains and want to use this feature, you must either restart or reconfigure the template after creating new Route Domains. For more information on configuring Route Domains, see the BIG-IP system documentation..*

  a. *Which TCP port does your ICA traffic use?*
  Select which TCP port your ICA traffic uses. Select 2598 if all Citrix clients support session reliability, otherwise select 1494. Clients fall back to 1494 when session reliability (2598) is unavailable.

  b. *Do you need to support Multi-Stream ICA?*
  Select whether you need the BIG-IP system to support Citrix Multi-Stream ICA. Multi-Stream ICA uses multiple TCP connections to carry the ICA traffic between the client and the server.

  - **No, only a single stream is required**
    Select this option if you are not using Multi-Stream ICA, or do not require Multi-Stream ICA support on the BIG-IP system.
  - **Yes, support Multi-Stream ICA**
    Select this option if you are using Multi-Stream ICA and require Multi-Stream ICA support on the BIG-IP system. You can (but are not required to) enter up to three additional TCP ports. These ports are defined as CGP port1, CGP port2, and CGP port3 within each Xen server computer and user policy.
    The BIG-IP system creates additional virtual servers on the ports you specify.

    *i). What is the first TCP port you configured for Multi-Stream ICA?*
    Specify one of the ports you configured for Multi-Stream ICA on the Citrix Xen servers.

    *ii). What is the first TCP port you configured for Multi-Stream ICA?*
    Specify one of the ports you configured for Multi-Stream ICA on the Citrix Xen servers.

    *iii). What is the first TCP port you configured for Multi-Stream ICA?*
    Specify one of the ports you configured for Multi-Stream ICA on the Citrix Xen servers.

  c. *What are the IP addresses of your ICA application servers?*
  Specify the IP addresses of each of your ICA application servers. Click the Add button to include additional servers.

  d. *What is your public-facing route domain?*
  Select the public-facing route domain you configured.

  e. *What is the route domain of your ICA application servers?*

Select the existing route domain for the ICA application servers from the list. This must be a different route domain than you selected in the previous question.

2. ***Do you want to add any iRules to the virtual server for ICA traffic?*** Advanced
   Select if have preexisting iRules you want to add for ICA traffic. While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.
   For more information on iRules, see *https://devcentral.f5.com/HotTopics/iRules/tabid/1082202/Default.aspx.*

   ***Important***

   *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 want to add iRules, from the **Options** box, select the iRule(s) you want to include, and then click the Add (**<<**) button.

### Finished

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

## Modifying the Citrix configuration

This section contains modifications to the Citrix configuration that you may have to make depending on the way you configured the BIG-IP system.

### Modifying the Citrix Web Interface configuration

The next task is to make important modifications to the Citrix servers running v6.5. *This section is not necessary if you chose Dynamic Webtops to replace the Web Interface servers*.

#### Modifying the Web Interface servers to point at the BIG-IP virtual server

You must modify the Web Interface server configuration so the Web Interface devices send traffic to the BIG-IP XML Broker virtual server and not directly to the XML Brokers. You must also make sure "Use the server list for load balancing" is unchecked, as shown below.

**To modify the Web Interface servers to point at the XML Broker virtual server**

1. From a Web Interface server, open the Access Management Console.
2. In the Navigation pane, select XenApp Web Sites, and then the site name.
3. Right-click your site name, and then select **Server Farms**.
4. From the list, select the appropriate farm, and then click **Edit**.
5. In the **Server** box, select each entry and then click the **Remove** button.
6. Click the **Add** button.
7. Type the IP address of the XML Broker virtual server.
8. Clear the check from the **Use the server list for load balancing** box.
9. Click the **OK** button. Repeat this procedure for any/all additional Web Interface servers.

### Configuring Citrix to retrieve the correct client IP address

Citrix XenApp needs to be configured to look for the client IP address in the **X-Forwarded-For** HTTP header. Otherwise, every connection will appear to be coming from the BIG-IP LTM and not from its actual location. This can only be done by editing Java files.

**To reconfigure the Citrix to Read X-Forwarded-For headers for the Client IP address**

1. Open the file **\Inetpub\wwwroot\Citrix\XenApp\app_code\PagesJava\com\citrix\wi\pageutils\Include.java** on the Web Interface server, and find the function named **getClientAddress**. In version 5.x, it looks like the following:

```
public static String getClientAddress(WIContext wiContext) {
     String ageClientAddress = AGEUtilities.getAGEClientIPAddress(wiContext);
     return (ageClientAddress != null
          ? ageClientAddress
          : wiContext.getWebAbstraction().getUserHostAddress());
}
```

2. Edit this function so it looks like the following:

```
public static String getClientAddress(WIContext wiContext) {
     String ageClientAddress = AGEUtilities.getAGEClientIPAddress(wiContext);
     String userIPAddress = wiContext.getWebAbstraction().getRequestHeader("X-FORWARDED-FOR");
          if (userIPAddress == null) {
               userIPAddress = wiContext.getWebAbstraction().getUserHostAddress();
          }
     return (ageClientAddress != null ? ageClientAddress : userIPAddress);
}
```

3. Repeat this change for each Web Interface server. Make sure to **restart** each Web Interface server for the changes to take effect.

## Modifying the Citrix StoreFront configuration if using BIG-IP APM

If you configured the BIG-IP system for Citrix StoreFront, and are using BIG-IP APM, you must add the following **hosts** file entry on each StoreFront server. For specific instructions to how to add to the hosts file, see the appropriate documentation.

Use the following syntax to add the hosts file entries on each StoreFront server:

```
127.0.0.1   citrix fqdn
::1         citrix fqdn
```

Where **citrix fqdn** equals the FQDN used for your Citrix environment. If you have modified your IIS server to use a specific address rather than the default (**all unassigned**), you need to use a specific address rather than a loop back address.

The default directory installation for your windows hosts file is located in the following directory: **%systemroot\system32\drivers\etc**.

## Next steps

After completing the Application Template, the BIG-IP system presents a list of all the configuration objects created to support XenApp or XenDesktop. 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 XenApp implementation to point to the BIG-IP system's Web Interface 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 disabled, 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 Citrix 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 view statistics for BIG-IP configuration objects by using the following procedure.

**To view object-level statics**

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

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

## Troubleshooting

This section contains troubleshooting steps in case you are having issues with the configuration produced by the template.

- **Users can't connect to the Web Interface servers**
  Make sure users are trying to connect using the BIG-IP virtual server address (or a FQDN that resolves to the virtual server address).

- **Users can connect to the Web Interface servers, but there are connectivity problems to and from the XML Broker servers.**
  This type of problem is usually a routing issue. If you chose *XML Broker servers use the BIG-IP as default gateway* when asked how you have configured routing on your XML Broker servers, you must manually configure the proper routes on the XML Broker farm servers.

  If you mistakenly answered that the XML Brokers use the BIG-IP system as their default gateway, you can re-run the template, leaving the route question at No (the default).
  Alternatively, you can open each virtual server created by the template, and then from the **SNAT Pool** list, select **Auto Map**.

- **Users initially see an IIS page or a page other than the Citrix log on page**
  This is typically a web server configuration issue. Make sure the proper Citrix URI is the default web site on your web server. Consult your web server documentation for more information.

  This may also be the case if all of your Web Interface servers are being marked DOWN as a result of the BIG-IP LTM health check. Check to make sure that at least one node is available. You can also use the procedure in the following section to temporarily disable the monitor itself.

- **Citrix XML Broker servers are being incorrectly marked DOWN by the BIG-IP LTM**
  If your XML Broker servers are being incorrectly marked down, you may have made an error in the template when answering the health monitor questions. The health monitor is very precise, calculating the Content Length header based on your responses in the template.

  One common error is that the domain for the specified user account was entered as a fully qualified domain name (FQDN). It should just be the NetBIOS name. For example, CITRIX, not citrix.example.com.

  If you need to check the health monitor configuration, the safest and easiest way is to re-enter the iApp template to make any necessary changes.

  To verify or make changes to the health monitor, use the procedure *Modifying the iApp configuration on page 28* to re-enter the iApp template.

- **You are unable to launch your application and you receive "SSL Error 61"**
  SSL errors are usually due to mismatched or untrusted security certificates. Review your certificates and verify they match the domain name used to login to your Citrix environment. Example – if *citrix.example.com/Citrix/XenApp/* is used to resolve to your Citrix environment then your trusted certificate must be issued to *citrix.example.com*.

- **Application icons are not appearing when using F5 dynamic Webtops**
  This is usually due to communication problems between the BIG-IP system and your XML Brokers. Verify at least one pool member is in an active state.
  Dynamic compression is disabled by default and must remain disabled in IIS on your XML Brokers. Verify this setting is disabled by opening **IIS Manager**, clicking the affected server, and double-clicking "Compression". Uncheck the "Enable dynamic content compression" box. Save your changes.

