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

Important: **The fully supported version of this iApp has been released, so this guide has been archived. See *http://www.f5.com/pdf/deployment-guides/citrix-vdi-iapp-dg.pdf* for the latest version.**

Welcome to the F5 deployment guide for Citrix® VDI applications, including XenApp® and XenDesktop® with the BIG-IP v11.4 system and later. This guide shows how to configure the BIG-IP Local Traffic Manager (LTM), Access Policy Manager (APM), and Advanced Firewall Manager (AFM) 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 VDI deployments.

This document contains guidance on configuring the BIG-IP APM for two factor authentication with RSA SecurID, as well as supporting smart card authentication.

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, APM, AFM	11.4, 11.4.1, 11.5, 11.5.1, 11.6
Citrix XenApp[1]	7.6 and 7.5[2], 6.5
Citrix XenDesktop[1]	7.6 and 7.5[2], 7.1, 7.0, 5.6
Citrix StoreFront[3]	2.6 and 2.5[2], 2.1, 2.0, 1.2
iApp Template version	f5.citrix_vdi.v2.1.0rc1
Deployment Guide revision	1.1 (see *Document Revision History on page 71*)

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

[2] XenApp and XenDesktop 7.6 and 7.5, and StoreFront 2.6 and 2.5 require a hotfix and BIG-IP 11.4.1 or later. Note that BIG-IP 11.6 does not require a hotfix.
- BIG-IP 11.4.1 requires Hotfix-BIGIP-11.4.1-HF4-647.41.iso
- BIG-IP 11.5.0 requires Hotfix-BIGIP-11.5.0.4.1.245-HF4.iso
- BIG-IP 11.5.1 requires Hotfix-BIGIP-11.5.1.5.0.147-HF5.iso

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

[3] Standalone Receivers are currently only supported using Legacy mode

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 or StoreFront 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 or StoreFront servers and the Citrix XML Broker or Desktop Delivery Controller (DDC) 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. For an additional layer of security, you can use the BIG-IP Advanced Firewall Manager (AFM) to your implementation.

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 VDI 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 the Citrix versions called out in the table on page 1. If you are using a previous version, see the deployment guide index on F5.com (*https://f5.com/solutions/deployment-guides*).
- 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 11.4 or later. Version 11.4 has a number of fixes, features, and performance enhancements not found in earlier v11 versions. 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 APM with smart card authentication or with two-factor authentication using RSA SecurID.
  - If deploying two factor authentication using SecurID, 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 deploying smart card authentication, be sure to see *Appendix A: Citrix server changes required to support smart card authentication on page 36.* Note we currently do not support smart card authentication with StoreFront version prior to 2.5; only Web Interface server 5.4 and StoreFront 2.5 and later are supported.
- In the configuration described in this guide, domain pass-through is required if using smart cards with kerberos authentication.

Domain pass-through is only supported in StoreFront 2.5 and later, therefore previous versions of StoreFront are not supported for this scenario.

- If using Web Interface servers, 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.

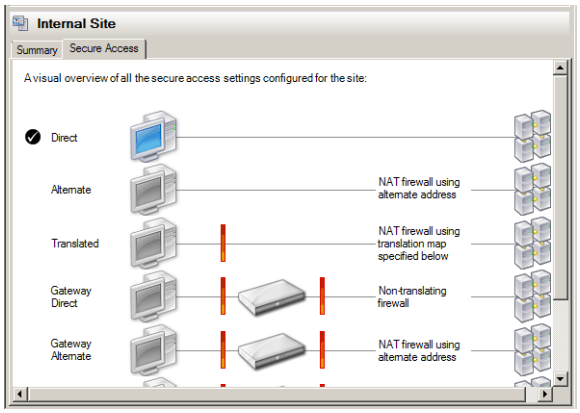


Figure 1: *Citrix Session configuration*

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 or StoreFront servers and the XML Broker or DDC servers.

In this implementation, traffic to the Citrix Web Interface or StoreFront servers and the Citrix XML Broker or DDC 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.

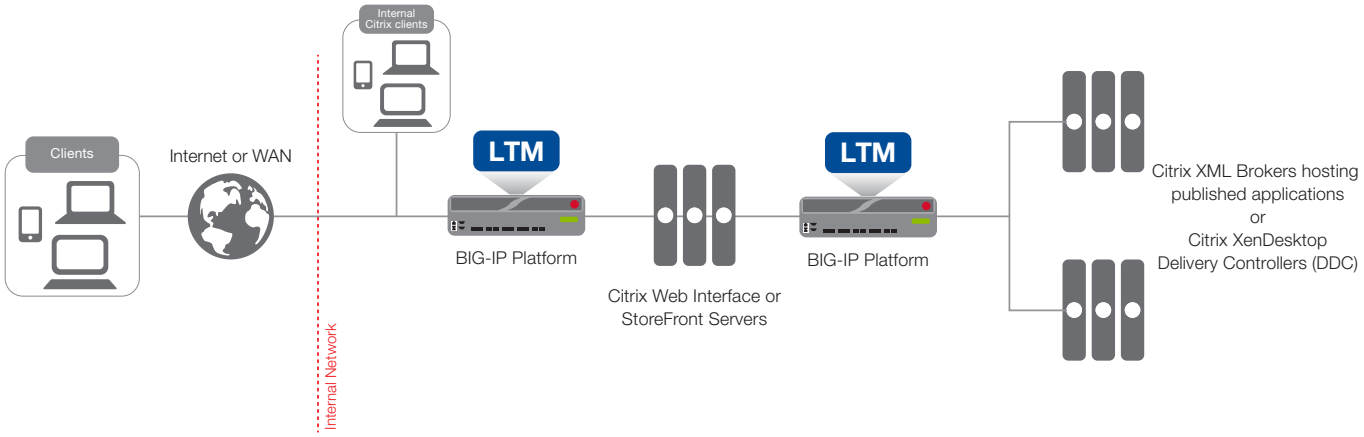


Figure 2: *Logical configuration example*

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

In this scenario, the BIG-IP APM Dynamic Presentation Webtop functionality is used to replace the Citrix Web Interface or StoreFront 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.

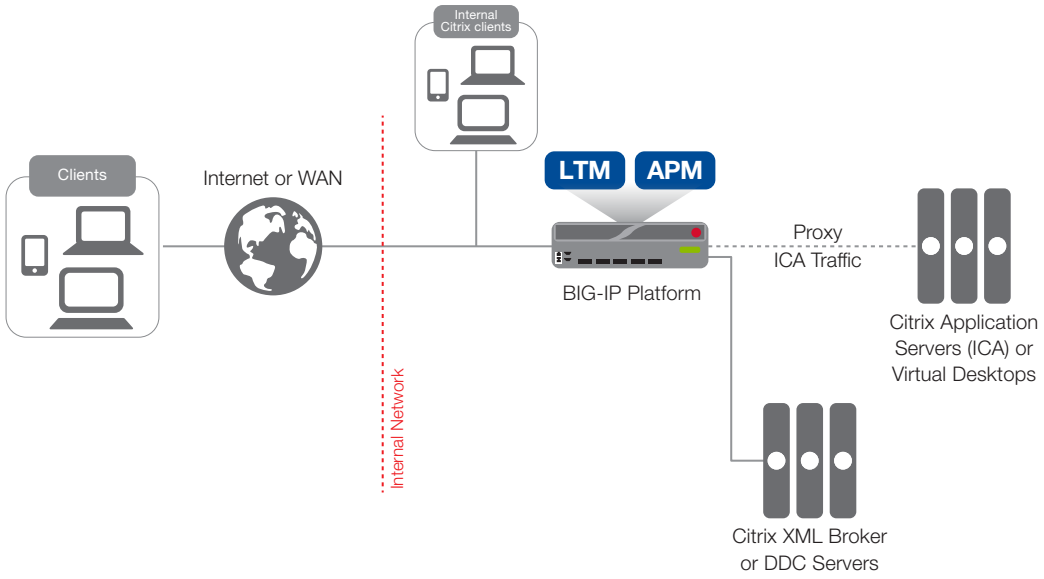


Figure 3: *Using the BIG-IP APM to replace the Web Interface or StoreFront servers*

Using the BIG-IP APM and Web Interface or StoreFront 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 or StoreFront devices.

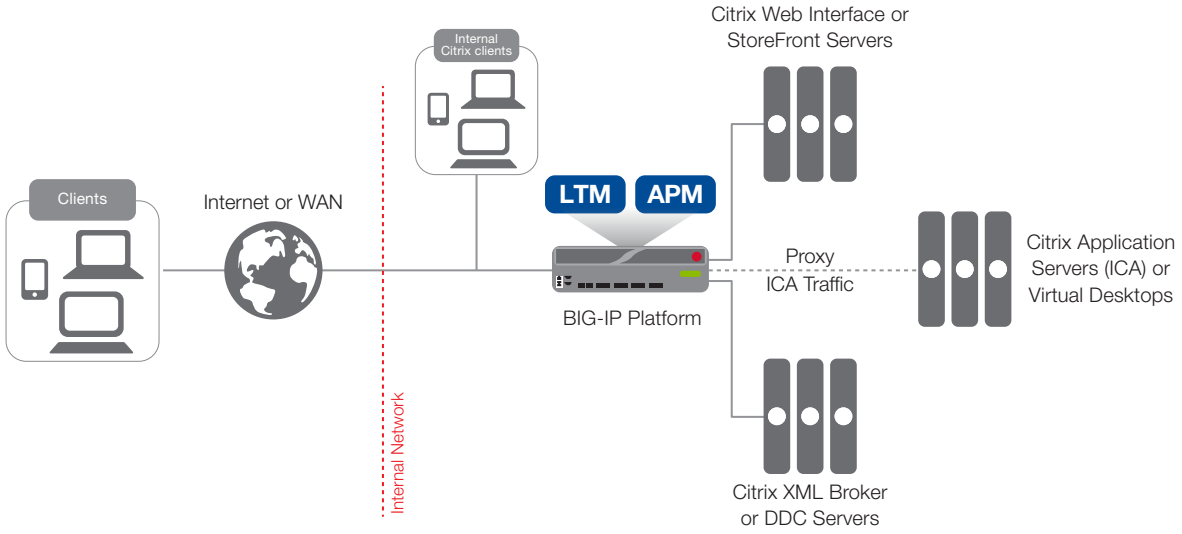


Figure 4: *Using the BIG-IP APM with Web Interface or StoreFront servers*

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 *downloads.f5.com*.
2. Click **Find a Download**, and then click **BIG-IP v11.x / Virtual Edition**.
3. If necessary, select a BIG-IP product version from the list, and then click **iApp-Templates**.
4. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
5. Extract the files. This version Release Candidate version of this iApp is in the **RELEASE-CANDIDATE** folder.
6. Extract (unzip) the **f5.citrix_vdi.v2.1.0rc1** file (or a newer version if applicable).
7. Log on to the BIG-IP system web-based Configuration utility.
8. On the Main tab, expand **iApp**, and then click **Templates**.
9. Click the **Import** button on the right side of the screen.
10. Click a check in the **Overwrite Existing Templates** box.
11. Click the **Browse** button, and then browse to the location you saved the iApp file.
12. Click the **Upload** button. The iApp is now available for use.

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.v2.1.0rc1** (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 to securely proxy application (ICA) traffic and authenticate users into your Citrix environment?***
   Select whether you are using BIG-IP APM 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 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 Citrix 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 Citrix 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 Domain Name used for your Citrix 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 or StoreFront Servers on page 16.*

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 or StoreFront 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 versions prior to 2.5; only Web Interface server 5.4 and StoreFront v2.5 and later are supported.

Important

Be sure to see Appendix A: Citrix server changes required to support smart card authentication on page 36 for important guidance on configuring your Citrix and Active Directory devices.

If you are using smart card authentication, go directly to Yes, BIG-IP APM should support smart card authentication on page 10.

- **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.

  a. *Do you want to replace Citrix Web Interface or StoreFront servers with the BIG-IP system?*
  You can use the BIG-IP system to eliminate the need for the Citrix Web Interface or StoreFront servers altogether.

