



Deploying the BIG-IP APM v11 with Citrix XenApp or XenDesktop

What's inside:

- 2 Prerequisites and configuration notes
- 3 Configuration example
- 4 Traffic flow
- 5 Preparation worksheet
- 5 Configuring the DNS settings
- 6 Configuring the NTP settings
- 6 Downloading and importing the APM iApp for XenApp and XenDesktop
- 7 Getting Started with the APM iApp for Citrix XenApp or XenDesktop
- 10 Next Steps
- 11 Modifying the BIG-IP LTM configuration (optional)
- 13 Manually configuring the BIG-IP APM for XenApp or XenDesktop
- 16 Document Revision History

Document Version

1.2

Welcome to the BIG-IP APM deployment guide for Citrix® XenApp™ or XenDesktop™. With the combination of BIG-IP Access Policy Manager (APM) version 11 and Citrix XenApp or XenDesktop, organizations can deliver a complete remote access solution that allows for scalability, security, compliance and flexibility.

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 APM module, along with the BIG-IP LTM module, secures and scales the environment. 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.

For more information on the F5 BIG-IP system, see <http://www.f5.com/products/big-ip>

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

Products and versions tested

Product	Version
BIG-IP APM	11.0
Citrix XenApp	5.0 and 6.0
Citrix XenDesktop	5.0

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

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.

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:

- ▶ You must have an existing BIG-IP LTM deployment for either Citrix XenApp or XenDesktop before running this iApp.
If you do not have an existing LTM deployment, see the following BIG-IP version 11 deployment guides for running the LTM iApps:
 - » XenApp: <http://www.f5.com/pdf/deployment-guides/citrix-xenapp-iapp-dg.pdf>.
 - » XenDesktop: <http://www.f5.com/pdf/deployment-guides/citrix-xendesktop-dg.pdf>.
- ▶ The configuration of this iApp depends on whether your LTM configuration is on the same physical BIG-IP device as the APM you are configuring, or if it is on a separate device.
 - » *Same physical BIG-IP device*
If your LTM configuration is on the same BIG-IP device on which you are configuring this APM iApp, you will enter the individual IP address of your Web Interface servers when prompted in this iApp, and the BIG-IP system creates a new virtual server. In this scenario, your existing LTM virtual server for the Citrix Web Interface servers will go unused.
 - » *Separate devices for LTM and APM*
If your LTM configuration is on a separate physical device than the APM iApp you will be creating, you will enter the existing IP address of your BIG-IP LTM Web Interface virtual server when prompted in this iApp.
- ▶ This deployment guide configures the BIG-IP system to terminate SSL connections on the APM. When you configured the BIG-IP *LTM* for XenApp or XenDesktop, you may have configured the BIG-IP LTM for offloading SSL. If you configured the BIG-IP LTM to offload SSL, you have two options in your APM configuration.
 - » *Re-encrypt to the LTM*
Using the default configuration in this guide, the BIG-IP APM re-encrypts connections before sending them to the BIG-IP LTM. No modification to the BIG-IP LTM configuration is necessary.
 - » *SSL Offload (unencrypted connections between the APM and LTM)*
If you want the BIG-IP APM to offload SSL connections, and have previously configured the LTM for offload, you must modify your BIG-IP LTM configuration for XenApp or XenDesktop to listen on port 80 and not port 443. See *Modifying the BIG-IP LTM configuration (optional)* on page 11.
- ▶ This iApp template configures objects in the Common partition. After configuring the iApp, you can find the individual objects only in the Common partition.
- ▶ This deployment guide provides guidance for using a downloadable iApp for BIG-IP APM and Citrix XenApp or Desktop. Future versions of the BIG-IP system will include this iApp by default.
- ▶ Session Reliability on the Citrix backend servers is supported, but not required. The configuration described in this guide is valid whether Session Reliability is enabled or disabled on the backend servers.
- ▶ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system. For more information, see the BIG-IP LTM documentation.
- ▶ 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.