- **Troubleshooting Web Interface Kerberos authentication issues**

  a. *Review the service principal names –*
     Mismatched/mistyped service principal names account for nearly 99% of Kerberos-related errors. Review the service principal names used in the Kerberos SSO AD user service account, APM Kerberos SSO profile, and the service name of the Web Interface resources (which should be the HTTP service of the hostname (ex. http/wi1.homelab.com).

b. *Review the APM access policy reports and logs.*
The reports can be accessed via the management UI and the logs can be accessed from the management shell at /var/log/apm (tail –f /var/log/apm displays log and any new updates). To make the logs more verbose, in the management UI go to System, Logs, then click on Configuration and then Options. Toward the bottom of this page, find the "Access Policy" and "SSO" options and set them to debug3.
**Remember to turn off debug logging when it's no longer required.

c. *Add a Citrix Web Interface server to the Local Intranet sites list of another machine in the domain and attempt to access it from this machine which removes BIG-IP from the equation.*
If the Web Interface is accessible without having to type in credentials, then the Web Interface and IIS configurations are correct. Verify, for this test, browsers user authentication is set to Automatic logon with current user name and password.

d. *Open the /etc/krb5.conf file in the management shell: vi /etc/krb5.conf or SCP program.*
There is a possibility that the access policy configuration will not change the default values in this file. If the default_realm value equals EXAMPLE.COM, change it to the actual Active Directory domain name4. Remove any section that contains configuration information for EXAMPLE.COM and ensure that the dns_lookup_kdc option is also equals true. Close the file by hitting the escape key and issuing the following command:
**:wq**

**Type the "i" character to enter VI edit/insert mode. Type the escape character to exit this mode, and type the following to exit without saving changes: !q

e. *Ensure that time is synchronized between the BIG-IP and Active Directory.*
Aside from setting the BIG-IP's NTP settings to a time server in the domain, here is a simple way to quickly synchronize the BIG-IP's clock from the management shell:

**/etc/init.d/ntpd stop**
**ntpdate <IP address of a domain controller>**
**/etc/init.d/ntpd start**

f. *Ensure that the BIG-IP can resolve (forward and reverse) all of the Web Interface resources from Active Directory DNS*
To test, from the BIG-IP management shell, issue forward and reverse DNS lookups to objects in the domain.

g. *Install Wireshark*
Install Wireshark on a domain machine (preferably on the domain controller if on a switched network) and observe Kerberos traffic between the BIG-IP system, domain controller, and Web Interface resources. Kerberos issues will usually manifest as ERROR messages.

➤ **Troubleshooting Smartcard authentication to the Web Interface virtual server and remote desktop/application issues**

a. Review and verify that the client certificate is issued by one of the certificates in the bundle file, that all of the certificates are valid (not expired), and that the bundle file contains every issuing certificate in the path from the end entity to self-signed root.

b. Verify that the issuer of the client certificates, and every certificate in the path to and including the self-signed root certificate, is in the domain's NTAuth store.

c. Verify that the above certificates are propagating to the other machines in the domain via the group policy.

d. Verify that the domain controller has a certificate issued to it from the local CA.

➤ **Troubleshooting general smart card authenication issues**

a. Review the configuration and make sure the environment settings match those in this guide.

b. Review ltm logs to verify iRule used to extract user principle name from user's certificate is not generating errors. If errors are noted review iRule to make sure it was entered correctly.

**tail –f /var/log/ltm**

c. In the event that none of the above resolves the issue, please contact support.

## Configuring the BIG-IP system for Citrix using BIG-IP APM and Route Domains

If you want to use route domains in your implementation along with BIG-IP APM, you must use the following guidance to configure the BIG-IP system. A ***route domain*** is a configuration object that isolates network traffic for a particular application on the network, allowing you to assign the same IP address or subnet to multiple nodes on a network, provided that each instance of the IP address resides in a separate routing domain. For more specific information on route domains, see the BIG-IP system documentation.

**To configure the BIG-IP system for APM and route domains**

1. Create a new partition on the BIG-IP system (click **System** > **Users** > **Partition List** > **Create**).
2. Create a new route domain and make it default for your new partition (click **Network** > **Route Domains** > **Create**).
3. Switch to your new partition (the partition list is in the upper right corner of the Configuration utility) and create a new VLAN, Self IP, and Route (if applicable) in the new partition.
4. While still in the partition you created, run the iApp template as applicable for your configuration.
5. After submitting the iApp configuration, you must modify the configuration produced by the iApp using the following guidance:
    a. Disable the Strict Updates feature (click **iApp** > **Application Services** > [*name you gave this iApp*] > **Properties** (on the Menu bar) > uncheck Strict Updates (if necessary).
    b. Click the Remote Desktop object created by the iApp (click **Access Policy** > **Application Access** > **Remote Desktops** > [*name you gave this iApp*]***_apm_remote_desktop_1***"
    c. Modify the Remote Desktop object to use the XML broker pool created by the iApp template (in the Destination row, click the **Pool** button and then, from the list select appropriate XML pool created by the iApp. This is either: [*name you gave this iApp*]***_xml_http_pool*** or [*name you gave this iApp*]***_xml_https_pool***.
    d. In the **Caption** field, type an appropriate caption.
    e. Click **Update**.

To check the proper route domain is assigned, from the **Partition** list, select **All [Read Only]**, and then click either Virtual Servers or Pools. You can see a %<route_domain#> next to your pool member and virtual server IP addresses.

# Appendix A: Citrix server changes required to support smart card authentication

This appendix provides guidance for configuring Citrix Web Interface servers, Active Directory Kerberos servers, Citrix XML Broker and application servers, client desktops, and the BIG-IP system in support of Citrix XenApp and XenDesktop smartcard access with two smartcard PIN prompts. Some assumptions are made throughout concerning the initial Citrix, Microsoft Windows, and F5 BIG-IP system configurations and installations. This section deals specifically with the requirements to support smartcard access when using the BIG-IP system to securely proxy ICA connections and manage single sign on smart card Kerberos authentication.

***Warning***

*This information is posted as guidance only. For specific instructions on configuring Citrix or Active Directory devices, consult the appropriate documentation. F5 cannot provide support for these products.*

## Base software requirements

The following base requirements are assumed for this configuration.

- Microsoft Windows 2008 R2
- Citrix XenApp 6.5 and XenDesktop 5.6
- BIG-IP system 11.2.0 with LTM and APM provisioned modules
- Smartcard cryptographic service provider (CSP) software

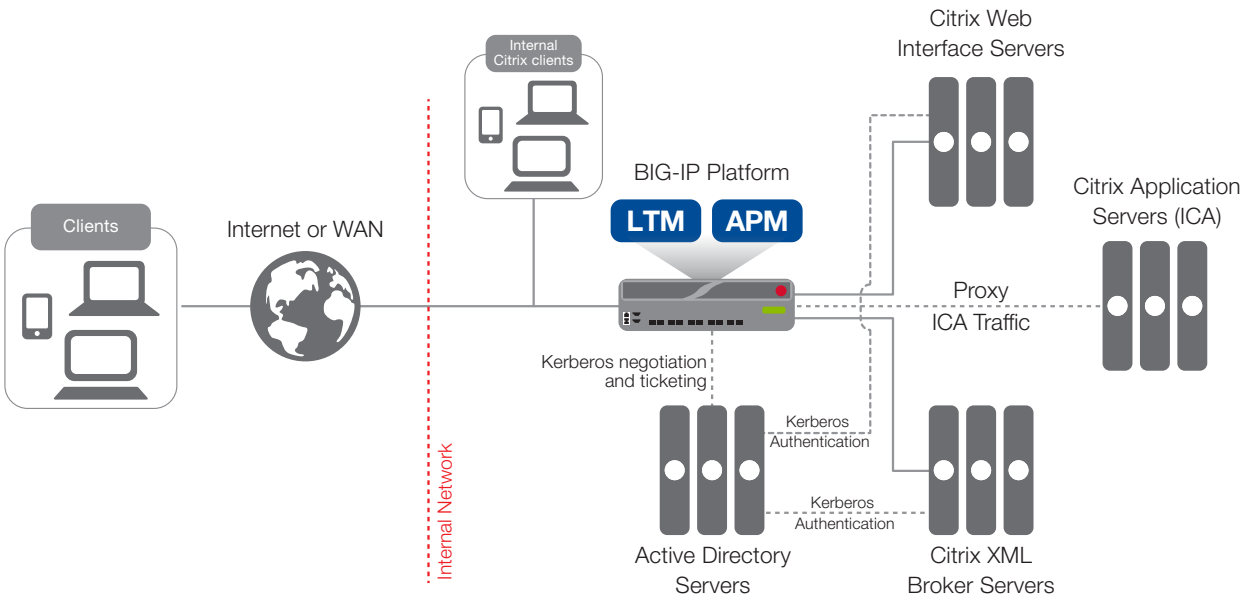
## Process and traffic flow

Citrix typically facilitates single sign-on with user name/password authentication by passing the user's encoded credentials through the Citrix client to the Citrix application server, via the ICA configuration file, where a specialized Graphical Identification and Authentication (GINA) process decodes the data and passes it to Windows GINA for logon.

Smart cards have to use an alternate method, because there is not a password credential to send to the Citrix GINA to use for authentication. The Windows environment needs specific configuration changes to support smartcard logon directly. The user authenticates to the Web Interface via smartcard, and then authenticates separately via smartcard to the Windows server hosting the Citrix applications or desktops. Because these are separate authentications, the user is prompted for their smartcard PIN twice.

The authentication process using smart cards is as follows:

1. The client makes a normal browser call to the Citrix Web Interface which is load balanced by the BIG-IP system. The BIG-IP APM module generates a client certificate request, validates the certificate, and then stores the certificate information in the access session.
2. BIG-IP APM performs Kerberos authentication to the Web Interface server to authenticate the user and get a list of published applications.
3. When the user clicks on an application or desktop icon, APM rewrites a portion of the ICA file pointing the application or desktop to the same physical VIP.
4. The user is presented with a (second) smartcard authentication prompt to authenticate to the chosen application or desktop.