  - **No, do not replace the Citrix Web Interface or StoreFront servers**
    Select this option if you do not want to use the BIG-IP system to replace the Web Interface or StoreFront servers from your environment.
  - **Yes, replace Citrix Web Interface or StoreFront servers with the BIG-IP system**
    Select this option if you want the BIG-IP system to replace the need for Citrix Web Interface or StoreFront servers. This configures the BIG-IP system with APM and uses a single HTTPS (port 443) virtual server to provide proxy authentication and secure remote access to XenApp or XenDesktop services without requiring the use of an F5 Edge Client. It also provides the option of using BIG-IP Dynamic Presentation Webtop functionality to replace Citrix Web Interface or StoreFront servers in the Virtual Server for Web Interface or StoreFront servers section.

    For this scenario to work properly, the BIG-IP system must have connectivity to a Citrix XML Broker or DDC server.

  b. *Create a new AAA object or select an existing one?*
  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.

  - *Select the AAA Server you created from the list*
    If you have previously created an AAA Server for your Citrix implementation, select that object you created from the list. Continue with *c. Do you want the BIG-IP system to proxy RSA SecurID for two-factor authentication? on page 9.*
  - **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.

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

    ii). *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.

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

    - **Yes, anonymous binding is allowed**
      Select this option if anonymous binding is allowed. No further information is required.
    - **No, credentials are required for binding**
      If credentials are required for binding, you must specify an Active Directory user name and password for use in the AAA Server.

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

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

iv). *Which monitor do you want to use?*
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 is available in the list.
  Go to *c. Do you want the BIG-IP system to proxy RSA SecurID for two-factor authentication?* on this page.
- **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.
  Go to *c. Do you want the BIG-IP system to proxy RSA SecurID for two-factor authentication?* on this page.
- **Create a new LDAP monitor for the Active Directory pool**
  Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

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

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

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

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

  5). *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.

  6). *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.

c. *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 *Virtual Server for Web Interface or StoreFront Servers on page 16.*
- **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. Continue with *Virtual Server for Web Interface or StoreFront Servers on page 16.*

- **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 or StoreFront server, and once as the Citrix application or desktop is launched.

a. *Do you want to replace Citrix Web Interface or StoreFront servers with the BIG-IP system?*
You can use the BIG-IP system to eliminate the need for the Citrix Web Interface or StoreFront servers altogether. If you do not replace the Web Interface or StoreFront servers with the BIG-IP system, Citrix published applications are presented using Citrix Web Interface or StoreFront servers.

- **Yes, replace Citrix Web Interface or StoreFront servers with the BIG-IP system**

Select this option if you want to replace the need for Citrix Web Interface or StoreFront servers with the BIG-IP system. In this case, Citrix published applications are presented using an F5 Dynamic Presentation Webtop instead of the Citrix Web Interface or StoreFront. With this approach, you do not need Citrix Web Interface or StoreFront servers in your environment. This BIG-IP system must have connectivity to a Citrix XML Broker or DDC server, or a BIG-IP virtual server that load balances a pool of XML Broker or DDC servers.

Important

Citrix XML Brokers and Desktop Delivery Controllers require that SID enumeration is enabled when using smart card authentication with Webtops. Citrix article CTX117489 describes how to enable SID enumeration for XenApp servers and CTX129968 describes the process for Desktop Delivery Controllers. XML Brokers and DDCs also need to trust XML requests sent to XML services. Citrix article CTX132461 contains procedures on how to enable XML trust on DDC.

i). *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. Continue with *Virtual Server for Web Interface or StoreFront Servers on page 16.*
- **No, the UPNs are different**
Select this option if the UPNs are not the same. In this case, the iApp either creates an Active Directory AAA Server profile object which is used to query and determine the correct UPN to use, or uses the profile you specify in the following question.

1). *Create a new AAA object or select an existing one?*
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.

* **Select the AAA Server you created from the list**
If you have previously created an AAA Server for your Citrix implementation, select that object you created from the list. Continue with *Virtual Server for Web Interface or StoreFront Servers on page 16.*

* **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 Citrix 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.

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

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

d). *Which monitor do you want to use?*
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 is available in the list.
- **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.
- **Create a new LDAP monitor for the Active Directory pool**
  Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

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

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

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

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

5). *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.

6). *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.

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

i). *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.

1). *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.

2). *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 system to Web Interface or StoreFront 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**.

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

4). *What is the Kerberos Key Distribution Center (KDC) for the server realm?*
Type the KDC for the server's realm. This is normally an Active Directory domain controller. If you leave this empty, the KDC must be discoverable through DNS, for example, BIG-IP system must be able to fetch SRV records for the server realm's domain, where the name is usually the same as the realm's name. If the domain name is different from the realm name, it must be specified in /etc/krb5.conf file, otherwise adding the realm configuration to that file is not required. Kerberos SSO processing is fastest when KDC is specified by its IP address, and slower if it is specified by host name, and even slower if it is left empty (due to additional DNS queries). When the user's realm is different from the server's realm, KDC must be left empty. This is also true in cases of multi-domain realms. If you leave this field blank, set dns_lookup_kdc parameter to equal true in BIG-IP /etc/krb5.conf file.

Continue with *Virtual Server for Web Interface or StoreFront Servers on page 16*.

- **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.

1). *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 lower case letters when you submit the template.

2). *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 system to Web Interface or StoreFront 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**.

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

4). *What is the Kerberos Key Distribution Center (KDC) for the server realm?*
Type the KDC for the server's realm. This is normally an Active Directory domain controller. If you leave this empty, the KDC must be discoverable through DNS, for example, BIG-IP system must be able to fetch SRV records for the server realm's domain, where the name is usually the same as the realm's name. If the domain name is different from the realm name, it must be specified in /etc/krb5.conf file, otherwise adding the realm configuration to that file is not required. Kerberos SSO processing is fastest when KDC is specified by its IP address, and slower if it is specified by host name, and even slower if it is left empty (due to additional DNS queries). When the user's realm is different from the server's realm, KDC must be left empty. This is also true in cases of multi-domain realms. If you leave this field blank, set dns_lookup_kdc parameter to equal true in BIG-IP /etc/krb5.conf file.

5). *Create a new AAA object or select an existing one?*
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.

* *Select an existing AAA Server object*
  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.

* **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 Citrix 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.

  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.

- **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.
- **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 logging in 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.

Advanced Firewall Manager (AFM)

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

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

   - **No, do not use Application Firewall Manager**
     Select this option if you do not want to enable BIG-IP AFM at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.
   - *Select an existing AFM policy from the list*
     If you already created a BIG-IP AFM policy for your Citrix implementation, select it from the list. Continue with ***c***.
   - **Yes, use F5's recommended AFM configuration**
     Select this option if you want to enable BIG-IP AFM using F5's recommended configuration.

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

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

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

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

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

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

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

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

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

- **Do not apply a logging profile**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing logging profile from the list*
  If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging**

Profiles. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the ***BIG-IP Network Firewall: Policies and Implementations*** guide for more information.

Virtual Server for Web Interface or StoreFront Servers

The next section of the template asks questions about the BIG-IP virtual server for the Citrix Web Interface or StoreFront 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.

If you chose to proxy ICA traffic and authenticate users and replace the Web Interface or StoreFront servers, start with #2.

1. ***How should the BIG-IP system handle encrypted traffic to Web Interface or StoreFront Servers?***
   This question only appears if you chose not to proxy ICA traffic and authenticate users with the BIG-IP system or chose to proxy ICA traffic but not replace the Web Interface or StoreFront servers.

   Chose how you want the BIG-IP system to process encrypted traffic destined for the Web Interface or StoreFront servers.

   - **Terminate SSL for clients, plaintext to Citrix servers (SSL offload)**
     Select this option if you want the BIG-IP system to offload SSL processing from the Citrix servers. In this case, the BIG-IP system decrypts incoming traffic and then sends the traffic to the Citrix servers unencrypted.
   - **Terminate SSL for clients, re-encrypt to Citrix servers (SSL bridging)**
     Select this option if your Citrix servers expect encrypted traffic. In this case, the BIG-IP system decrypts incoming traffic and then re-encrypts it before sending it to the Citrix servers.

2. ***Which Client SSL profile do you want to use?***
   The iApp can create a new Client SSL profile, or if you have created a Client SSL profile which contains the appropriate SSL certificate and key for your Citrix implementation, you can select it from the list.

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

   - *Select the Client SSL profile you created from the list*
     If you manually created a Client SSL profile, select it from the list.
   - **Create a new Client SSL profile**
     Select this option if you want the iApp to create a new Client SSL profile.

     a. *Which SSL certificate do you want to use for authentication?*
     Select the SSL certificate you imported onto the BIG-IP system for decrypting client connections.

     If you have not yet imported a certificate, you can leave the default selections and reconfigure this iApp after obtaining the certificates. Using the default certificate and key results in an incomplete configuration which is not secure until you import and assign a trusted certificate and key that are valid for all fully qualified domain names used to access the application.

     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.

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

     c. *Which intermediate certificate do you want to use?*
     If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is

already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown. See http://support.f5.com/kb/en-us/solutions/public/13000/300/sol13302.html for help creating an intermediate certificate chain.

2. ***Which Server SSL profile do you want to use?***
This question only appears if you chose SSL Bridging.

   Select whether you want the iApp to create the F5 recommended Server SSL profile, or if you want to choose a Server SSL profile you already created.

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

   The servers must also process the encrypted traffic, so you have to install and manage certificates on both the servers and the BIG-IP system. Certificates that you install on the servers may be self-signed and can be a lesser encryption strength (shorter bit length) than the certificate on the BIG-IP system if internal encryption requirements are different than those that apply to public-facing traffic.

3. ***If using not using the default PNAgent URI, what is the custom PNAgent URI?***
This question only appears if you chose to proxy ICA traffic but not use smart cards and not to replace the Web Interface or StoreFront servers.

   If you are not using a default PNAgent URI, specify the custom PNAgent URI for your environment. The default PNAgent URI for Web Interface servers is /**Citrix/PNAgent/config.xml**. Verify StoreFront legacy PNAgent support is enabled, Citrix clients use **/Citrix/<storename>/PNAgent/config.xml**.

   If you are using a default PNAgent URI, leave this field blank.

4. ***Should the iApp remove the APM session when users log out of the Web Interface or StoreFront servers?***
This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system, and not to replace the Web Interface or StoreFront servers.

   Choose whether you want the system to remove the APM session from the BIG-IP APM when users log out of the Web Interface or StoreFront servers. If you select Yes, the system terminates all active APM sessions for that user, including any open ICA sessions. If you select No, the system leaves APM user sessions active when users are logged out from Citrix Web Interface or StoreFront servers. The BIG-IP APM removes these user sessions after the default idle timeout of 15 minutes.

5. ***What IP address will clients use to access the Web Interface or StoreFront 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 or StoreFront 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 or StoreFront servers.

   If you are using Citrix StoreFront in your implementation, select the version of StoreFront you are using. Otherwise, select No, my Citrix environment does not use StoreFront. The BIG-IP system supports Citrix StoreFront software, version 1.2, 2.0, 2.1, 2.5, and 2.6.

   - **Yes, my Citrix environment uses StoreFront 1.x, 2.0 or 2.1**
     Select this option if you have replaced the standard Web Interface servers with StoreFront version 1.x, 2.0 or 2.1.
   - **Yes, my Citrix environment uses StoreFront 2.5 or 2.6**
     Select this option if you have replaced the standard Web Interface servers with StoreFront version 2.5 or 2.6.
   - **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. *What are the URLs of the Citrix Secure Ticket Authority Servers (if required)?* **Advanced**
     This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system, not to use Smartcard authentication, and not replacing the Web Interface or StoreFront servers.

If your implementation requires that Receiver client ICA files issued by Citrix Secure Ticket Authorities be unaltered by APM, you must specify the full URL for each Citrix Secure Ticket Authority, such as https://<STA FQDN>/scripts/ctxsta.dll.

Citrix Web Interface servers need to be configured to use Direct Gateway secure access mode. The Gateway setting on the Web interface servers uses the FQDN which resolves to the BIG-IP APM virtual server address. The Secure Ticket Authority URLs used in the Web Interface Gateway settings should match URLs you specify here.

7. ***What is the URI used on StoreFront or Web Interface servers for XenApp or XenDesktop?***
Specify the URI you are using on your Web Interface or StoreFront servers. The default URI when using Web Interface servers for XenApp is **/Citrix/XenApp/**. The default URI for XenDesktop 5.x is **/Citrix/XenDesktopweb/**. The URI when using StoreFront follows the pattern **/Citrix/<storename>Web/** where <storename> is replaced with the name you used when creating the store for this Citrix site. You can verify your URI for StoreFront by opening the StoreFront console and highlighting **Receiver for Web**. The **Website URL:** field contains the URI you should use here.