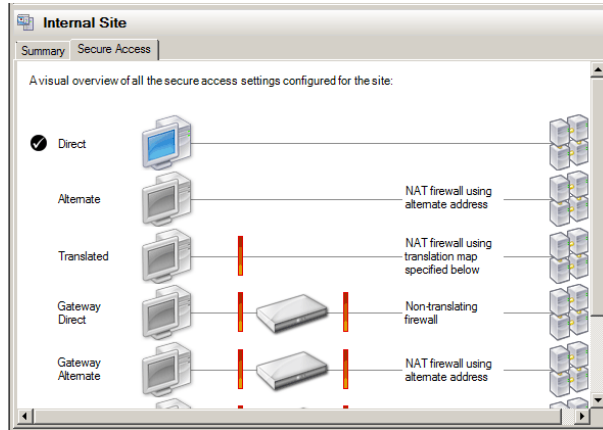
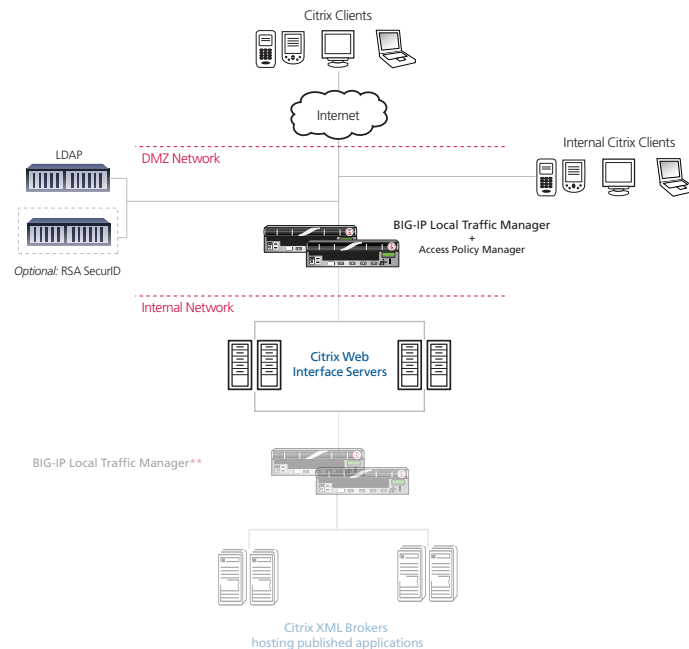


Figure 1: Citrix Session configuration

Configuration example

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 Proxy mode. In secure proxy mode, no F5 BIG-IP APM client is required for network access. 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 directory 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.



** The BIG-IP LTM configuration is shown in this diagram for completeness

Traffic flow

This section describes the connection flow from a user perspective and then from the administrator's perspective.

Secure Proxy user traffic flow

In the Secure Proxy mode, the user experience takes the following path:

1. The user enters a Virtual Address such as `https://citrix.example.com`.
2. The user is prompted for a user name and password by a customizable login screen on the BIG-IP APM, and enters his or her credentials.
3. The user is logged into Citrix XenApp/XenDesktop.
4. If the user has never logged into the site or does not have the Citrix client, the user is prompted to download and install the client.
5. The user is presented with the list of available applications.

Secure Proxy administrative traffic flow

In the Secure proxy mode, the administrator has total control over the compliance, security, scalability and TCP connections of the Citrix session.

1. The user enters a Virtual Address such as `https://citrix.example.com`. This request is answered by the BIG-IP APM. The APM provides SSL offload, terminating the SSL connection, reducing resource usage on the Active Directory and the Citrix Servers.
2. Optionally at this step, additional compliance and security checks may be carried out through the Visual Policy Editor (VPE™). For example, the APM can store for future evaluation whether the user is from a certain geographic region or whether the user has the correct browsers and be redirected to appropriate landing pages.
3. Once the user enters credentials, the BIG-IP APM contacts Active Directory and authenticates the user's credentials. Once the user is authenticated, appropriate cookies are transmitted to the user's browser to create session states. This authentication is then transparently (to the user) passed to the Citrix login form and the user is logged in. The user only ever sees the single login page.
4. The BIG-IP APM checks the user's access against the configured policy to determine the capabilities of the client's browser. If the Citrix client is not installed, the user is prompted to download and install the client. BIG-IP APM's single-sign-on policy ensures the user does not have to login again because the user's credentials are cached and presented to the Citrix server when needed.
5. The administrator now has total control with the BIG-IP system to scale, secure, accelerate and optimize the connections from users to Citrix.

Preparation worksheet

For each section of the iApp Template, you need to gather some information, such as virtual server IP addresses and authentication information. This worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages. You might find it useful to print this table and then enter the information.