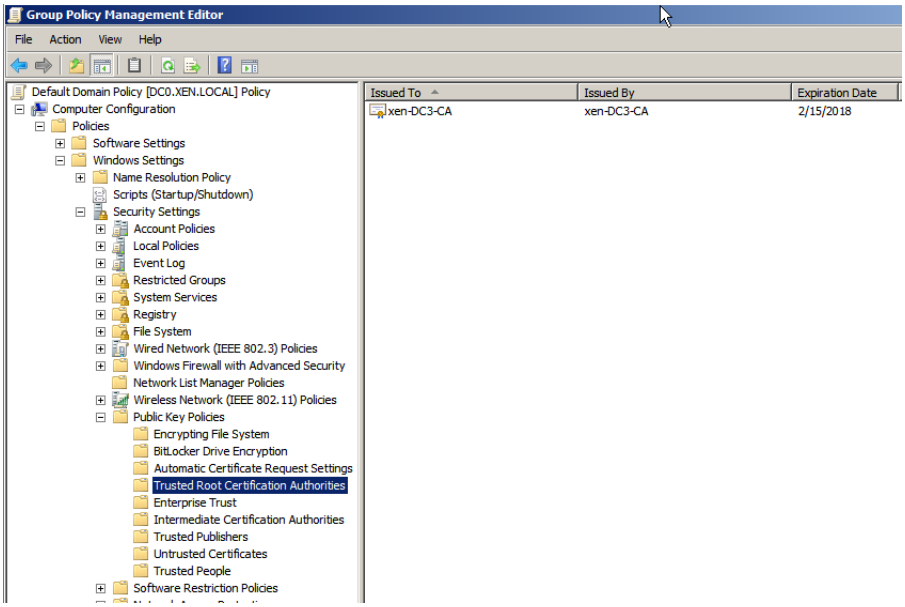

## Windows domain Configuration

This+ section describes the steps necessary to configure the Windows domain for smart card access and allow APM to perform Kerberos authentication to the Citrix Web Interface servers.

1. Add the Certificate Services role on the domain controller.
    a. Open Windows 2008 Server Manager, and then select **Roles**.
    b. Check the **Active Directory Certificate Services** option.
    c. Proceed through the installation with default settings.
2. Ensure that the domain controller has been issued a certificate. The installation of certificate services automatically generates this certificate, but we strongly recommend verifying the certificate, just in case something went wrong during installation.
    a. Open a Command prompt and type **mmc** to open Microsoft Management Console.
    b. From the **File** menu, select **Add/Remove** Snap-in.
    c. Highlight **Certificates**, and the select **Add**.
    d. Chose Computer account, and then click Next.
    e. Click **Finish**, and then click **Ok**.
    Local certificates are located under Certificates | Personal | Certificates. You should see a certificate issued by your new certificate authority to the local domain controller.
    f. Verify each domain controller has been issued a certificate from your new CA. If the certificate is missing, you can request a new certificate from the domain controller(s) missing a certificate by right-clicking **Certificates** | **All Tasks** | **Request New Certificate**.
    g. Click **Next**, and then highlight **Active Directory Enrollment Policy**.
    h. Click **Next**, select **Domain Controller**, and then click **Enroll**.
3. Export third-party root CA certificates in *Base64-encoded X.509* format. This document assumes the use of third-party CA-issued certificates and does not specifically cover creating and issuing smartcard certificates.

    If using locally-issued certificates, this and the next two steps are not required.

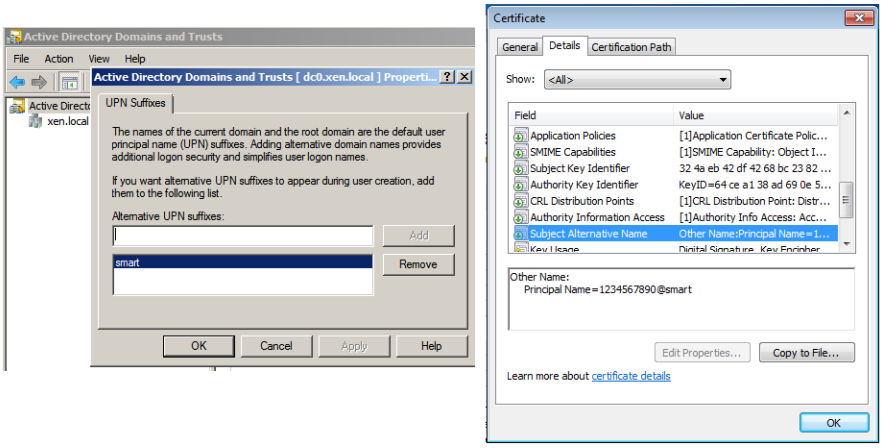
4. Add the third-party root CA certificate to the Trusted Root Certification Authorities using an Active Directory Group Policy object.
    a. On the domain controller, open the Group Policy Management console and edit the default domain policy.
    b. Import the root CA certificate to the **Trusted Root Certification Authorities** folder as shown in the following screenshot.




5. Add the third-party subordinate CA certificates to the Intermediate Certification Authorities in the domain using an Active Directory Group Policy object.
    a. On the domain controller, open the Group Policy Management console and edit the default domain policy.
    b. Import any subordinate issuer CA certificates to the **Intermediate Certification Authorities** folder (as seen just below Trusted Root Certification Authorities in the previous screenshot.

6. Add the third-party root CA certificates to the NTAuth store on the domain controller. You can do this from the MMC console (easier method) or the command line.
    - *MMC console*
      Open a MMC console, add the **Enterprise PKI** snap-in, right click the **Enterprise PKI** object, and select **Manage AD Containers**.
    - *Command line*
      From the command line issue the following command:
      **`certutil.exe -dspublish <filename> NTAuthCA`**

7. As required, create an alternate UPN suffix in the domain to match the UPN realm suffix on the smartcard.
    a. From a domain controller, open **Active Directory Domains and Trusts**.
    b. Right click the top-most object in the tree and select **Properties**.
    This shows a UPN suffix box as illustrated in the following screenshot.
    c. Add the alternate UPN suffix that is on the smartcard. Look for the Subject Alternative Name – User Principal Name object in the certificate.




8. Install the smart card cryptographic services provider (CSP) software used to generate the users certificate onto: Citrix client computer, Citrix application servers, and Citrix virtual desktop agent.

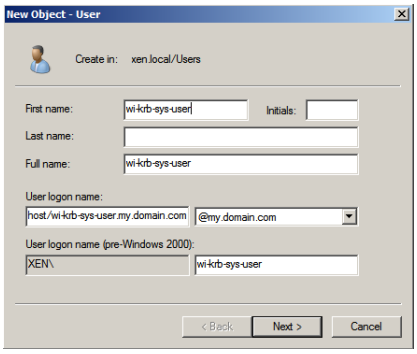
   *This is a critical step for smartcard authentication to work with Windows servers.*

9. Verify that Active Directory DNS is configured with *forward* and *reverse* DNS records.

## Configuring the Active Directory SSO service account

This account is used by APM Kerberos SSO profile to enable Kerberos Protocol Transition and Constrained Delegation to the Web Interface resources.

1. Create an Active Directory user account. The name you choose is not important, but the user logon name must be in the form of an arbitrary server principal name, such as:
   **host/wi-krb-sys-user.my.domain.com.**



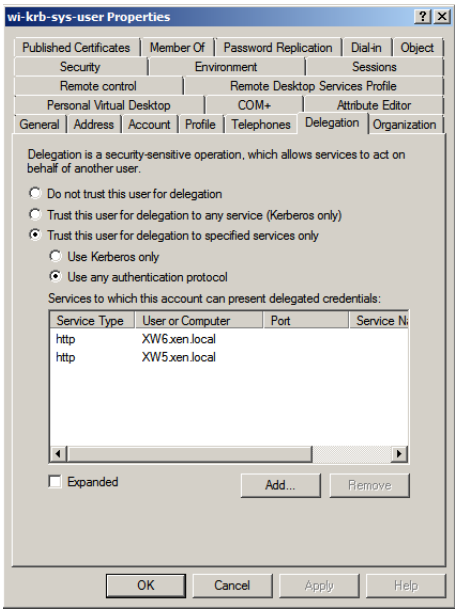

2. Set the account's **servicePrincipalName** attribute to the same user logon name value. You can either open **ADSIEDIT.msc**, or right-click a folder in AD Users and Computers, select **View**, and then select **Advanced Features**. Navigate to the previously created account, go to the *Attribute Editor* tab, find the **servicePrincipalName** entry, and then add the service principal name value that was used for the user logon name.

3. Close and re-open the user object to configure delegation.
   When you re-open the user object, there is a Delegation tab.

   a. Click the Delegation tab.

   b. Click the **Trust this user for delegation to specified services only** option, and then click the **Use any authentication protocol** option.

c. Click the **Add** button and type the name of a Web Interface server host, and then select its HTTP service only. Do this for every Web Interface server.




## Citrix configuration

This section details the steps required to configure the Citrix XML broker and Web Interface servers.