8. ***Which port do you want to use for this HTTPS virtual server?***
Specify the HTTPS port you want to use for the BIG-IP virtual server. The text box displays default port for HTTPS: **443**. Change the port if necessary.

9. ***Which CA certificate bundle do you want to use for your trusted and advertised certificate authorities?***
This question only appears if you specified you are using smart card authentication and chose to create a new Client SSL profile.

   Select the CA certificate bundle you want to use for this implementation. You must have imported a Certificate Authority certificate bundle onto the BIG-IP system, or use the BIG-IP system's internal ca-bundle.crt bundle. If you want to use a third-party certificate bundle, it must already be imported onto the system for it to appear in this list. The certificate bundle is used in the BIG-IP Client SSL profile created by the iApp in the Trusted Certificate Authorities and Advertised Certificate Authorities fields.

10. ***Do you want to redirect inbound HTTP traffic to HTTPS?*** **Advanced**
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.

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

> ***Note***
>
> *If you chose to replace the Web Interface or StoreFront servers with the BIG-IP system, this question is referring to where the virtual servers be in relation to the XML Broker servers.*

    - **Same subnet for BIG-IP virtual servers and Web Interface or StoreFront servers**
    If the BIG-IP virtual servers and Web Interface or StoreFront 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 or StoreFront server?*
      Select whether you expect more or fewer than 64,000 concurrent connections to each Web Interface or StoreFront 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 or StoreFront 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 or StoreFront servers**
  If the BIG-IP virtual servers and Web Interface or StoreFront servers are on different subnets, the following question appears asking how routing is configured.

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

  - **Web Interface or StoreFront servers do NOT use BIG-IP as the default gateway**
    If the Web Interface or StoreFront 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 or StoreFront server?
    Select whether you expect more or fewer than 64,000 concurrent connections to each Web Interface or StoreFront 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 or StoreFront 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.

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

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

    - *Select an existing network optimization profile*
      If you created a custom TCP profile for this implementation, select it from the list.

- **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.

15. ***Do you want to add any custom iRules to this configuration?*** 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 or StoreFront servers

In this section, you add the Web Interface or StoreFront servers and configure the load balancing pool. Even if you chose to replace the Web Interface or StoreFront 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 or StoreFront servers. This is the name that resolves (or will resolve) to the BIG-IP virtual server address you specified for the Web Interface or StoreFront servers in the previous section.

   If you selected to use APM to proxy ICA traffic and authenticate users and to replace the Web Interface or StoreFront servers with the BIG-IP system, this section ends here; continue with *Virtual Server for XML Broker or Desktop Delivery Controller (DDC) Servers on page 21.*

2. ***Which pool do you want to use?***
   Select whether you want the system to create a new pool for the Web Interface or StoreFront servers, or if you have already created a Web Interface or StoreFront pool on this BIG-IP system.
   - *Select an existing pool from the list*
     If you created a custom load balancing pool for the Web Interface or StoreFront servers, select it from the list. Unless you have a specific reason to use an existing pool (with a custom health monitor) we recommend allowing the iApp template to create one.

     If you select an existing pool, the rest of the questions in this section disappear. Continue with *Virtual Server for XML Broker or Desktop Delivery Controller (DDC) Servers on page 21.*
   - **Create a new pool of Web Interface or StoreFront servers**
     Select this option for the system to create a new pool for the Web Interface or StoreFront servers. The following questions appear, depending on which configuration mode you selected.

     a. *Which port have you configured for Web Interface or StoreFront HTTPS traffic?*
        Specify the TCP port you configured for Web Interface or StoreFront traffic. The default is 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 or StoreFront 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 Citrix 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 system 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 or StoreFront server in the Priority box described in step 3.

  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.

3. ***What are the IP addresses of your Web Interface or StoreFront servers?***
Specify the IP Address and Port for each Web Interface or StoreFront 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.

4. ***Which monitor do you want to use?***
Select whether you want the system to create a new health monitor for the Web Interface or StoreFront servers, or if you have already created a Web Interface or StoreFront health monitor on this BIG-IP system.

- *Select an existing monitor from the list*
  If you created a custom health monitor for the Web Interface or StoreFront servers, select it from the list. Unless you have a specific reason to use a custom health monitor, we recommend allowing the iApp template to create one.

- **Create a new health monitor**
  Select this option for the system to create a new health monitor for the Web Interface or StoreFront servers. This monitor queries Citrix Web Interface or StoreFront 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 or Desktop Delivery Controller (DDC) Servers

The next section of the template asks questions about the BIG-IP virtual server for the Citrix XML Broker or DDC devices.

1. ***How many unique XML Broker or DDC farms are you using?*** Advanced
   This question only appears if you chose Advanced, to replace the Web Interface or StoreFront 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 or DDC farms are a part of your Citrix implementation. The iApp supports up to five XML Broker or DDC farms.

2. ***What IP address do you want to use for the XML Broker or DDC virtual server?***
   *This question only appears if you are using BIG-IP version **11.2.x - 11.3** and chose not to replace the Web Interface or StoreFront servers with the BIG-IP system.*

   Specify the BIG-IP virtual server IP address for the XML Broker or DDC devices. This must be an IP address your Web Interface or StoreFront servers can access. Use this address as the Web Interface or StoreFront 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. ***How will requests from the Web Interface or StoreFront servers arrive?***
   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 or DDC requests will arrive encrypted (HTTPS)**
     Select this option if XML Broker or DDC requests from the Web Interface or StoreFront servers will arrive encrypted. This determines the default port used for the BIG-IP virtual server (you can change this port in the following question).

     a. *Which port do you want to use for this HTTPS virtual server?*
     Specify the port this XML Broker or DDC 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 or StoreFront server farm.

     b. *Which certificate do you want the BIG-IP XML Broker or DDC virtual server to use for authentication?*
     This question only appears if you chose not to replace the Web Interface or StoreFront servers with the BIG-IP system.

     Select the certificate you imported for the XML Broker or DDC 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?*
     This question only appears if you chose not to replace the Web Interface or StoreFront servers with the BIG-IP system.

     Select the associated key from the list.

   - **XML Broker or DDC requests will arrive unencrypted (HTTP)**
     Select this option if XML Broker or DDC requests from the Web Interface or StoreFront servers will arrive unencrypted. This determines the default port used for the BIG-IP virtual server (you can change this port in the following question).

     a. *Which port do you want to use for this HTTP virtual server?*
     Specify the port this XML Broker or DDC 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 or StoreFront server farm.

4. ***Which Citrix Client Bundle do you want to use?***
   This question only appears if you chose to replace the Web Interface or StoreFront servers with the BIG-IP system.

   Select the Citrix Client Bundle you want to use for this implementation. If you want to support HTML 5 clients for use when a Receiver client is not available, you must select a Citrix Client Bundle that you have already created that includes the proper Windows file

package. If you do not require HTML 5 client support, or would like to use a custom URL, select Create a new Citrix Client Bundle. If you have already created a custom Citrix Client Bundle, you can select it from the list. NOTE:

For information on configuring a Citrix Client Bundle that includes HTML5 support, see *Creating the Citrix Client Bundle for HTML 5 support on page 46.*

Important

A Citrix Client Bundle is required for HTML 5 support. You cannot create the client bundle from the iApp template, you must manually create a bundle that includes the proper Windows file package. HTML 5 Citrix Client support requires BIG-IP 11.4 or later with the latest HF applied.

2. ***Where do you want to direct users when a Receiver client is not detected on their host?***
This question only appears if you chose to replace the Web Interface or StoreFront servers with the BIG-IP system.

   Specify a URL to direct users to if a Citrix Receiver client is not detected on their host device. The default is receiver.citrix.com, where users can download the latest Receiver client.

3. ***Where will your BIG-IP virtual servers be in relation to your XML Broker or DDC servers?***
This and all the following questions in this section only appear if you chose NOT to replace the Web Interface or StoreFront servers with the BIG-IP system.

   Select whether your BIG-IP virtual servers are on the same subnet as your XML Broker or DDC 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 or DDC servers**
   If the BIG-IP virtual servers and XML Broker or DDC 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. *What is the maximum number of connections you expect to each XML Broker or DDC 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 or DDC 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 or DDC server is reached, new requests fail.

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

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

- **XML Broker or DDC 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). *What is the maximum number of connections you expect to each XML Broker or DDC server?*
  Select whether you expect more or fewer than 64,000 concurrent connections to each XML Broker or DDC 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 or DDC 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 or DDC servers use BIG-IP as the default gateway**
  Select this option if the XML Broker or DDC servers use the BIG-IP system as their default gateway. If they do, the concurrent user question does not appear.

5. ***Do you want to add any iRules to this configuration?*** Advanced
   Select if have preexisting iRules you want to add to this XML Broker or DDC virtual server. 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 or DDC Servers

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

1. ***Should the iApp create a new pool or use an existing one?***
   This question only appears if you chose to proxy ICA traffic and authenticate users with the BIG-IP system and to replace Web Interface or StoreFront servers.

   - *Select an existing pool of XML Broker or DDC servers*
     If you have already created a pool of XML Broker or DDC servers for this configuration, select it from the list.

     If you choose an existing pool, be aware 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 or DDC servers.

     a. *What custom caption do you want to use for the XML Broker or DDC farm?*
     The iApp gives you the option of providing a caption message to users in the event the farm they are trying to reach is unavailable. If you want the system to display a caption, type the message in the box. Note there is a 22 character limit for the caption message. Continue with *Finished on page 28.*

- **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 or DDC devices.

  a. *What custom caption do you want to use for the XML Broker or DDC farm?*
  The iApp gives you the option of providing a caption message to users in the event the farm they are trying to reach is unavailable. If you want the system to display a caption, type the message in the box. Note there is a 22 character limit for the caption message.

  b. *Which load balancing method do you want to use?* **Advanced**
  Specify the load balancing method you want to use for this XML Broker or DDC 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 Citrix 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 XML Broker server in the Priority box described in #4.

    i). *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.

  e. *What are the IP addresses of your XML Broker or DDC 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 (80 or 443) for the XML Broker or DDC 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.

  f. *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 or DDC servers, or if you have already created a health monitor on this BIG-IP system for these servers.

- *Select an existing health monitor*
  If you have already configured a health monitor for the XML Broker or DDC servers, select it from the list. 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.
- **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 Citrix 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.

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 Citrix servers. It is important to use a published resource that will always be available since all XML Broker or DDC members will be marked down if chosen published application is removed or becomes unavailable.

Additional XML Broker or DDC server farms

If you answered the question "How many unique XML Broker or DDC farms are you using?" (only visible if you selected to replace the Web Interface or StoreFront servers and to proxy ICA traffic and authenticate users with the BIG-IP system), you see the previous section repeated for each farm you specified you were using. If necessary, return to *XML Broker or DDC Servers on page 24* for guidance.

ICA Traffic

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

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

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. Continue with *Finished on page 28*

- **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 Citrix 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. 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. *Which ports are assigned to Multi-Stream ICA?*
If you require Citrix Multi-Stream ICA support, you can include up to three additional ports. Multi-Stream ICA uses multiple TCP connections to carry the ICA traffic between the client and the server. Click Add to include more ports.

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 more servers.

d. *What is your public-facing route domain?*
Select the public-facing route domain you configured. As described in the Important note above, you must already have route domains configured before you can select them from the list.

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 you must understand how each iRule affects your deployment, including application behavior and BIG-IP system performance. 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 you may have to make depending on how you configured the BIG-IP system.

Modifying the Citrix Web Interface or StoreFront 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 or StoreFront servers*.

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

You must modify the Web Interface or StoreFront server configuration so these devices send traffic to the BIG-IP XML Broker or DDC virtual server and not directly to the XML Brokers or DDC servers themselves. You must also make sure "Use the server list for load balancing" is unchecked, as shown in the following example. The procedure depends on whether you are using Web Interface or StoreFront Servers.

To modify the Web Interface servers to point at the XML Broker or DDC 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.

To modify the StoreFront servers to Point at the XML Broker or DDC virtual server

1. From the Storefront server, open the Citrix StoreFront management console.
2. In the Navigation pane, select **Stores**, and then the store name.
3. Click the **Action** menu item at the top and select **Manage Delivery Controllers**.
4. Edit the existing delivery controller(s).
5. Remove existing servers and add the BIG-IP XML Broker or DDC virtual server address.
6. Click the **OK** button. Repeat this procedure for any/all additional StoreFront 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**.

Modifying the XML Brokers or Desktop Delivery Controllers to trust XML requests when using F5 Dynamic Webtops to replace Citrix Web Interface or StoreFront servers

You must modify the XML brokers or DDC servers to accept XML requests from the BIG-IP APM. The process is slightly different for XML Brokers and DDC devices, use the appropriate procedure.

To modify the XML Broker profile in XenApp 6.5 installations

1. Open Citrix App Center.
2. Select **Policies** in navigation pane.
3. Select active computer policy and then select Edit.
4. Select the Settings tab.
5. Search for **Trust XML requests**.
6. Select and edit **Trust XML requests**.
7. Select **Enabled**.
8. Click **OK** in Settings window
9. Click **OK** in Policy window
10. You should now see policy in Summary tab noted as an Active setting.

To modify DDC to accept XML requests for XenDesktop 5.6, or XenDesktop 7.x

1. Open Windows PowerShell
2. Type **asnp Citrix*** to verify the Citrix cmdlets are available.
3. Type **Set-BrokerSite - TrustRequestsSentToTheXmlServicePort $true**.
4. Verify setting and type **Get-BrokerSite** and look to see if **TrustRequestsSentToTheXMLServicePort**' is equal to **True**.
5. Close PowerShell.

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 or StoreFront 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 or StoreFront 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 or StoreFront 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 or StoreFront 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 31* 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 or StoreFront 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 or StoreFront 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 or StoreFront 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 or StoreFront is accessible without having to type in credentials, then the Web Interface or StoreFront 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 system'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 smart card authentication to the Web Interface or StoreFront 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 authentication 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. Use the command **tail –f /var/log/ltm**.

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

➤ **Why am I see the following error after rebooting a BIG-IP system that contains an XML monitor produced by the Citrix iApp: The configuration has not yet loaded. If this message persists, it may indicate a configuration problem.**

BIG-IP version 11.5 introduced a bug that improperly handled escape characters that were a part of health monitors. The latest BIG-IP v11.5 Hotfix resolves this issue. If you are unable to install the latest hotfix, use the following guidance to work around the issue.

Run the following tmsh command to verify the health monitor created by the iApp is the issue: **load sys config verify**.

If the monitor is causing the issue, you see a error message like the following: *Monitor /Common/citrix-sf25.app/citrix-sf25_xml_http parameter contains unescaped " escape with backslash. Unexpected Error: Validating configuration process failed*.

To resolve this issue, use the following procedure:

a. Backup the BIG-IP configuration (**System > Archive > Create**). For specific instructions, see the BIG-IP documentation.

b. Using **winscp** or similar program, open **/config/bigip.conf** on your BIG-IP system.

c. Search for Citrix XML monitor(s) which use unescaped characters. A easy way to find monitors is to search for POST /scripts.

d. Delete the monitor Send String POST and replace with double quotes "". You have to recreate this monitor after the configuration has successfully loaded.

For example, if your monitor looks like the following:

```
send "POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Length: 578\r\nContent-Type: text/xml\r\
nConnection: close\r\nHost: sf25-5.citrix.local.com\r\n\r\n<?xml version=\"1.0\" encoding=\"UTF-
8\"?><!DOCTYPE NFuseProtocol SYSTEM \"NFuse.dtd\"><NFuseProtocol version=\"5.1\"><RequestAppData>
<Scope traverse=\"subtree\"></Scope><DesiredDetails>permissions</DesiredDetails><ServerType>all</
ServerType><ClientType>ica30</ClientType><ClientType>content</ClientType><Credentials><UserName>
user1</UserName><Password encoding=\"cleartext\">password</Password><Domain type=\"NT\">citrix</
Domain></Credentials><ClientName>citrix-sf25_http_xmlb_monitor</ClientName><ClientAddress
addresstype=\"dot\">0.0.0.0</ClientAddress></RequestAppData></NFuseProtocol>\r\n\r\n"
```

You would change it to the following:

```
send ""
```

e. Save the BIG-IP configuration.

f. Verify the configuration for errors by running tmsh command: **load sys config verify**

g. If verification runs free from errors, load the configuration using the tmsh command: **load sys config**.

h. To prevent the error from reoccurring, update your BIG-IP system to latest hotfix.

i. Rerun iApp template to recreate appropriate send string in XML Monitor.

➤ **Users are unable to load published resources when using the HTML5 client**

There is a known issue when using HTML5 clients with BIG-IP partitions. The issue will be addressed in a future release and can be resolved by creating the associated Citrix client bundle in the BIG-IP common partition (see *Creating the Citrix Client Bundle for HTML 5 support on page 46*).

➤ **Application resources do not properly launch when using the HTML5 client with Google Chrome**

Verify your browser allows pop-ups for your Citrix website using explicit exceptions. In some cases, if pop-ups are enabled with explicit exceptions you will not be able to open the selected resource. Until this issue has been corrected, the only viable workaround is to modify Chrome to allow ***all*** pop-ups, rather than having an explicit exception for pop-ups for your Citrix website.

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/StoreFront servers, Active Directory Kerberos servers, Citrix XML Broker/DDC and application servers, client desktops, and the BIG-IP system in support of Citrix XenApp and XenDesktop smart card access with two smart card 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 smart card access when using the BIG-IP system to securely proxy ICA connections and manage single sign on smart card Kerberos authentication.

We recommend you review the F5 ***Citrix Integration*** guide for more information on Citrix, BIG-IP APM, and using smart cards: *http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-citrix-integration-11-4-0.html*.

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
- Web Interface 5.4 or Storefront 2.5 or later
- Citrix XenApp 6.5 and 7.5 and XenDesktop 7.x and 5.6.
- BIG-IP system 11.2 or later with LTM and APM provisioned modules
- Smart card 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 smart card logon directly. The user authenticates to the Web Interface via smart card, and then authenticates separately via smart card to the Windows server hosting the Citrix applications or desktops. Because these are separate authentications, the user is prompted for their smart card PIN twice.

Using smart cards when using Web Interface or StoreFront servers

The authentication process using smart cards with Web Interface or StoreFront servers is as follows:

1. The client makes a normal browser call to the Citrix Web Interface or StoreFront 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 or StoreFront 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 virtual server.
4. The user is presented with a (second) smart card authentication prompt to authenticate to the chosen application or desktop.

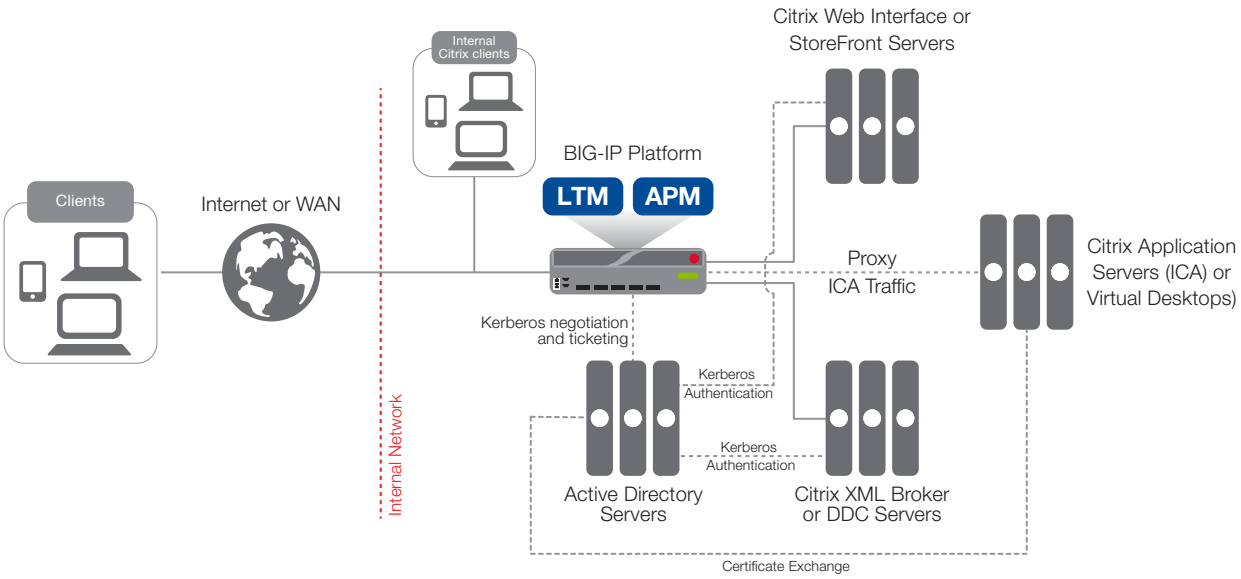


Figure 5: *Using smart card authentication with Web Interface or StoreFront servers*

Using smart cards when replacing the Web Interface or StoreFront servers with the BIG-IP system

The authentication process using smart cards is as follows:

1. The client makes a normal browser call to 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 authentication and gets published applications for user by sending certificate security identifier (users SID) to XML Broker or Desktop Delivery Controller.
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 virtual server.

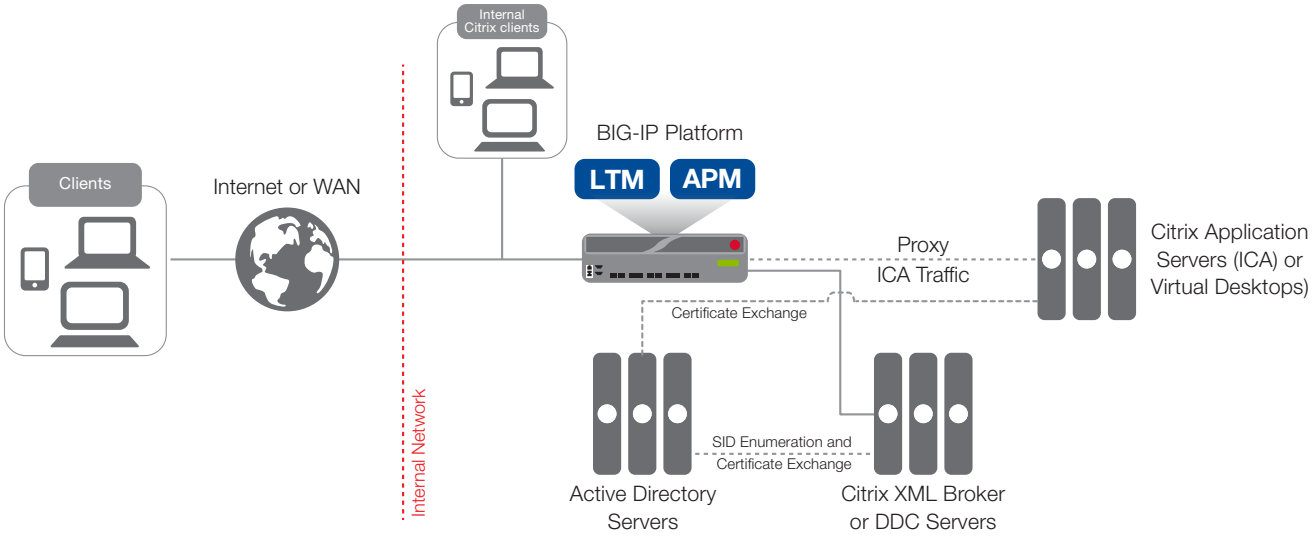
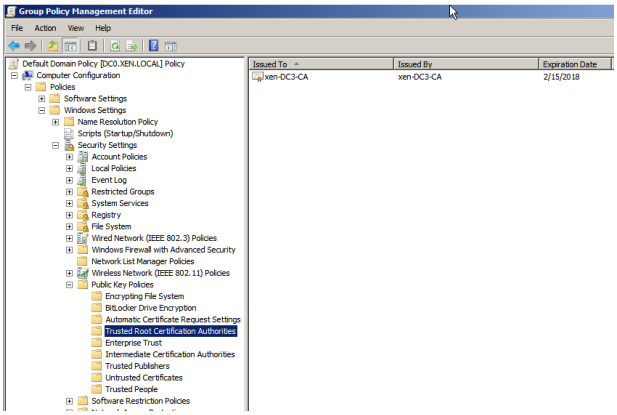


Figure 6: *Using smart card authentication when replacing Web Interface or StoreFront servers with the BIG-IP system*

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. You can request a new certificate if one is missing by right-clicking **Certificates** | **All Tasks** | **Request New Certificate** from the domain controller missing the 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 smart card 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.