### Configuring the XML Broker

- If configuring XenApp, create a new computer policy in the Citrix AppCenter to enable XML trust.
- If configuring XenDesktop, use the following PowerShell commands to enable XML trust:

```
Add-PSSnapin Citrix.* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

### Configuring the Web Interface

The following section details the configuration of Web Interface and Microsoft IIS. If re-encrypting the traffic from the BIG-IP to the Web Interface, complete all of the steps. If not re-encrypting, the first three steps can be skipped.

1. Install a server certificate on the Web Interface IIS host. The following example assumes a web server certificate has already been issued and exported from the domain controller running Certificate services.
   a. In the IIS Manager application on the Web interface host, click the host name in the left pane, and then click the Server Certificates button in the center.
   b. Click the Import link on the far right.
   c. Select the .pfx file and associated password.
2. In IIS, create an HTTPS binding:
   a. Click the Default Web Site.
   b. Select the Bindings link on the far right.

c. Add an HTTPS binding and then, from the **SSL certificate** list, select the certificate that you imported previously.

3. Enable SSL for the Default Web Site:
   a. Click the **SSL Settings** button.
   b. Check the **Require SSL** box.
   c. In the Client certificates section, click the **Ignore** button.
4. In the Citrix Web Interface Management utility, create a new HTTPS site.
   a. On the Specify Point of Authentication page, select **At Web Interface**.
   b. After setting the XML broker information, on the Configure Authentication Methods page, check the Pass-through box.
5. Enable Kerberos authentication:
   a. After the site is created, select it from the list.
   b. Click the Authentication Methods link on the right of the application.
   c. Verify that **Pass-through** is the only option checked, and then click the **Properties** button.
   d. Under Kerberos Authentication, check the **Use Kerberos authentication to connect to servers** button.

# Appendix B: Manual configuration table

While we recommend using the iApp template for configuring the BIG-IP system for Citrix applications, users familiar with the BIG-IP system can use the following table to manually configure the BIG-IP device. This table contains all non-default settings used in our configuration.

## BIG-IP APM configuration table

The table on this page contains configuration objects for BIG-IP APM. If you are not using BIG-IP APM in your deployment, continue with *BIG-IP LTM Configuration table on page 43*

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **DNS and NTP settings** | See *Configuring additional BIG-IP settings on page 54 for instructions.* | |
| **Health Monitor** (*Main tab-->Local Traffic -->Monitors*) | ***Configuration*** | Select **Advanced** from the Configuration list (if necessary). |
| | ***Name*** | Type a unique name, such as AD_LDAP_monitor. |
| | ***Type*** | **LDAP** |
| | ***Interval*** | **10** (recommended) |
| | ***Timeout*** | **31** (recommended) |
| | ***User Name*** | Type a user name with administrative permissions |
| | ***Password*** | Type the associated password |
| | ***Base*** | Specify your LDAP base tree. For example, CN=Citrix Users,DC=my,DC=domain,DC=com |
| | ***Filter*** | Specify the filter. We type **cn=user1**, using the example above: user1 in OU group "Citrix Users" and domain "my.domain.com" |
| | ***Security*** | Select a Security option (either None, SSL, or TLS) |
| | ***Chase Referrals*** | **Yes** |
| | ***Alias Address*** | ***All Addresses** |
| | ***Alias Address Port*** | **389** (for None or TLS) or **686** (for SSL) |
| **AAA Servers** (*Access Policy-->AAA Servers*) | ***Active Directory AAA Server*** | |
| | ***Name*** | Type a unique name. We use **citrix-domain** |
| | ***Type*** | **Active Directory** |
| | ***Domain Name*** | Type the FQDN of the Windows Domain name |
| | ***Server Connection*** | Click **Use Pool** if necessary. |
| | ***Domain Controller Pool Name*** | Type a unique name |
| | ***Domain Controllers*** | **IP Address**: Type the IP address of the first domain controller<br>**Hostname**: Type the FQDN of the domain controller<br>Click **Add**. Repeat for each domain controller in this configuration. |
| | ***Server Pool Monitor*** | Select the monitor you created above. |
| | ***Admin Name***[1] | Type the Administrator name |
| | ***Admin Password***[1] | Type the associated password |
| | ***Optional: SecurID AAA Server for two factor authentication*** | |
| | ***Name*** | Type a unique name. We use **citrix-rsa** |
| | ***Type*** | **SecurID** |
| | ***Agent Host IP Address*** | Click **Select from Self IP LIst**. Select the self IP address that you have configured on your RSA Authentication server as an Authentication Agent. |
| | ***SecurID Configuration File*** | Click **Choose File** and then browse to your SecurID Configuration file. This is the file you generated and downloaded from your RSA Authentication server. |
| **SSO Configurations** (*Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar)*) | ***XenApp SSO Configuration* (If you are using Web Interface Servers only)** | |
| | ***SSO Configurations By Type*** | **Forms-Client Initiated** |
| | ***SSO Configuration Name*** | Type a unique name. We use **XenApp-SSOv2** |
| | ***Forms in this SSO Configuration*** (v11.2)<br>***Form Settings*** *in left pane* (v11.3, 11.4) | Click **Create**. The New Forms Definition page opens. |
| | ***Form Name*** | Type a unique name. We use **XenApp-Form** |

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

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **SSO Configurations**<br>(*Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar)*)<br><br>Important:<br>Only create a SSO Configuration if you are using Web Interface servers.<br><br>If you are replacing the Web Interface servers with F5 Dynamic Webtops, do **NOT** create the SSO Configuration. | ***Form Parameters*** | Click **Create** (v11.2) or click **Form Parameters** in the left pane, and then **Create** (11.3, 11.4) The New Form Parameter page opens. |
| | | **Form Parameter Type**[1] Select **Username** from the list.<br>**Username Parameter Name** **user**<br>**Username Parameter Value** **%{session.sso.token.last.username}**<br>Click **Ok**, and then click **Create** again in the Forms Parameters box.<br>**Parameter Type**[1] Select **Password** from the list.<br>**Password Parameter Name** **password**<br>**Password Parameter Value** **%{session.sso.token.last.password}**<br>Click **Ok**, and then click **Create** again in the Forms Parameters box.<br>**Parameter Type**[1] Select **Custom** from the list<br>**Form Parameter Name** **domain**<br>**Form Parameter Value** **{domain-name-in-NetBIOS-format}**[3]<br>Click **Ok**. |
| | ***Form Detection*** | In the left pane of the New Form Definition box, click **Form Detection**. |
| | ***Detect Form by*** | **URI** |
| | ***Request URI*** | **/Citrix/XenApp/auth/login.aspx**[2] (do NOT click OK). |
| | ***Form Identification*** | In the left pane of the New Form Definition box, click **Form Identification**. |
| | ***Identify Form by*** | **Action Attribute** |
| | ***Form Action*** | **login.aspx** |
| | ***Successful Logon Detection*** | In the left page of the New Form Definition box, click **Successful Logon Detection**. |
| | ***Detect Logon by*** | **Redirect URI** |
| | ***Request URI*** | **/Citrix/XenApp/site/default.aspx**[2] Click **Ok** twice to complete the SSO Configuration. |
| | ***XenDesktop SSO Configuration* (If you are using Web Interface Servers only)** | |
| | ***SSO Configurations By Type*** | **Forms-Client Initiated** |
| | ***SSO Configuration Name*** | Type a unique name. We use **XenDesktop-SSOv2** |
| | ***Forms in this SSO Configuration*** (v11.2)<br>***Form Settings*** *in left pane* (v11.3, 11.4) | Click **Create**. The New Forms Definition page opens. |
| | ***Form Name*** | Type a unique name. We use **XenDesktop-Form** |
| | ***Form Parameters*** | Click **Create** (v11.2) or click **Form Parameters** in the left pane, and then **Create** (11.3, 11.4) The New Form Parameter page opens. |
| | | **Parameter Type**[1] Select **Username** from the list.<br>**Username Parameter Name** **user**<br>**Username Parameter Value** **%{session.sso.token.last.username}**<br>Click **Ok**, and then click **Create** again in the Forms Parameters box.<br>**Parameter Type** Select **Password** from the list.<br>**Password Parameter Name** **password**<br>**Password Parameter Value** **%{session.sso.token.last.password}**<br>Click **Ok**, and then click **Create** again in the Forms Parameters box.<br>**Parameter Type**[1] Select **Custom** from the list.<br>**Form Parameter Name** **domain**<br>**Form Parameter Value** **{domain-name-in-NetBIOS-format}**[3]<br>Click **Ok**. |
| | ***Form Detection*** | In the left page of the New Form Definition box, click **Form Detection**. |
| | ***Detect Form by*** | **URI** |

[1] 11.2 only. There are minor differences in the SSO Configuration wizard between versions.
[2] By default, XenApp Web Interface URLs begin with /Citrix/XenApp/. If your Web Interface named differently, (i.e. DesktopWeb) you have to adjust these URLs
[3] domain-name is the Active Directory domain name for the users being authenticated. This must be in NetBIOS format. In our example, **domain LABDOMAIN**)
[4] You may need to adjust these URLs to match your configuration

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **SSO Configurations** (*Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar)*)<br><br>Important:<br>Only create a SSO Configuration if you are using Web Interface servers. | ***Request URI*** | **/Citrix/XenDesktop/auth/login.aspx**[1] (do NOT click OK). |