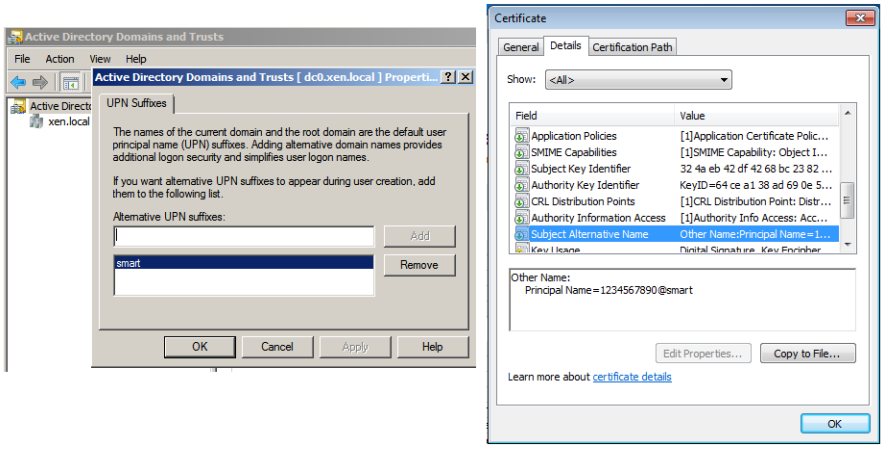
   - *MMC console*
     Open a MMC console, add the **Enterprise PKI** snap-in, right click the **Enterprise PKI** object, and select **Manage AD Containers**.
   - *Command line*
     From the command line issue the following command:
     `certutil.exe -dspublish <filename> NTAuthCA`

7. As required, create an alternate UPN suffix in the domain to match the UPN realm suffix on the smart card.

   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 smart card. Look for the Subject Alternative Name – User Principal Name object in the certificate.



   d. BIG-APM queries the Citrix Active directory sAMAccountName attribute to look up username. Add the correct value to the attribute by using the following guidance:

      - Open the **Active Directory Users and Computers** admin console for the Citrix domain controller.
      - From the **View** menu, select **Advanced Features**.
      - Select the correct User that was issued the smart card certificate.
      - Right-click the user and then click **Properties**.
      - Click Attribute Editor, and then locate the **sAMAccountName** attribute.
      - Double-click the attribute and then add a value (usually an identifiable user name; this value is displayed to the user).

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.

   Warning

   This is a critical step for smart card authentication to work with Windows servers.

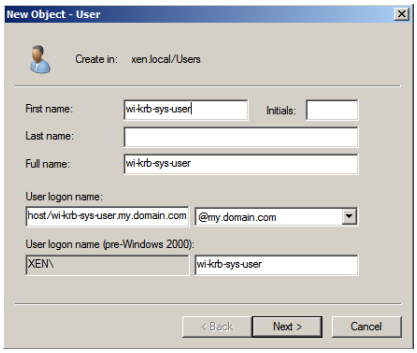
2. Verify that Active Directory DNS is configured with *forward* and *reverse* DNS records.

Configuring the Active Directory SSO service account

***Important:** This section is not necessary if replacing the Web Interface or StoreFront servers with the BIG-IP system. Continue with Citrix configuration on page 41.*

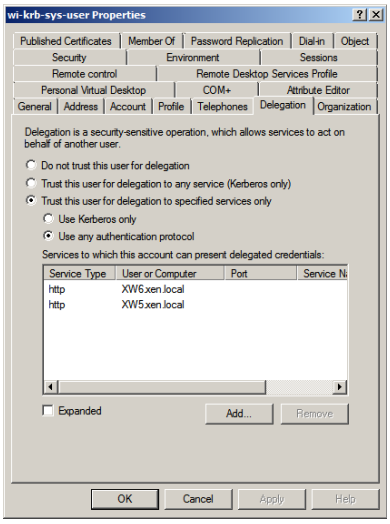
This account is used by APM Kerberos SSO profile to enable Kerberos Protocol Transition and Constrained Delegation to the Web Interface resources.

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 contains the Citrix configuration changes. For specific details on configuring Citrix devices, consult the Citrix documentation.

If replacing Web Interface or StoreFront servers with the BIG-IP system

If you are using the BIG-IP system to replace the Web Interface or StoreFront devices, you must enable SID Enumeration on XenApp and XenDesktop as described in Citrix knowledge articles CTX117489 and CTX129968.

Remember that if you are replacing Web Interface or StoreFront servers, smart card support if is only available in BIG-IP v11.4 or later.

If not replacing Web Interface or StoreFront servers

This section details the steps required to configure the Citrix XML Broker or DDC servers and Web Interface or StoreFront servers.

Configuring the XML Broker or DDC

- 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
```

See *Modifying the Citrix configuration on page 29* for a description of these changes.

Configuring the Web Interface or StoreFront servers

The following section details the configuration of Web Interface or StoreFront and Microsoft IIS. If re-encrypting the traffic from the BIG-IP to the Web Interface or StoreFront, 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 or StoreFront 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 or StoreFront 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. Create a site and enable Kerberos authentication
   This procedure differs depending on whether you are using Web Interface or StoreFront servers. Use the appropriate procedure.
   - **If using Web Interface servers**
     a. *In the Citrix Web Interface Management utility, create a new HTTPS site.*
        - On the Specify Point of Authentication page, select At Web Interface.
        - After setting the XML broker information, on the Configure Authentication Methods page, check the Pass-through box.
     b. *Enable Kerberos authentication:*

- After the site is created, select it from the list.
- Click the Authentication Methods link on the right of the application.
- Verify that Pass-through is the only option checked, and then click the Properties button.
- Under Kerberos Authentication, check the Use Kerberos authentication to connect to servers button.

- **If using StoreFront 2.5 or 2.6 servers**

> ***Note***
>
> *This implementation of smart cards with StoreFront requires domain pass through which is only available on StoreFront 2.5 and later*

a. *In the Citrix Storefront Management utility, create a new site*
   - If using SSL, select and verify in Server Group Base URL is set to use https://yoursite.com
   - Highlight Stores and select Create Store
   - Enter the store name and appropriate DDC information
   - Select None for Remote Access

b. *Enable Kerberos authentication:*
   - Highlight Authentication and select Add/Remove Methods
   - Add Domain pass-through and verify it is enabled
   - Highlight Receiver for Web in main menu and highlight newly created site
   - Select Choose Authentication, check Domain pass-though and uncheck any other available methods.

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 51*

BIG-IP LTM Object	Non-default settings/Notes	
DNS and NTP settings	See *Configuring additional BIG-IP settings on page 70 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. This should be in Canonical Name format. For example, CN=user1,CN=Users,DC=citrix,DC=local,DC=com
	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 **Hostname**: Type the FQDN of the domain controller Click **Add**. Repeat for each domain controller in this configuration.
	Server Pool Monitor	Select the monitor you created above.
	Admin Name[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) ***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 (*Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar)*) Important: Only create a SSO Configuration if you are using Web Interface or StoreFront servers. 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. **Username Parameter Name** **user** **Username Parameter Value** **%{session.sso.token.last.username}** Click **Ok**, and then click **Create** again in the Forms Parameters box. **Parameter Type**[1] Select **Password** from the list. **Password Parameter Name** **password** **Password Parameter Value** **%{session.sso.token.last.password}** Click **Ok**, and then click **Create** again in the Forms Parameters box. **Parameter Type**[1] Select **Custom** from the list **Form Parameter Name** **domain** **Form Parameter Value** **{domain-name-in-NetBIOS-format}**[3] 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) ***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. **Username Parameter Name** **user** **Username Parameter Value** **%{session.sso.token.last.username}** Click **Ok**, and then click **Create** again in the Forms Parameters box. **Parameter Type** Select **Password** from the list. **Password Parameter Name** **password** **Password Parameter Value** **%{session.sso.token.last.password}** Click **Ok**, and then click **Create** again in the Forms Parameters box. **Parameter Type**[1] Select **Custom** from the list. **Form Parameter Name** **domain** **Form Parameter Value** **{domain-name-in-NetBIOS-format}**[3] 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)*) Important: Only create a SSO Configuration if you are using Web Interface or StoreFront 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 StoreFront Servers only)**	
	Name	Type a unique name. We use **StoreFront-SSO**.
	SSO Method	**Forms**
	Use SSO Template	**None**
	Start URI	*If using StoreFront 1.x, 2.0, or 2.1* <URI of StoreFront website>**/authentication/Login*** *If using StoreFront 2.5 or 2.6:* <URI of StoreFront website>**/ExplicitAuth/Login***
	Pass Through	**Enable**
	Form Method	**POST**
	Form Action	***If using StoreFront 1.x, 2.0, or 2.1:*** <URI of StoreFront website>**/authentication/LoginAttempt** ***If using StoreFront 2.5 or 2.6:*** <URI of StoreFront website>**/ExplicitAuth/LoginAttempt**
	Form Parameter for User Name	**username**
	Form Parameter for Password	**password**
	Hidden Form Parameters/Values	**LoginBtn Log+On** **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 or StoreFront 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>
	KDC	Type the IP address of the Citrix data center (optional)
	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
	Note: *if you require HTML5 support, see Creating the Citrix Client Bundle for HTML 5 support on page 46*	
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	If using BIG-IP v11.2/11.3: Type the IP address or Host Name of the destination If using BIG-IP v11.4 or later: Select Citrix XML Broker or DDC Pool
	Port	Type the appropriate port (typically 80 or 443)

[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	
Remote Desktop (*Access Policy-->Application Access-->Remote Desktops*)	***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**
iRule Data Group[1] (*Local Traffic-->iRules-->Data Group List*)	***Data Group for use with the Dynamic Webtop***[1]	
	Name	**APM_Citrix_PNAgentProtocol** **This must be the name of the Data Group for v11.2/11.3**
	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 Web Interface servers or StoreFront servers[1]	
	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/storefront/PNAgent/config.xml**
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
	Logout URI	If you are using Web Interface Servers and want to terminate user sessions when users log off from StoreFront or Web Interface servers, type: **/Citrix/<sitename>Web/auth/loggedout.aspx for Web Interface servers and /Citrix/<store>Web/Authentication/Logoff for storefront servers**
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 56* for instructions.
iRules (*Local Traffic-->Rules*)	Create the iRule using the appropriate iRule definition in *Creating the iRules on page 47*.	

[1] If both data groups are present on the same BIG-IP system, a conflict may occur. Use only the data group required for your implementation.

Creating the Citrix Client Bundle for HTML 5 support

Download the Citrix Receiver for HTML5 from the Citrix website. You add the Citrix Receiver for HTML5 to a Citrix bundle, and then add the bundle to a connectivity profile so BIG-IP APM can deliver the Citrix Receiver for HTML5 to clients. Use the following section for creating and importing the archive onto the BIG-IP system (only required when using F5 Webtops to replace Citrix Storefront servers):

Verify you are running latest HF for BIG-IP versions 11.4.1 or newer

1. Download most current HTML5 client executable from citrix.com.
2. Install the client executable on a supported Windows Server using the default settings.
3. In Windows Explorer, browse to **c:\Program Files\Citrix**.
4. Right-click the **HTML5Client** folder and then from the **Send to** options, select **Compressed (zipped) folder**.
5. From the BIG-IP Configuration utility, on the Main tab, click **Access Policy > Application Access > Remote Desktops > Citrix Client Bundles**, and then click **Create**.
6. In the **Name** field, type a name which includes **html5** in the name.
7. From the **Source** list, select the Windows Package File.
8. Click **Choose File** and upload the **HTML5Client.zip** archive you created in step 4.
9. Click **Finished**.

Once you have created the client bundle, you must associate the bundle with the relevant APM Connectivity profile and allow access to imported files. The way you do this depends on if you are using the iApp to configure the device, or manually configuring the system.

Using the iApp template

Use the following guidance if you are using the iApp template for CItrix.

1. Either open your existing Citrix iApp template Application service, or create a new one.
2. In the question *Which Citrix Client Bundle do you want to use?* select the Citrix bundle you just created

Configuring the BIG-IP APM manually

1. On the Main tab, click **Access Policy > Secure Connectivity**.
   a. Click the Connectivity Profile List tab.
   b. Select the Connectivity profile you want to update.
   c. Click **Edit Profile**. A popup screen opens.
   d. Click **Citrix Client Settings**.
   e. From the **Citrix Client Bundle** list, select the bundle with html5 in its name.
2. On the Main tab, click **Access Policy > Hosted Conten t> Manage Profile Access**
   a. Check the box next to the correct Citrix Access Policy (BIG-IP version 11.6 has filed name “Retain Public Access” above the checkbox.
   b. Click **OK**.

This completes the Citrix Client Bundle configuration.

Creating the iRules

Use this section for guidance on configuring the iRule for this implementation. While this section contains the following five iRules, only create the one iRule appropriate for your configuration.

- *iRule if using Web Interface or StoreFront servers and NOT using smart cards* on this page
- *iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are the same* on this page
- *iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are different on page 48*
- *iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are the same, input required on page 49*
- *iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are different, input required on page 50*

Use the code in one of the following iRules in the iRule Definition, but do not include the line numbers. Replace <store name> with your store name if applicable in the iRule you are using.

iRule if using Web Interface or StoreFront servers and NOT using smart cards

Replace <store name> in lines 5 and 6 with your store name.