| | ***Form Identification*** | In the left pane of the New Form Definition box, click **Form Identification**. |
| | ***Identify Form by*** | **Action Attribute** |
| | ***Form Action*** | **login.aspx** |
| | ***Successful Logon Detection*** | In the left page of the New Form Definition box, click **Successful Logon Detection**. |
| | ***Detect Logon by*** | **Redirect URI** |
| | ***Request URI*** | **/Citrix/XenDesktop/site/default.aspx**[1] Click **Ok** twice. |
| | ***StoreFront SSO Configuration* (If you are using Web Interface Servers only)** | |
| | ***Name*** | Type a unique name. We use **XenDesktop-SSO**. |
| | ***SSO Method*** | **Forms** |
| | ***Use SSO Template*** | **None** |
| | ***Start URI*** | <URI of StoreFront website>**/authentication/Login*** |
| | ***Pass Through*** | **Enable** |
| | ***Form Method*** | **POST** |
| | ***Form Action*** | <URI of StoreFront website>**/authentication/LoginAttempt** |
| | ***Form Parameter for User Name*** | **username** |
| | ***Form Parameter for Password*** | **password** |
| | ***Hidden Form Parameters/Values*** | **domain <**domain-name-in-NetBIOS-format**>**[2]<br>**LoginBtn Log+On**<br>**StateContext** |
| | ***Successful Logon Detection Match Type*** | **By Presence of Specific Cookie** |
| | ***Successful Logon Detection Match Value*** | **CtxsAuthId** |
| | ***Smart Card SSO Configuration* (If you are using Web Interface Servers with smart cards only)** | |
| | ***Name*** | Type a unique name. We use **smart-card-SSO**. |
| | ***SSO Method*** | **Kerberos** |
| | ***Kerberos Realm*** | <Citrix Kerberos Realm in all caps> |
| | ***Account Name*** | Type the user name in SPN format |
| | ***Account Password*** | Type the associated password |
| | ***Confirm Account Password*** | Confirm the password |
| **Citrix Client Bundles** (*Access Policy--> Application Access--> Remote Desktops--> Citrix Client Bundles*) | ***Name*** | Type a unique name |
| | ***Download URL*** | Modify the Download URL if necessary |
| **Connectivity Profile** (*Access Policy-->Secure Connectivity*) | ***Name*** | Type a unique name |
| | ***Parent Profile*** | **connectivity** |
| | **Important:** *After creating the Connectivity profile, open it again, and then from the Menu bar, click* **Client Configuration**. *From the* **Citrix Client Bundle** *list, select the Citrix Client Bundle you just created.* | |
| **Remote Desktop** (*Access Policy-->Application Access-->Remote Desktops*) | ***Name*** | Specify a unique name. We use **citrix-domain** |
| | ***Type*** | **Citrix** |
| | ***Destination*** | Type the IP address or Host Name of the destination |
| | ***Port*** | Type the appropriate port (typically 80 or 443) |
| | ***Server Side SSL*** | If you require SSL to the servers, check the Enable box |
| | ***ACL Order*** | Select the next unused number |
| | ***Auto Logon*** | Check the Enable box (leave the Username, Password, and Domain Source at their defaults) |
| | ***Caption*** | Type a descriptive caption |
| **Webtop** (*Access Policy-->Webtops*) | ***Name*** | Type a unique name |
| | ***Type*** | **Full** |

[1] By default, XenDesktop Web Interface URLs begin with /Citrix/XenDesktop/. If your Web Interface named differently, (i.e. DesktopWeb) you have to adjust these URLs

[2] domain-name is the Active Directory domain name for the users being authenticated. This must be in NetBIOS format. In our example, **domain LABDOMAIN**)

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **iRule Data Group** (*Local Traffic-->iRules--> Data Group List*) | ***Data Group for use with the Dynamic Webtop*** | |
| | ***Name*** | **APM_Citrix_PNAgentProtocol** **This must be the name of the Data Group** |
| | ***Type*** | **String** |
| | ***String*** | **<URL clients use to access the Citrix environment>** |
| | ***Value*** | **1** |
| | ***Data Group for use with a non-standard URI or if you are using WebInterface servers or StoreFront servers*** | |
| | ***Name*** | **APM_Citrix_ConfigXML** **This must be the name of the Data Group** |
| | ***Type*** | **String** |
| | ***String*** | **<URL being used to access the site>** For example: **citrix.domain.com** |
| | ***Value*** | **<URI being used to access the site>** For example: **/citrix/storefrontweb** |
| **Access Profile** (*Access Policy-->Access Profiles*) | ***Name*** | Type a unique name |
| | ***SSO Configuration*** | **If you are using Web Interface Servers only (and not replacing them with F5 Dynamic Webtops)**, select the SSO Configuration you created above |
| **Access Policy** (*Access Profiles*) | ***Edit*** | Edit the Access Profile you created using the VPE. See *Editing the Access Profile with the Visual Policy Editor on page 47* for instructions. |
| **iRules** (*Local Traffic-->Rules*) | ***iRule if using Web Interface servers and BIG-IP APM*** *(only necessary if you are using Web Interface servers and the BIG-IP APM)* | |
| | ***Name*** | Type a unique name |
| | ***Definition*** | `when ACCESS_ACL_ALLOWED {`<br>`  if {[HTTP::uri] contains "loggedout" } {`<br>`  after 2000  { ACCESS::session remove}`<br>`  }`<br>`}` |
| | ***iRule if using Smart card authentication where the UPN domain is same as the Citrix domain*** *)* | |
| | ***Name*** | Type a unique name |
| | ***Definition*** | `when HTTP_RESPONSE_DATA priority 501 {`<br>`  if { [string tolower [HTTP::header Content-Type]] contains "application/x-ica" } {`<br>`  set payload [ regsub -nocase -line {^SSLEnable=On.*\n} [HTTP::payload] "SSLEnable=On\r\`<br>`nDisableCtrlAltDel=Off\r\n" ]`<br>`  HTTP::payload replace 0 [HTTP::header Content-Length] $payload`<br>`  }`<br>`}`<br>`when ACCESS_POLICY_AGENT_EVENT {`<br>`  switch [ACCESS::policy agent_id] {`<br>`  "CERTPROC" {`<br>`  if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {`<br>`  ACCESS::session data set session.logon.last.username [lindex [split [findstr [ACCESS::session`<br>`data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 0]`<br>`  ACCESS::session data set session.logon.last.domain [lindex [split [findstr [ACCESS::session`<br>`data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 1]`<br>`  }`<br>`  }`<br>`  }`<br>`}` |
| | ***iRule if using Smart card authentication where the UPN domain is same as the Citrix domain*** *)* | |
| | ***Name*** | Type a unique name |
| | ***Definition*** | `if { [string tolower [HTTP::header Content-Type]] contains "application/x-ica" } {`<br>`  set payload [ regsub -nocase -line {^SSLEnable=On.*\n} [HTTP::payload] "SSLEnable=On\r\`<br>`nDisableCtrlAltDel=Off\r\n" ]`<br>`  HTTP::payload replace 0 [HTTP::header Content-Length] $payload`<br>`  }`<br>`}`<br>`when ACCESS_ACL_ALLOWED {`<br>`  ACCESS::session data set session.logon.last.username [ACCESS::session data get "session.ad.last.attr.`<br>`sAMAccountName"]`<br>`}`<br>`when ACCESS_POLICY_AGENT_EVENT {`<br>`  switch [ACCESS::policy agent_id] {`<br>`  "CERTPROC" {`<br>`  if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {`<br>`  ACCESS::session data set session.custom.certupn [findstr [ACCESS::session data get session.`<br>`ssl.cert.x509extension] "othername:UPN<" 14 ">"]`<br>`  }`<br>`  }`<br>`  }`<br>`}` |

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **iRules**<br>(*Main tab-->Local Traffic -->Rules*) | ***iRule for logging off APM sessions two seconds after users log off of the Web Interface servers*** | |
| | ***Name*** | Type a unique name |
| | ***Definition*** | `when ACCESS_ACL_ALLOWED {`<br>`  if {[HTTP::uri] contains "loggedout" } {`<br>`  after 2000 { ACCESS::session remove }`<br>`  }`<br>`}` |
| | ***iRule for logging off APM sessions two seconds after users log off of StoreFront*** | |
| | ***Name*** | Type a unique name |
| | ***Definition*** | `when ACCESS_ACL_ALLOWED {`<br>`  if {[HTTP::uri] contains "Logoff" } {`<br>`  after 2000 { ACCESS::session remove }`<br>`  }`<br>`}` |

[1] Used for legacy PNAgent support when using a F5 Webtop

This completes the BIG-IP APM configuration objects. Continue with the LTM configuration objects on the following page.

## BIG-IP LTM Configuration table

*Use a unique name for each BIG-IP object. We recommend names that start with the application name , such as* **xendesktop-wi-pool**

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **Health Monitor** (*Local Traffic-->Monitors*) | ***StoreFront Monitor*** | |
| | ***Name*** | Type a unique name |
| | ***Type*** | **HTTPS** (Use **HTTP** if offloading SSL) |
| | ***Interval*** | **4** (recommended) |
| | ***Timeout*** | **13** (recommended) |
| | ***Send String*** | **GET <uri>/ HTTP/1.1\nHost:<host>\nConnection: Close\r\n\r\n** |
| | ***Receive String*** | **Citrix Receiver** |
| | ***Web Interface Monitor*** | |
| | ***Name*** | Type a unique name |
| | ***Type*** | **HTTPS** (Use **HTTP** if offloading SSL) |
| | ***Interval*** | **4** (recommended) |
| | ***Timeout*** | **13** (recommended) |
| | ***Send String*** | **GET <uri>/ HTTP/1.1\nHost:<host>\nConnection: Close\r\n\r\n** |
| | ***Receive String*** | **Citrix Systems** |
| | ***XML Broker Monitor*** | |
| | See *Health monitor configuration on page 46* for instructions on configuring the health monitors | |
| **Route Domains** (*Network-->Route Domains*) | If you want the BIG-IP system to replicate ICA IP addresses using existing route domains, you must already have route domains configured on the BIG-IP system. Configuring Route Domains is outside the scope of this document. For information, see the online help or BIG-IP documentation, available at *http://support.f5.com/kb/en-us.html* | |
| **Pools** (*Local Traffic-->Pools*) | ***Web Interface Pool*** | |
| | ***Health Monitor*** | Select the Web Interface monitor you created |
| | ***Load Balancing Method*** | Choose your preferred load balancing method |