```
1  when ACCESS_ACL_ALLOWED {
2     set type [ACCESS::session data get session.client.type]
3     if { !($type starts_with "citrix") } {
4        if { [HTTP::uri] == "/" } {
5           log local0. "Redirecting to /Citrix/<store name>Web/"
6           ACCESS::respond 302 Location "https://[HTTP::host]/Citrix/<store name>Web/"
7        }
8     }
9  }
```

iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are the same

```
# iRule used with Citrix Web Integration or Web Replacement configuration where the certificate uses the same UPN as Citrix Environment
when RULE_INIT {
   # set static::citrix_sf25_DEBUG 1 to enable logging
   set static::citrix_sf25_DEBUG 0
}
# Capture certificate payload and add auto ctrl-alt-delete into payload ("SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n")
when HTTP_RESPONSE_DATA priority 501 {
   if { [string tolower [HTTP::header Content-Type]] contains "application/x-ica" } {
      set payload [ regsub -nocase -line {^SSLEnable=On.*\\n} [HTTP::payload] "SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n" ]
      HTTP::payload replace 0 [HTTP::header Content-Length] $payload
   }
}
# When Access policy event (see VPE) with id "CERTPROC" occurs, certificates universal principle name is extracted from Subject
# Alternative Name into format user@domain
# Session variable session.logon.last.username is set by parsing before @ symbol
# Session variable session.logon.last.domain is set by parsing after @ symbol
# Enable Debug to verify session variable values are correct, log entry will append to /var/log/ltm
when ACCESS_POLICY_AGENT_EVENT {
   switch [ACCESS::policy agent_id] {
      "CERTPROC" {
         if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {
           ACCESS::session data set session.logon.last.username [lindex [split [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 0]
           ACCESS::session data set session.logon.last.domain [lindex [split [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 1]
           if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Certificate extension equals: [ACCESS::session data get session.ssl.cert.x509extension]"}
           if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, User name set as: [ACCESS::session data get session.logon.last.username]"}
           if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Domain name set as: [ACCESS::session data get session.logon.last.domain]"}
           }
        }
    }
}
```

iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are different

```
# iRule used with Citrix Web replacement configuration were the certificate uses a different UPN than Citrix Environment
when RULE_INIT {
   # set static::citrix_sf25_DEBUG 1 to enable logging
   set static::citrix_sf25_DEBUG 0
}
# When Access policy event (see VPE) with id "CERTPROC" occurs, certificates universal principle name is parsed from Subject Alternative Name into format user@domain
# Session variable session.custom.certupn is set to parsed UPN. Variable is then used in ad query (see VPE) to acquire sAMAccount attribute in AD
# Enable Debug to verify variable value is correct, log entry will append to /var/log/ltm
# When Access policy event (see VPE) with id "SAMNAME" occurs, variable session.logon.last.username is set to returned AD sAMAccountName
# Enable Debug to verify returned sAMAcount name
# session.logon.last.username is used to logon to xml broker or DDC (defined in Citrix Remote desktop profile) using SID Enumeration
when ACCESS_POLICY_AGENT_EVENT {
   switch [ACCESS::policy agent_id] {
      "CERTPROC" {
         if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {
            ACCESS::session data set session.custom.certupn [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"]
            if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Subject Alternative Name returned in cert: [ACCESS::session data get session.custom.certupn]"}
            }
         }
      "SAMNAME" {
         ACCESS::session data set session.logon.last.username [ACCESS::session data get "session.ad.last.attr.sAMAccountName"]
         if {$static::citrix_sf25_DEBUG} {log local0. "Event SAMNAME, Active Directory sAMAcount name is: [ACCESS::session data get session.logon.last.username]"}
      }
   }
}
```

iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are the same, input required

Replace <store name> in lines 34 and 35 with your store name.

```
1  ## iRule used with Citrix Web Integration or Web Replacement configuration were the certificate uses the same UPN as Citrix Environment
2  when RULE_INIT {
3     # set static::citrix_sf25_DEBUG 1 to enable logging
4     set static::citrix_sf25_DEBUG 0
5  }
6  # Capture certificate payload and add auto ctrl-alt-delete into payload ("SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n")
7  when HTTP_RESPONSE_DATA priority 501 {
8     if { [string tolower [HTTP::header Content-Type]] contains "application/x-ica" } {
9        set payload [ regsub -nocase -line {^SSLEnable=On.*\\n} [HTTP::payload] "SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n" ]
10       HTTP::payload replace 0 [HTTP::header Content-Length] $payload
11    }
12 }
13 # When Access policy event (see VPE) with id "CERTPROC" occurs, certificates universal principle name is extracted from Subject Alternative Name into format user@domain
14 # Session variable session.logon.last.username is set by parsing before @ symbol
15 # Session variable session.logon.last.domain is set by parsing after @ symbol
16 # Enable Debug to verify session variable values are correct, log entry will append to /var/log/ltm
17 when ACCESS_POLICY_AGENT_EVENT {
18    switch [ACCESS::policy agent_id] {
19       "CERTPROC" {
20          if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {
21             ACCESS::session data set session.logon.last.username [lindex [split [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 0]
22             ACCESS::session data set session.logon.last.domain [lindex [split [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"] "@"] 1]
23             if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Certificate extension equals: [ACCESS::session data get session.ssl.cert.x509extension]"}
24             if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, User name set as: [ACCESS::session data get session.logon.last.username]"}
25             if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Domain name set as: [ACCESS::session data get session.logon.last.domain]"}
26          }
27       }
28    }
29 }
30 when ACCESS_ACL_ALLOWED {
31    set type [ACCESS::session data get session.client.type]
32    if { !($type starts_with "citrix") } {
33       if { [HTTP::uri] == "/" } {
34          log local0. "Redirecting to /Citrix/<store name>Web/"
35          ACCESS::respond 302 Location "https://[HTTP::host]/Citrix/<store name>Web/"
36       }
37    }
38 }
```

iRule if replacing Web Interface/StoreFront servers and using smart cards; cert and Citrix domain (UPNs) are different, input required

Replace <store name> in lines 21 and 22 with your store name.

```
1  # iRule used with Citrix Web Integration or StoreFront Integration configuration were the certificate uses a different UPN than the
2    Citrix Environment
3  when RULE_INIT {
4     # set static::citrix_sf25_DEBUG 1 to enable logging
5     set static::citrix_sf25_DEBUG 0
6  }
7  # Capture certificate payload and add auto ctrl-alt-delete into payload ("SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n")
8  when HTTP_RESPONSE_DATA priority 501 {
9     if { [string tolower [HTTP::header Content-Type]] contains "application/x-ica" } {
10       set payload [ regsub -nocase -line {^SSLEnable=On.*\\n} [HTTP::payload] "SSLEnable=On\r\nDisableCtrlAltDel=Off\r\n" ]
11       HTTP::payload replace 0 [HTTP::header Content-Length] $payload
12    }
13 }
14 # Enable Debug to verify returned sAMAcount name
15 when ACCESS_ACL_ALLOWED {
16    ACCESS::session data set session.logon.last.username [ACCESS::session data get "session.ad.last.attr.sAMAccountName"]
17    if {$static::citrix_sf25_DEBUG} {log local0. "Access policy has finished and user is allowed, sAMAcount name set as: [ACCESS::session data get session.logon.last.username]"}
18    set type [ACCESS::session data get session.client.type]
19       if { !($type starts_with "citrix") } {
20          if { [HTTP::uri] == "/" } {
21             log local0. "Redirecting to /Citrix/<store name>Web/"
22             ACCESS::respond 302 Location "https://[HTTP::host]/Citrix/<store name>Web/"
23          }
24       }
25 }
26 # Session variable session.custom.certupn is set to extracted UPN. Variable is then used in ad query (see VPE) to acquire sAMAccount attribute in AD
27 # Enable Debug to verify sesion variable values are correct, log entry will append to /var/log/ltm
28 when ACCESS_POLICY_AGENT_EVENT {
29    switch [ACCESS::policy agent_id] {
30       "CERTPROC" {
31          if { [ACCESS::session data get session.ssl.cert.x509extension] contains "othername:UPN<" } {
32             ACCESS::session data set session.custom.certupn [findstr [ACCESS::session data get session.ssl.cert.x509extension] "othername:UPN<" 14 ">"]
33             if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, Certificate extension equals: [ACCESS::session data get session.ssl.cert.x509extension]"}
34             if {$static::citrix_sf25_DEBUG} {log local0. "Event CERTPROC, certupn equals: [ACCESS::session data get session.custom.certupn]"}
35             }
36          }
37     }
38 }
```

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***		
	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		
	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 54* 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**		
Profiles (*Local Traffic-->Profiles*)	***HTTP***	Parent Profile	**http**
		Insert X-Forwarded-For	**Enabled**
		Redirect Rewrite	**Matching**
		Request Header Erase *(only if using StoreFront or WebInterface servers with APM)*	**Accept-Encoding**

BIG-IP LTM Object	Non-default settings/Notes		
Profiles (*Local Traffic-->Profiles*)	***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:* Select the Web Interface pool you created *If you **are** replacing the Web Interface servers with BIG-IP:* 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	
	VDI & Java Support *(in v11.4 and later)*	Check **Enable** (This is not necessary if using BIG-IP version 11.6 or later).	
	VDI Profile	11.6 and later only: Select either the default VDI profile, or the VDI 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 *(in v11.2/11.3 only)*	Check the box to enable Citrix support
	XML Broker Virtual Server (not necessary if using Dynamic Webtops with v11.4 and later)	
	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 **Auto Map**[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 **Auto Map**[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 **Auto Map**
	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. Use one of the following procedures:

- *Editing the Access Profile with the Visual Policy Editor when using F5 Dynamic Webtops to replace Web Interface servers* on this page.
- *Editing the Access Profile with the VPE when using Web Interface servers or StoreFront servers on page 58*
- *Editing the Access Profile with the Visual Policy Editor when using Web Interface servers with smart card authentication on page 61*
- *Editing the Access Profile with the Visual Policy Editor when replacing Web Interface or StoreFront servers with the BIG-IP system and using smart card authentication on page 63*

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 **Client Type** option button (if using v11.4 or later, click the End Point Security (Server-Side) tab) and then click **Add item**.
   a. In the **Name** field, you can type a new name. In our example, we use **Client Pre-Check**.
   b. Click the Branch Rules tab.
   c. Delete all of the default branches by clicking the **x** button on the right side of each row.
   d. Click the **Add Branch Rule** button.
   e. In the **Name** field, type **Browser or Citrix Receiver**.
   f. Click the **change** link, and then click the Advanced tab.
   g. In the Advanced box, type (or copy and paste) the following expression:
   ```
   expr { [mcget {session.ui.mode}] == 0 || [mcget {session.ui.mode}] == 9 || [mcget {session.ui.mode}] == 6 || [mcget {session.client.type}] == "citrix-agee" || [mcget {session.client.type}] == "citrix-pnagent" }
   ```
   h. Click **Finished** and then click **Save**.
5. Click the **+** symbol between **Client Pre-Check** and **Deny**. A box opens with options for different actions.
6. Click the **Logon Page** option button, and then click **Add Item**.
   a. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
   b. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. The options box opens.
8. Click the **Variable Assign** option button (if using v11.4 or later, click the Assignment tab) and then click **Add Item**.
   a. In the Name box, type **Domain Variable Assign**.
   a. Click **Add new entry**, and then click the **change** link.
   b. In the **Custom Variable** box, type **session.logon.last.domain**.

c. In the **Custom Expression** box, type **`Add expr { "<domain>" }`** where *<domain>* is your NetBIOS domain name for authenticating Citrix users.

d. Click **Finished** and then click **Save**.

9. Click the **+** symbol between **Domain Variable Assign** and **Deny**. The options box opens.
10. Click the **AD Auth** option button (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
    a. From the **Server** list, select the AAA Server you created using the table above. In our example, we select **Citrix_domain**.
    b. 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 **Advanced Resource Assign** (Full Resource Assign prior to v11.4) option button (if using v11.4 or later, click the Assignment tab), and then click **Add Item**.
    a. Click **Add new entry**.
    b. Click the **Add/Delete** link on the new entry.
    c. Click Remote Desktop Resources tab.
    d. Check the box for the Remote Desktop top profile you created using the table.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop profile you created using the table.
    g. Click **Update**
    h. Click the **Save** button.
13. On the fallback path between **Full Resource Assign** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
14. *Optional configuration to support two factor authentication with RSA SecurID.*
    If you are not using two factor authentication with RSA SecurID, continue with #15.
    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**.

15. 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.
16. 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.

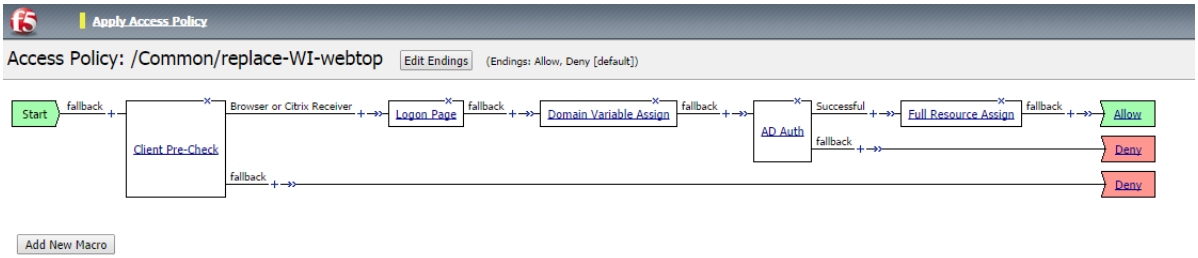


Figure 7: *Access Policy without two factor authentication*

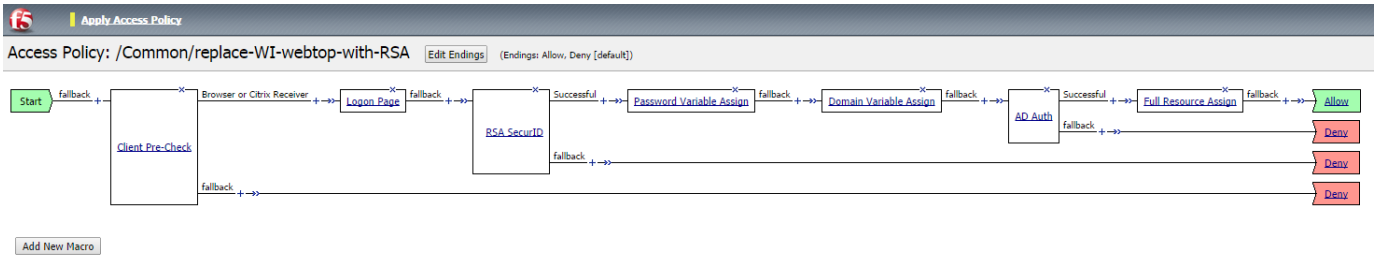


Figure 8: *Access Policy including two factor authentication*

Editing the Access Profile with the VPE when using Web Interface servers or StoreFront servers

Use this procedure if you are not using Dynamic Presentation Webtops to replace the Web Interface or StoreFront 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 **Client Type** option button (if using v11.4 or later, click the End Point Security (Server-Side) tab) and then click **Add item**.
   a. In the **Name** field, you can type a new name. In our example, we use **Client Pre-Check**.
   b. Click the Branch Rules tab.
   c. Delete all of the default branches by clicking the **x** button on the right side of each row.

d. Click the **Add Branch Rule** button.

e. In the **Name** field, type **Browser or Citrix Receiver**.

f. Click the **change** link, and then click the Advanced tab.

g. In the Advanced box, type (or copy and paste) the following expression:
```
expr { [mcget {session.ui.mode}] == 0 || [mcget {session.ui.mode}] == 9 || [mcget {session.ui.mode}] == 6 || [mcget {session.client.type}] == "citrix-agee" || [mcget {session.client.type}] == "citrix-pnagent" }
```

h. Click **Finished** and then click **Save**.

5. Click the **+** symbol between **Client Pre-Check** and **Deny**. A box opens with options for different actions.
6. Click the **Logon Page** option button, and then click **Add Item**.
   a. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
   b. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. The options box opens.
8. Click the **AD Auth** option button (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
   a. From the **Server** list, select the AAA Server you created using the table above. In our example, we select **Citrix_domain**.
   b. Configure the rest of the Active Directory options as applicable, and then click **Save**.
   You now see two paths, **Successful** and **Fallback**.
9. Click the **SSO Credential Mapping** option button (if using v11.4 or later, click the Assignment tab), and then click **Add Item**.
   a. Configure the Properties as applicable for your configuration. Use the following example to include a default domain:
   b. From the **SSO Token Username** list, select **Custom**.
   c. In the field under Custom, type **`expr {"<domain>\\[mcget {session.logon.last.username}]"}`** where you replace <domain> with the NetBIOS domain you want to include.
   d. Click the **Save** button.
10. Click the **+** symbol between **SSO Credential Mapping** and **Deny**. The options box opens.
11. Click the **Variable Assign** option button (if using v11.4 or later, click the Assignment tab) and then click **Add Item**.
    a. In the **Name** box, type **Domain Variable Assign**. If using Citrix Secure Ticket Authority (STA) type **STA Variable Assign**.
    b. Click **Add new entry**, and then click the **change** link.
    c. In the **Custom Variable** box, type **session.logon.last.domain**.
    d. In the **Custom Expression** box, type **`Add expr { "<domain>" }`** where *<domain>* is your NetBIOS domain name for authenticating Citrix users.
    e. *For STA/Direct Gateway support only, perform the following:*
       - Click **Add new entry**, and then click the **change** link.
       - In the Custom Variable box, type session.citrix.sta_servers
       - In the **Custom Expression** box, type **`Add expr {"<URL for STA server>"}`** where *<URL for STA server>* is the URL for your Citrix Secure Ticket Authority. Use a semicolon to delineate between servers, for example:
         `expr {"https://server1.mydomain.com/scripts/ctxsta.dll;https://server2.mydomain.com/scripts/ctxsta.dll"}`
    f. Click **Finished** and then click **Save**.
12. Click the **+** symbol between **Domain Variable Assign** and **Deny**.

13. Click the **Client Type** option button (if using v11.4 or later, click the End Point Security (Server-Side) tab) and then click **Add item**.
    a. In the **Name** field, you can type a new name. In our example, we use **Client Post-Check**.
    b. Click the Branch Rules tab.
    c. Delete all of the default branches by clicking the **x** button on the right side of each row.
    d. Click the **Add Branch Rule** button.
    e. In the **Name** field, type **Citrix Receiver**.
    f. Click the **change** link, and then click the Advanced tab.
    g. In the Advanced box, type (or copy and paste) the following expression:
    `expr { [mcget {session.client.type}] == "citrix-agee" || [mcget {session.client.type}] == "citrix-pnagent" }`
    h. Click **Finished**.
    i. Click the **Add Branch Rule** button.
    j. In the **Name** field, type **Full or Mobile Browser**.
    k. Click the **change** link, and then click the Advanced tab.
    l. In the Advanced box, type (or copy and paste) the following expression:
    `expr { [mcget {session.ui.mode}] == 0 || [mcget {session.ui.mode}] == 9 || [mcget {session.ui.mode}] == 6 }`
    m. Click **Finished** and then click **Save**.
14. On the Citrix Receiver path between **Client Post-Check** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
15. On the Full or Mobile Browser path between **Client Post-Check** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
16. *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**.
    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**, and then click **Save**.
    h. At the start of the VPE, click the **Logon Page** link/box.
    i. In row #2, perform the following:
    - In the **Post Variable Name** box, type **password1**.
    - In the **Session Variable Name** box, type **password1**.