| | ***Address*** | Type the IP Address of the Web Interface nodes |
| | ***Service Port*** | Type the appropriate port. This can be **80** or **443** depending on if you are using encryption. or a custom port. Repeat Address and Service Port for all nodes |
| | ***XML Broker Pool*** | |
| | ***Health Monitor*** | Select the XenApp monitor you created |
| | ***Load Balancing Method*** | Choose your preferred load balancing method |
| | ***Address*** | Type the IP Address of the XML Broker nodes |
| | ***Service Port*** | Type the appropriate port. This can be **80** or **443** depending on if you are using encryption. or a custom port, such as **8080**. Repeat Address and Service Port for all nodes |
| | ***XML Broker Enumeration Pool*** | |
| | ***Health Monitor*** | Select the built-in **UDP** monitor |
| | ***Load Balancing Method*** | Choose your preferred load balancing method |
| | ***Address*** | Type the IP Address of the XML Broker nodes |
| | ***Service Port*** | **137** (repeat Address and Service Port for all nodes) |
| | ***ICA Pool (when using route domains and routing ICA through the BIG-IP system)*** | |
| | ***Health Monitor*** | Select the built-in **TCP** monitor |
| | ***Load Balancing Method*** | Choose your preferred load balancing method |
| | ***Address*** | Type the address of one ICA node along with route domain ID using the following syntax: **<ipaddress>%<route domain ID>** |
| | ***Service Port*** | **2598** or **1494** depending on your configuration. |
| | ***Important: Create a separate ICA pool for each ICA node using these settings*** | |

| BIG-IP LTM Object | Non-default settings/Notes | | |
|---|---|---|---|
| **Profiles** (*Local Traffic-->Profiles*) | ***HTTP*** | Parent Profile | **http** |
| | | Insert X-Forwarded-For | **Enabled** |
| | | Redirect Rewrite | **Matching** |
| | ***TCP WAN*** | Parent Profile | **tcp-wan-optimized** |
| | | Proxy Buffer Low | **65536** |
| | | Idle Timeout | **1800** |
| | | Send Buffer | **1048576** |
| | | Receive Window | **1048576** |
| | | Keep Alive Interval | **75** |
| | | Selective NACK | **Enable** |
| | | Packet Lost Ignore Rate | **10000** |
| | | Packet Lost Ignore Burst | **8** |
| | | Initial Retransmission Timeout Base Multiplier for SYN Retransmission | **200** |
| | ***TCP LAN*** | Parent Profile | **tcp-lan-optimized** |
| | | Idle Timeout | **1800** |
| | ***Persistence*** | Persistence Type | **Cookie** |
| | ***Persistence*** | Persistence Type | **Source Address Affinity** |
| | ***Stream*** (only if replacing WI servers) | Parent Profile | **stream** |
| | ***Client SSL*** | Parent Profile | **clientssl** |
| | | Certificate and Key | Select the Certificate and Key |
| | | Trusted Certificate Authorities[1] | Select the Certificate |
| | | Advertised Certificate Authorities[1] | Select the Certificate |
| | ***Server SSL*** (only if you require encryption to the servers) | Parent Profile | **serverssl-insecure-compatible** |
| | | Secure Renegotiation | **Require** |
| **Virtual Servers** (*Local Traffic--> Virtual Servers*) | ***Web Interface HTTP virtual server*** | | |
| | ***Address*** | Type the IP Address for the virtual server | |
| | ***Service Port*** | **80** | |
| | ***iRule*** | **_sys_https_redirect** | |
| | ***Web Interface HTTPS virtual server*** | | |
| | ***Address*** | Type the IP Address for the virtual server | |
| | ***Service Port*** | **443** | |
| | ***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 to re-encrypt traffic to the servers, select that Server SSL profile. | |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Auto Map**[2] | |
| | ***Default Pool*** | *If you are **not** replacing the Web Interface servers:*<br>Select the Web Interface pool you created<br>*If you **are** replacing the Web Interface servers with BIG-IP:*<br>Select the XML Broker pool you created | |
| | ***Default Persistence Profile*** | Select the Cookie Persistence profile you created | |
| | ***Fallback Persistence Profile*** | Select the Source Address Persistence profile you created | |
| | *The following are only applicable if you are configuring BIG-IP APM* | | |
| | ***Stream Profile***[3] | Select the Stream Profile you created | |

[1] Only necessary if configuring the BIG-IP system for smart card authentication.
[2] *If 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 manuals for info on SNAT Pools.*
[3] The Stream profile is only necessary if you are replacing the Web Interface servers and using APM.

| BIG-IP LTM Object | Non-default settings/Notes | |
|---|---|---|
| **Virtual Servers** Continued | ***Access Profile*** | Select the Access Profile you created |
| | ***Connectivity Profile*** | Select the Connectivity profile you created |
| | ***Citrix Support*** | Check the box to enable Citrix support |
| | ***XML Broker Virtual Server*** | |
| | ***Address*** | Type the IP Address for the virtual server |
| | ***Service Port*** | **80**, **443** or **8080** depending on your implementation |
| | ***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 |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Automap**[1] |
| | ***Default Pool*** | Select the pool you created for the XML Brokers |
| | ***XML Broker Enumeration Virtual Server*** *(not necessary if using Dynamic Webtops)* | |
| | ***Address*** | Type the IP Address for the virtual server |
| | ***Service Port*** | **137** |
| | ***Protocol*** | Select **UDP** from the list. |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Automap**[1] |
| | ***Port Translation*** | Click the box to clear the check to ***Disable*** Port Translation. |
| | ***Default Pool*** | Select the pool you created for the XML Brokers |
| | ***ICA Forwarding Virtual Server*** *(only use if routing ICA traffic through BIG-IP system, not needed if using APM to proxy ICA traffic)* | |
| | ***Destination*** | *Type*: **Network** *Address:* Type the IP Address for the virtual server *Mask*: Type the associated mask |
| | ***Service Port*** | **2598** or **1494** depending on your implementation |
| | ***Protocol Profile (client)*** | Select the WAN optimized TCP profile you created |
| | ***Protocol Profile (server)*** | Select the LAN optimized TCP profile you created |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Automap** |
| | ***Address Translation*** | Click to clear the check box to **Disable** Address Translation |
| | ***Port Translation*** | Click to clear the check box to **Disable** Port Translation |
| | ***ICA Forwarding Virtual Server using Route Domains*** *(only use if routing ICA traffic through BIG-IP system and using route domains, not needed if using APM to proxy ICA traffic)* | |
| | ***Address*** | Use the following syntax for the address: **<virtual server IP address>%<route domain ID>** You must already have Route Domains configured. Configuring Route Domains is outside the scope of this guide, see the online help or BIG-IP system documentation. |
| | ***Service Port*** | **2598** or **1494** depending on your implementation |
| | ***Protocol Profile (client)*** | Select the WAN optimized TCP profile you created |
| | ***SSL Profile (Server)*** | If you created a Server SSL profile to re-encrypt traffic to the servers, select that Server SSL profile. |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Automap**[1] |
| | ***Default Pool*** | Select the ICA server pool you created |
| | ***ICA Forwarding Virtual Server with Multi Stream*** *(only use if routing ICA traffic through BIG-IP system and your environment is configured to use multi streaming, not needed if using APM to proxy ICA traffic)* | |
| | ***Destination*** | *Type*: **Network** *Address:* Type the IP Address for the virtual server *Mask*: Type the associated mask |
| | ***Service Port*** | Specify the appropriate port. The port number changes depending on your implementation |
| | ***Protocol Profile (client)*** | Select the WAN optimized TCP profile you created |
| | ***Protocol Profile (server)*** | Select the LAN optimized TCP profile you created |
| | ***SNAT Pool*** | As applicable for your configuration. We use **Automap** |
| | ***Address Translation*** | Click to clear the check box to **Disable** Address Translation |
| | ***Port Translation*** | Click to clear the check box to **Disable** Port Translation |

[1] *If 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 manuals for info on SNAT Pools.*

## Health monitor configuration

To ensure traffic is directed only to those servers that are responding to requests, it is important to configure health monitors on the BIG-IP LTM to verify the availability of the servers being load balanced.

For Citrix XenApp and XenDesktop, we create an advanced monitors. The monitor is for the Web Interface servers and attempts to login to the servers by using the user name and account of a test user. We recommend you create a test user that reflects users in your environment for this purpose. If a particular server fails authentication, traffic is diverted from those servers until those devices are fixed. If all authentication is down, users will not be able to connect. We recommend setting up a Fallback Host for these situations. Please see F5 product documentation on setting up Fallback Hosts in your pools

***Note:*** *The monitor uses a user account (user name and password) that can retrieve applications from the Citrix server. Use an existing account for which you know the password, or create an account specifically for use with this monitor. Be sure to assign an application to this user.*

The health monitor is created using a script, available on DevCentral. Use the appropriate link, depending on whether you are using XenApp or XenDesktop:

XenApp:
*https://devcentral.f5.com/wiki/TMSH.BIGIP-V11-Citrix-XenApp-Monitor.ashx*

XenDesktop:
*https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx*