    j. 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**.
    k. Under Customization, in the **Logon Page Input Field #3** box, type **Passcode**.
    l. Click **Save**.
    m. Click the **+** symbol between **Logon Page** and **Variable Assign**.

n. Click the **RSA SecurID** option button and then click **Add Item**.

o. From the **AAA Server** list, select the RSA SecurID AAA Server you created using the configuration table.

p. From the **Change Max Logon Attempts Allowed** list, select **1**.

q. Click **Save**.

17. Click the yellow Apply Access Policy link in the upper left part of the window, and then click the **Close** button on the upper right.

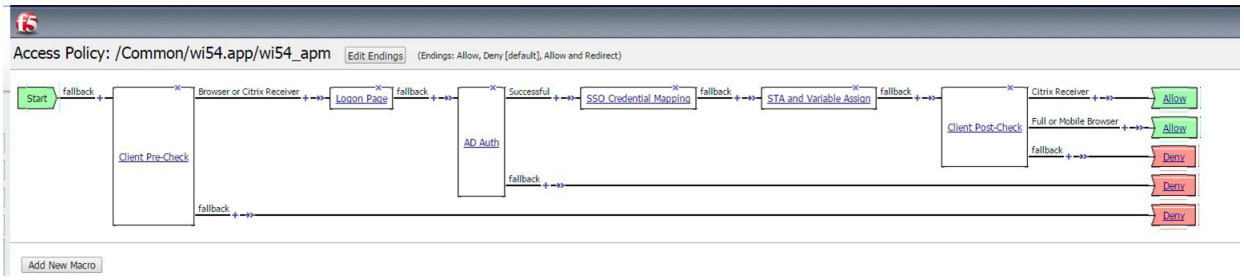


Figure 9: *VPE when using Web Interface or StoreFront servers and no RSA with optional STA*

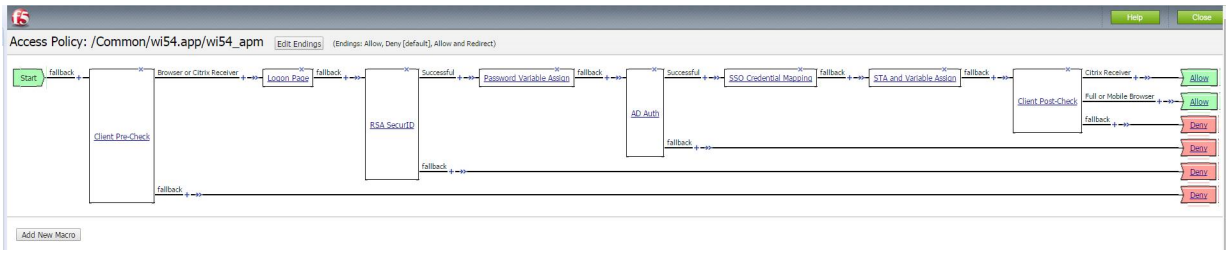


Figure 10 *VPE when using Web Interface or StoreFront servers with RSA SecurID with optional STA*

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 (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
   a. From the **Auth Mode** list, select **Require**.
   b. Click the **Save** button.
5. Click the **+** symbol between **On-Demand Cert Auth** and **Deny**. The options box opens
6. Click the **iRule Event** option button (if using v11.4 or later, click the General Purpose tab), and then click **Add Item**.
   a. In the **Name** box, you can type a name, such as iRule Event **CERTPROC**.
   b. In the **ID** field, type **CERTPROC**.
   c. Click **Save**.

7. On the fallback path between **iRule Event** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
8. *Optional configuration to support different UPNs*
    a. Click the + symbol on the fallback path between iRule Event and allow. A box opens with options for different actions.
    b. Click the **AD Query** option button (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
    c. From the **Server** list, select the AD server you created.
    d. In the Search Filter box, type **userPrincipalName=%{session.custom.certupn}**
    e. Click **Add new entry**.
    f. In the **Required Attributes (optional)** box, type **sAMAccountName**.
    g. Click the Branch Rules tab and delete the existing rule.
    h. Click **Save**.
    i. Click the **+** symbol between **AD Query** and **Allow**. The options box opens
    j. Select **Variable Assign** option button (if using v11.4 or later, click the Assignment tab), and then click **Add item**.
    k. Click **Add new entry**.
    l. Click the **Change** link.
    m. In the **Custom Variable** box, type **session.logon.last.domain**.
    n. In the **Custom Expression** box, type **expr { "<netbios domain>" }**.
    o. Click **Finished**.
    p. Click **Save**.
9. Click the yellow Apply Access Policy link in the upper left part of the window, and then click the **Close** button on the upper right.

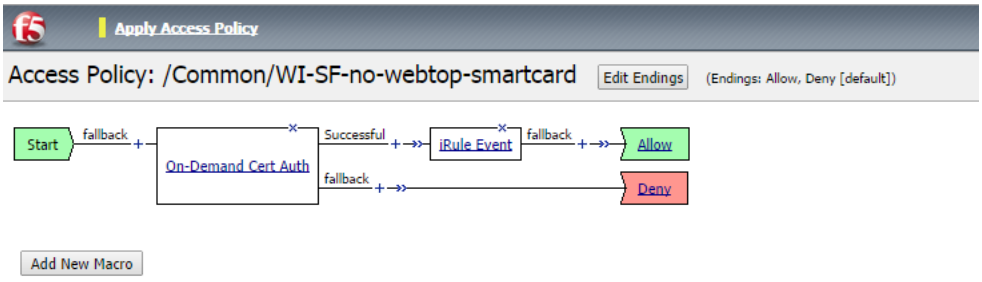


Figure 11 *VPE when using Web Interface or StoreFront servers with smart cards and same UPN*

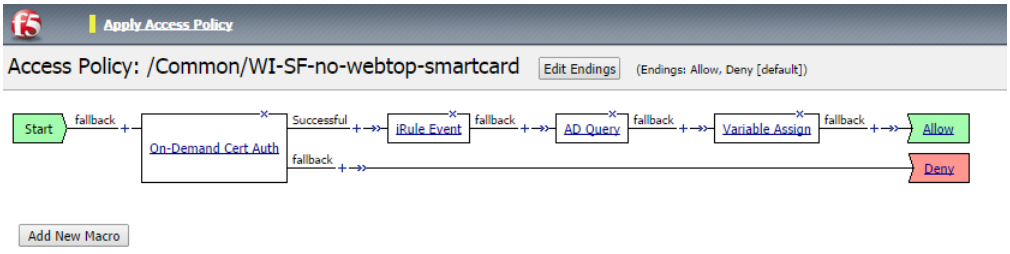


Figure 12 *VPE when using Web Interface or StoreFront servers with smart cards and different UPNs*

Editing the Access Profile with the Visual Policy Editor when replacing Web Interface or StoreFront servers with the BIG-IP system and using smart card authentication

Use this procedure if you are replacing the Web Interface or StoreFront 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 (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
    a. From the **Auth Mode** list, select **Require**.
    b. Click the **Save** button.
5. On the Successful path between **On-Demand Cert Auth** and **Deny**, click the **+** symbol. The options box opens
6. Click the **iRule Event** option button (if using v11.4 or later, click the General Purpose tab), and then click **Add Item**.
    a. In the **Name** box, you can type a name, such as **iRule Event CERTPROC**.
    b. In the **ID** field, type **CERTPROC**.
    c. Click **Save**.
7. *Optional configuration to support different UPNs. If using the same UPN, continue with #8.*
    a. Click the **+** symbol on the path between **iRule Event** and **Deny**. A box opens with options for different actions.
    b. Click the **AD Query** option button (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
    c. From the **Server** list, select the AD server you created.
    d. In the Search Filter box, type **userPrincipalName=%{session.custom.certupn}**
    e. Click **Add new entry**.
    f. In the **Required Attributes (optional)** box, type **sAMAccountName**.
    g. Click the Branch Rules tab and delete the existing rule.
    h. Click **Save**.
    i. Click the **+** symbol between **AD Query** and **Deny**. The options box opens.
    j. Click the **iRule Event** option button (if using v11.4 or later, click the General Purpose tab), and then click **Add Item**.
    k. In the **Name** box, you can type a name, such as **iRule Event SAMENAME**.
    l. In the **ID** field, type **SAMENAME**.
    m. Click **Save**.
    n. Click the **+** symbol between **iRule Event** and **Deny**. The options box opens.
    o. Select **Variable Assign** option button (if using v11.4 or later, click the Assignment tab), and then click **Add item**.
    p. Click **Add new entry**.
    q. Click the **Change** link.
    r. In the **Custom Variable** box, type **session.logon.last.domain**.

s. In the **Custom Expression** box, type **expr { "<netbios domain>" }**.

t. Click **Finished**, and then click **Save**.

8. Click the **+** symbol between **iRule Event CERTPROC** and **Deny** (or between **Variable Assign** and **Deny** if you used the optional configuration for supporting different UPNs in #7). The options box opens.
9. Click the **Advanced Resource Assign** (Full Resource Assign prior to v11.4) option button (if using v11.4 or later, click the Assignment tab), and then click **Add Item**.
   a. Click **Add new entry**.
   b. Click the **Add/Delete** link on the new entry.
   c. Click Remote Desktop tab.
   d. Check the box for the Remote Desktop profile you created using the table.
   e. Click the Webtop tab.
   f. Click the option button for the Webtop profile you created using the table.
   g. Click **Update**, and then click the **Save** button.
10. On the path between **Advanced Resource Assign** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
11. Click the yellow Apply Access Policy link in the upper left part of the window, and then click the **Close** button on the upper right.

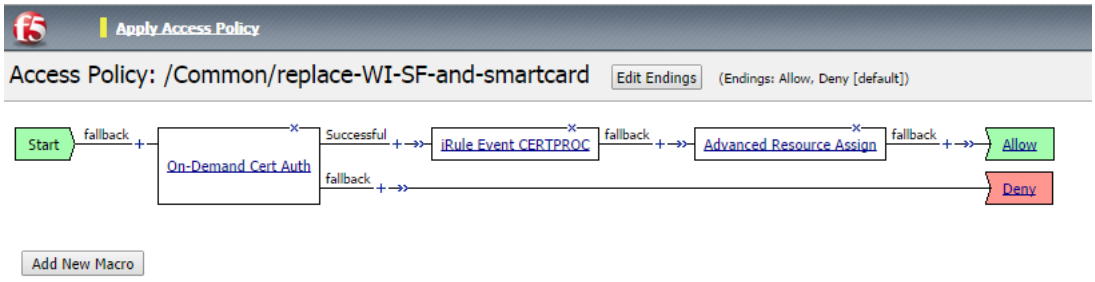


Figure 13 *VPE when replacing Web Interface or StoreFront servers with the BIG-IP system, using smart cards and same UPN*

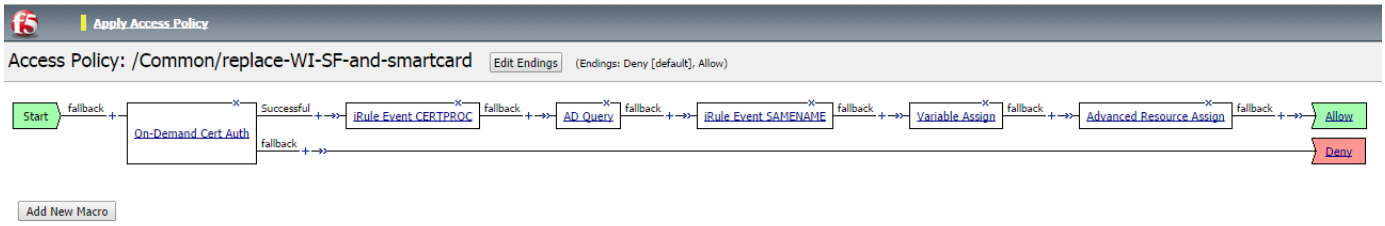


Figure 14 *VPE when replacing Web Interface or StoreFront servers with the BIG-IP system, using smart cards and different UPNs*

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

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

Network Firewall settings

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

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

Use the following guidance to configure the AFM for Citrix implementations. Note that if you are using Web Interface or StoreFront Servers in your Citrix environment, you will need to create two Network Firewall Policies as shown in the following procedure.

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

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

k. If necessary, from the **Action** list, select **Accept**.

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

m. Click **Finished**.

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

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

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

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

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

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

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

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

h. From the **Protocol** list, select **Any**.

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

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

k. If you configured a logging profile as described in *Optional: Configuring the BIG-IP system to log network firewall events on page 67*, from the **Logging** list, select **Enabled**. We recommend logging for this rule.

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

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

4. ***If you are using Web Interface or StoreFront servers only:*** Create an additional Network Firewall Policy:

a. From the Configuration utility, click **Security > Network Firewall > Policies**, and then click **Create**.

b. In the **Name** field, type a unique name for the policy, such as **Citrix--WI-SF-Policy**, and then click **Finished**.

c. Return to Step #2 and repeat that section to create a new rule to allow authorized hosts or networks to connect. Important: protocol.....In Step 2i, specify the addresses of the StoreFront or Web Interface servers. All other steps are identical.

d. Return to Step #3 and repeat that section to create a rule to block all other traffic. There are no changes.

5. Apply Your Firewall Policy to your Virtual Server

a. Click **Local Traffic > Virtual Servers**.

b. From the list, select the HTTP virtual server you created.

c. On the menu bar, click **Security > Policies**.

d. In the **Network Firewall** row, from the **Enforcement** list, select **Enabled**, and then select the first policy you created.

e. Click **Update**.

f. Repeat steps a-e for any of the following virtual servers you created: HTTPS, ICA Forwarding, ICA forwarding using Remote Desktop, and ICA Forwarding with Multi-stream.

g. If you created the second policy for the Web Interface or StoreFront servers, repeat steps a-e on the XML Broker and XML Broker Enumeration virtual server, selecting the appropriate policy in step d.

h. Click **Finished**.

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

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

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

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

To assign the IP intelligence policy to the Citrix virtual server

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

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

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

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

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

Creating the logging profile using the iApp template

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

To configure the logging profile iApp

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

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

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

Note

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

Creating logging profile manually

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

To manually configure a logging profile

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

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

2. Log into the BIG-IP system using the command line. Enter the tmsh shell, by typing **tmsh** from the prompt.
3. Create a Remote High Speed Log (HSL) destination:

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

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

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

5. Create a log publisher:

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

6. Create the logging profile to tie everything together.
   If you chose to log allowed connections, include the green text (as in step 2 substep l in *To configure the BIG-IP AFM to allow connections from a single trusted network on page 65)*.
   If you set the rule to drop incoming connections, include the text in blue.
   If you chose to log IP intelligence events, include the text in red to add the parameter that sets the log publisher.

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

Assigning the logging profile to the virtual server

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

To assign the logging profile to the Citrix virtual server

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

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 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
1.0	New deployment guide for App template version f5.citrix_vdi.v2.1.0rc1 which includes the following new features: - Added support for XenApp/XenDesktop 7.6 - Added support for StoreFront 2.6 - Added Citrix STA (Secure Ticket Authority) configuration - Added the option to include a customized caption for Remote Desktop objects - Added BIG-IP Advanced Firewall Configuration - Increased the minimum BIG-IP version for the iApp to 11.4	12-16-2014
1.1	- Modified the section *Creating the Citrix Client Bundle for HTML 5 support on page 46* with updated instructions. - Added two new troubleshooting entries: *Users are unable to load published resources when using the HTML5 client on page 34* and *Application resources do not properly launch when using the HTML5 client with Google Chrome on page 34*	02-26-2015

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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