Download the script to a location accessible by the BIG-IP device. Optionally, you can cut and paste the script directly into the TMSH editor on the BIG-IP device. However, cutting and pasting is error-prone and therefore we provide instructions here on how to copy the file to the BIG-IP device using secure-copy (SCP).

To create the Web Interface Monitor using the script, you must first copy the script into the BIG-IP device. The following procedures show you how to copy the file both on a Windows platform using WinSCP, and on Linux, UNIX or MacOS system using SCP.

**To import the script on a Windows platform using WinSCP**

1. Download the script found on the following link to a computer that has access to the BIG-IP device:
   XenApp: *https://devcentral.f5.com/wiki/TMSH.BIGIP-V11-Citrix-XenApp-Monitor.ashx*
   XenDesktop: *https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx*
2. Open a Windows compatible SCP client. We recommend WinSCP. It is available as a free download from *http://winscp.net/*. The login box opens.
3. In the **Host name** box, type the host name or IP address of your BIG-IP system.
4. In the **User name** and **Password** boxes, type the appropriate administrator log on information.
5. Click **Login**. The WinSCP client opens.
6. In the left pane, navigate to the location where you saved the script in step 1.
7. In the right pane, navigate to **/shared/tmp/** (from the right pane drop-down list, select **root**, double-click **shared**, and then double-click **tmp**).
8. In the left pane, select the script and drag it to the right pane.
9. You can now safely close WinSCP.

**To import the script using Linux/Unix/MacOS systems**

1. Download the script:
   XenApp: *https://devcentral.f5.com/wiki/TMSH.BIGIP-V11-Citrix-XenApp-Monitor.ashx*
   XenDesktop: *https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx*

2. Open a terminal session.
3. Use your built in secure copy program from the command line to copy the file. Use the following syntax:

   `scp <source file> <username>@<hostname>:<Destination Directory and filename>`
   In our example, the command is:

   `scp create-citrix-monitor.tcl root@bigip.f5.com:/shared/tmp/create-citrix-monitor`

The next task is to import the script you just copied to create the monitor. The following tasks are performed in the BIG-IP Advanced Shell (see the BIG-IP manual on how to configure users for Advanced shell access).

**To run the monitor creation script**

1. On the BIG-IP system, start a console session.
2. Type a user name and password, and then press Enter.
3. Change to the directory containing the creation script. In our example, we type:

   `cd /shared/tmp/`
   If you copied the script to a different destination, Use the appropriate directory.
4. Change the permissions on the script to allow for execute permission using the following command:

   `chmod 755 create-citrix-monitor`

You have now successfully imported the script. The next step is to run the script and provide the parameters to create the Citrix XenApp monitor for your environment.

**To run the monitor script**

1. At the system prompt, type **tmsh** and then press Enter.
   This opens the Traffic Management shell.
2. Typing **cli script** to enter CLI Script mode. The prompt changes to

   `root@bigip-hostname(Active)(tmos.cli.script)#`
3. From the command prompt, use the following command syntax, where file path is the path to the script:

   `run file <file path>/<filename>`
   In our example, we type

   `run file /shared/tmp/create-citrix-monitor`
   The script starts, you are prompted for four arguments. You are automatically switched to interactive mode.
4. At the **What is the User Name** prompt, type the user name of the XenApp user.
5. At the **What is the Password** prompt, type the associated password.
6. At the **What is the App name** prompt, type the name of an available application for the XenApp user. In our example, we use Notepad.
7. At **What is the domain name** prompt, type the Windows domain used for authentication of users. In our example, we use **corpdomain**. Do not use the fully-qualified-domain-name from DNS here; this is referring to Windows Domain only.

The script creates the monitor. You can view the newly created monitor from the web-based Configuration utility from the Main Tab, by expanding **Local Traffic** and then clicking **Monitors**. The name of the monitors starts with the App name you configured in step 6.

## Editing the Access Profile with the Visual Policy Editor

The next task is to edit the Access Policy you just created using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

For additional or more sophisticated authentication and policy options, see the Configuration Guide for BIG-IP Access Policy Manager, available on Ask F5 (https://support.f5.com/).

The procedure you use depends on whether you are using Web Interface servers, using APM to replace the Web Interface servers, and if you are using smart cards.

### Editing the Access Profile with the Visual Policy Editor when using F5 Dynamic Webtops to replace Web Interface servers

Use this procedure if you are using Dynamic Presentation Webtops to replace the Web Interface servers.

**To edit the Access Profile**

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you created, and then in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click **Add Item**.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
6. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. The options box opens
8. Click the **AD Auth** option button, and then click **Add Item**.
9. From the **Server** list, select the name of the AAA server you created in the table above. In our example, we select **Citrix_domain**.
10. Configure the rest of the Active Directory options as applicable, and then click **Save**.
    You now see two paths, **Successful** and **Fallback**.
11. Click the **+** symbol on the Successful path between **AD Auth** and **Deny**. The options box opens.
12. Click the **Variable Assign** option button and then click **Add Item**.
13. Click **Add new entry**.
14. Click the **Change** link on the new entry.
15. In the **Custom Variable** box, type **session.logon.last.domain**.
16. In the **Custom Expression** box, type **`Add expr { "<domain>" }`** where *<domain>* is your NetBIOS domain name for authenticating Citrix users.
17. Click **Finished**.
18. Click **Save**.
19. Click the **+** symbol between **Variable Assign** and **Deny**. The options box opens.
20. Click the **Full Resource Assign** option button, and then click **Add Item**.
21. Click **Add new entry**.
22. Click the **Add/Delete** link on the new entry.
23. Click **Remote Desktop Resources** tab
24. Check the box for the Remote Desktop top profile you created using the table.
25. Click the **Webtop** tab.
26. Click the option button for the Webtop profile you created using the table.
27. Click **Update**

28. Click the **Save** button.
29. On the fallback path between **Full Resource Assign** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
30. *Optional configuration to support two factor authentication with RSA SecurID.*
    *If you are not using two factor authentication with RSA SecurID, continue with #31.*
    a. Click the **+** symbol between **Logon Page** and **AD Auth**. The options box opens.
    b. Click the **Variable Assign** option button and then click **Add Item**.
    c. In the **Name** box, type **Variable Assign AD**.
    d. Click **Add new entry**, and then click the **change** link under Assignment.
    e. In the **Custom Variable** box, select **Secure**, and then type **session.logon.last.password** in the box.
    f. In the **Custom Expression** box, type
    **expr { [mcget {session.logon.last.password1}] }**.
    g. Click **Finished**.
    h. Click **Save**.
    i. At the start of the VPE, click the **Logon Page** link/box.
    j. In row #2, perform the following:
    - In the **Post Variable Name** box, type **password1**.
    - In the **Session Variable Name** box, type **password1**.
    k. In row #3, perform the following:
    - From the **Type** list, select **password**.
    - In the **Post Variable Name** box, type **password**.
    - In the **Session Variable Name** box, type **password**.
    l. Under Customization, in the **Logon Page Input Field #3** box, type **Passcode**.
    m. Click **Save**.
    n. Click the **+** symbol between **Logon Page** and **Variable Assign AD**.
    o. Click the **RSA SecurID** option button and then click **Add Item**.
    p. From the **AAA Server** list, select the RSA SecurID AAA Server you created using the configuration table.
    q. From the **Change Max Logon Attempts Allowed** list, select **1**.
    r. Click **Save**.
31. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.
32. Click the **Close** button on the upper right to close the VPE.

When you are finished, the Access Policy should look like one of the following examples, depending on whether you configured the optional two factor authentication section.

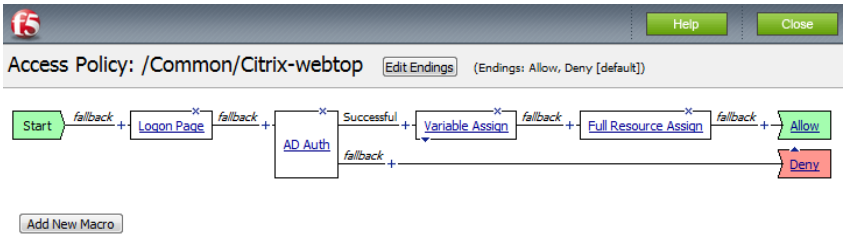



**Figure 5:** *Access Policy without two factor authentication*

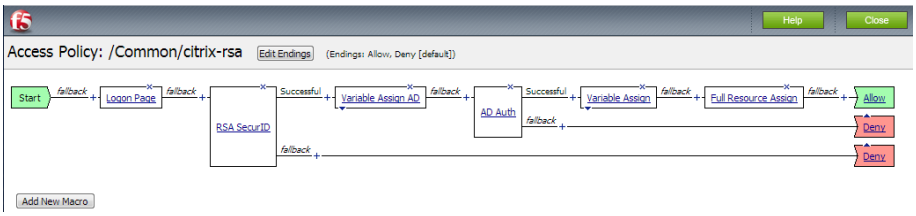



**Figure 6:** *Access Policy including two factor authentication*

### Editing the Access Profile with the Visual Policy Editor when using Web Interface servers

Use this procedure if you are not using Dynamic Presentation Webtops to replace the Web Interface servers.

#### To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you created, and then in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click **Add Item**.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
6. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. The options box opens
8. Click the **AD Auth** option button, and then click **Add Item**.
9. From the **Server** list, select the name of the AAA server you created in the table above. In our example, we select **Citrix_domain**.
10. Configure the rest of the Active Directory options as applicable, and then click **Save**.
    You now see two paths, **Successful** and **Fallback**.
11. Click the **+** symbol on the Successful path between **AD Auth** and **Deny**. The options box opens.
12. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
13. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.

    **Note:** *The Logon page can be customized to match the look-and-feel of your organization. For further information about this, see the BIG-IP APM Configuration Guide.*
14. Click the **Save** button.
15. Click the **+** symbol on the Fallback path between **Variable Assign** and **Deny**. The options box opens.
16. Click the Variable Assign option button and then click Add Item.
    a. In the **Name** box, type **Variable Assign AD**.
    b. Click **Add new entry**, and then click the change link under **Assignment**.
    c. In the **Custom Variable** box, select Secure, and then type **session.logon.last.domain** in the box.
    d. In the **Custom Expression** box, type **expr { "<netbios domain>" }**.
    e. Click **Finished**.
    f. Click **Save**.
17. On the fallback path between **Variable Assign** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.

18. *Optional configuration to support two factor authentication with RSA SecurID.*
    a. Click the **+** symbol between **Logon Page** and **AD Auth**. The options box opens.
    b. Click the **Variable Assign** option button and then click **Add Item**.
    c. In the **Name** box, type **Variable Assign AD**.
    d. Click **Add new entry**, and then click the **change** link under Assignment.
    e. In the **Custom Variable** box, select **Secure**, and then type **session.logon.last.password** in the box.
    f. In the **Custom Expression** box, type
    **expr { [mcget {session.logon.last.password1}] }**.
    g. Click **Finished**.
    h. Click **Save**.
    i. At the start of the VPE, click the **Logon Page** link/box.
    j. In row #2, perform the following:
    - In the **Post Variable Name** box, type **password1**.
    - In the **Session Variable Name** box, type **password1**.
    k. In row #3, perform the following:
    - From the **Type** list, select **password**.
    - In the **Post Variable Name** box, type **password**.
    - In the **Session Variable Name** box, type **password**.
    l. Under Customization, in the **Logon Page Input Field #3** box, type **Passcode**.
    m. Click **Save**.
    n. Click the **+** symbol between **Logon Page** and **Variable Assign AD**.
    o. Click the **RSA SecurID** option button and then click **Add Item**.
    p. From the **AAA Server** list, select the RSA SecurID AAA Server you created using the configuration table.
    q. From the **Change Max Logon Attempts Allowed** list, select **1**.
    r. Click **Save**.
19. Click the yellow Apply Access Policy link in the upper left part of the window. You must apply an access policy before it takes effect.
20. Click the **Close** button on the upper right to close the VPE.

When you are finished, the Access Policy should look like one of the following examples, depending on whether you configured the optional two factor authentication section.

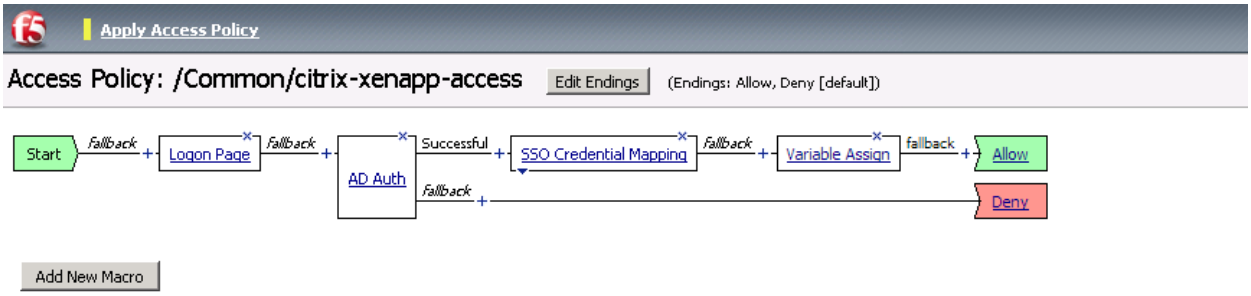



**Figure 7:** *Access Policy without two factor authentication*

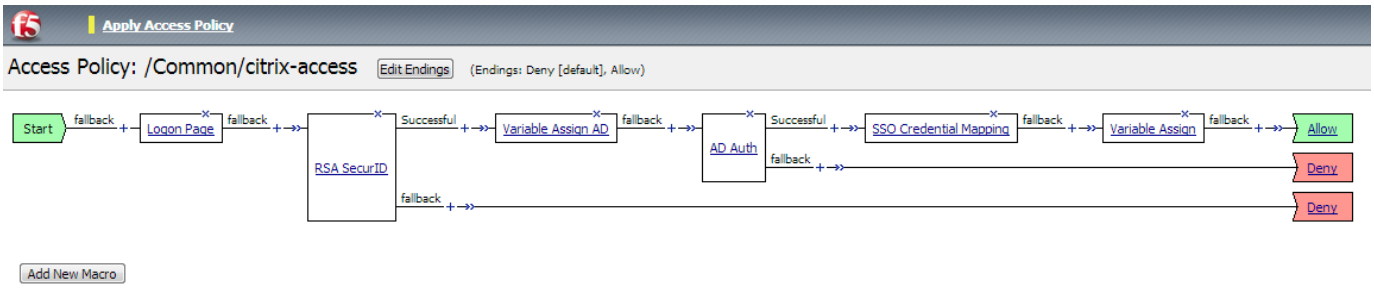



**Figure 12:** *Access Policy including two factor authentication*

### Editing the Access Profile with the Visual Policy Editor when using Web Interface servers with smart card authentication

Use this procedure if you are not using Dynamic Presentation Webtops to replace the Web Interface servers and are using smart cards for authentication. If you are using different UPN, there are additional steps

#### To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you created, and then in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **On-Demand Cert Auth** option button, and then click **Add Item**.
5. From the **Auth Mode** list, select **Require**.
6. Click the **Save** button.
7. Click the **+** symbol between **On-Demand Cert Auth** and **Deny**. The options box opens
8. Click the **iRule Event** option button, and then click **Add Item**.
9. In the **ID** field, type **CERTPROC**.
10. Click **Save**.
11. On the fallback path between **iRule Event** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.

Additional steps if you need to support different UPN's

12. Click the + symbol On the fallback path between iRule Event and allow. A box opens with options for different actions.
13. Click the + symbol between Start and Deny. A box opens with options for different actions.
14. Click the AD Query option button, and then click Add Item.
    a. From the **Server** list, select the AD server you created.
    b. In the Search Filter box, type **userPrincipalName=%{session.custom.certupn}**
    c. Click **Add new entry**.
    d. In the **Required Attributes (optional)** box, type **sAMAccountName**.
    e. Click **Save**.
15. Click the **+** symbol between **AD Query** and **Allow**. The options box opens

16. Select **Variable Assign** option, and then click **Add item**.
    a. Click **Add new entry**.
    b. Click the **Change** link.
    c. In the **Custom Variable** box, type **session.logon.last.domain**.
    d. In the **Custom Expression** box, type **expr { "<netbios domain>" }**.
    e. Click **Finished**.
    f. Click **Save**.

This completes the configuration.

# Configuring additional BIG-IP settings

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

## Configuring DNS and NTP settings

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

### Configuring the DNS settings

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

***Note***

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

***Important***

*The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.*

**To configure DNS settings**

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

### Configuring the NTP settings

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

**To configure NTP settings**

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

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

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

## Document Revision History

| Version | Description | Date |
|---|---|---|
| RC-1 | New deployment guide for Citrix XenApp and XenDesktop using iApp template version f5.citrix_vdi.v1.1.0 | 07-01-2013 |
| RC-1a | Added the section *Modifying the BIG-IP APM SSO Configuration created by the iApp if using StoreFront 2.0* to include a new SSO parameter. Only necessary if using BIG-IP APM, StoreFront 2.0, and not replacing the Web Interface servers. | 07-11-2013 |
| RC-2 | Updated deployment guide for RC-2, which includes the correct SSO parameters if using BIG-IP APM, StoreFront 2.0, and not replacing the Web Interface servers. Removed the entire *Modifying the BIG-IP APM SSO Configuration created by the iApp if using StoreFront 2.0* section. | 07-15-2013 |
| RC-3 | Updated deployment guide for RC-3, which included two code fixes:<br>- If using BIG-IP APM and WebTops, the server side SSL profile was not attached to webui_https virtual server when using an encrypted XML virtual server.<br>- The chain/intermediate certificate (if used) was not being attached to client side SSL profile when selecting to add an intermediate certificate.<br>Added the section *Modifying the Citrix StoreFront configuration if using BIG-IP APM on page 27.* | 09-12-2013 |
| RC-3a | Corrected the example in the manual configuration table for the "Data Group for use with a non-standard URI or if you are using Web Interface server or StoreFront servers" on *page 41.* The example now reads /citrix/storefrontweb. The previous example was missing the leading forward slash. | 09-30-2013 |
| RC-4 | Updated the guide for RC-4, which included only the following code fixes and no change to the content of this guide:<br>- LDAP monitor username and password now accepts spaces<br>- Resolved error noted when forwarding traffic to another BIG-IP system and not replacing web interface servers<br>- Corrected configuration when choosing to forwarding traffic to another BIG-IP and replacing Web Interface<br>- Resolved SSO configuration error when using a custom URI with Web interface server 5.4.<br>- Added data group delete record commands when reconfiguring iApp between “Replace Web Interface” to “Integrate with Web Interface” and vice versa. This eliminates issues noted with clients when entries are created in both iApp generated data-groups. | 10-10-2013 |
| RC-5 | Updated this guide for RC-5, which included the following changes:<br>- Removed the requirement in the iApp to have LTM provisioned. The iApp now supports BIG-IP APM only licensing.<br>- Added logic to the SSO configuration to support URI containing query parts (users logging out of the Web Interface servers are now correctly redirected to a logon screen when they want to log back into the Web Interface). Added this change to the manual configuration table on *page 40.*<br>- Resolved an iApp error found when users chose to use an existing pool when building XML Broker pool with an existing monitor.<br>- Resolved an iApp error found when users chose not to use the HTTP redirect virtual server<br>- Added support for BIG-IP version 11.4.1. | 12-12-2013 |
| RC-6 | Updated deployment guide for RC-6, which included the following changes:<br>- Added support for XenDesktop 7.0 and 7.1<br>- Added support for StoreFront 2.1.<br>- Resolved issue when using BIG-IP partitions | 01-17-2014 |

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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