IP Address	SSL Offload	Citrix Web Interface URI	Health Monitor	Authentication
Virtual server IP address. (this is the address remote clients use to connect for Citrix access):	You must have imported a certificate and key into the BIG-IP system before running the template. Certificate: Key:	If the URI of your Web Interface implementation has been customized from the default (/Citrix/XenApp for XenApp and /Citrix/DesktopWeb for XenDesktop), you need this URI for the template Customized URI If applicable:	User account that retrieve applications from XenApp or XenDesktop: Associated password: Name of the Site or Desktop Farm: Windows domain for the specified user account:	Username to bind with Active Directory if anonymous binds are not supported: Associated password: FQDN of your Active Directory: IP address of the Active Directory Domain Controller:
If using separate physical BIG-IP devices for LTM/APM: IP address and port of your existing BIG-IP LTM Web Interface virtual server:				
If using the same BIG-IP device for LTM/APM: IP addresses of your Web Interface servers:				

Configuring the DNS settings

The first task is to configure the DNS settings on the BIG-IP system to point to the Active Directory server.

➤ **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 Route to the Active Directory server. 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 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**.

Downloading and importing the APM iApp for XenApp and XenDesktop

The first task is to download the iApp for BIG-IP APM and Citrix XenApp or XenDesktop from DevCentral and import it onto the BIG-IP system. Future versions of the BIG-IP system will contain this iApp by default. Be sure you are downloading the most recent version, currently found in the file **citrix_xenapp_xendesktop_apm.2011-11-18.zip** file.

To download and import the iApp from DevCentral

1. Open a web browser and go to <http://devcentral.f5.com/wiki/iApp.Citrix-XenApp-XenDesktop-APM-Template.ashx>
2. Download the **citrix_xenapp_xendesktop_apm.2011-11-18.zip** file to a location accessible from your BIG-IP system.
You must download the file, and not copy and paste the contents. F5 has discovered the copy paste operation does not work reliably.
3. Extract (unzip) the **citrix_xenapp_xendesktop_apm.tmpl** file, and read the README file to learn about the new version of the template.
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

Important



Configuring the APM iApp for Citrix XenApp or XenDesktop

To begin the XenApp or XenDesktop iApp Template, use the following procedure.

1. On the Main tab, expand **iApp**, and then click **Application Services**.
2. Click **Create**. The Template Selection page opens.
3. In the **Name** box, type a name. In our example, we use **Citrix-APM_**.
4. From the **Template** list, select **f5.citrix_xenapp_xendesktop_apm.2011-11-18**. The iApp for APM and XenApp and XenDesktop 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.

Important



If you plan on using Device and Traffic Groups with the iApp for Citrix, you must have configured the Device Group and Traffic Group before beginning the iApp. For more information on Device Management, see the Online help or product documentation.

1. **Configure Device and Traffic Groups?**

If you want to configure the Application for Device and Traffic groups, select **Advanced** from the **Template Selection** list.

- a. **Device Group**

If you select Advanced from the list, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

- a. **Traffic Group**

If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Virtual Server Questions

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

1. **IP address for the BIG-IP APM virtual server**

This is the address your remote clients will use to connect to for Citrix access. You need an available, external IP address to use here.

2. **Default route set to the BIG-IP?**

The next question asks whether the servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, or whether the BIG-IP system should translate the client's source address if needed to deliver response data to the client.

We recommend choosing **No** from the list because it does not require you to configure routing manually.

Selecting No causes the BIG-IP system to specify the Automap setting for the SNAT Pool option on the associated virtual server (one exception, see #3). In this case, the servers send response data to the BIG-IP system, which then translates the destination address and delivers response data to the client.

3. **More than 64,000 simultaneous connections**

If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #4.

If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat with an additional IP address for each multiple of 64,000 simultaneous connections.

4. **Certificate**

Before running the iApp you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the **Configuration Guide for BIG-IP Local Traffic Manager** available at <http://support.f5.com/kb/en-us.html>.

Select the certificate for you imported for Citrix XenApp or XenDesktop from the list.

5. **Key**

Select the associated key you imported for Citrix XenApp or XenDesktop from the list.

Citrix Infrastructure type

The next section of the template asks whether you are using XenApp or XenDesktop, and the URI of your Web Interface (if it is a non-default URI).

1. **XenApp or XenDesktop**

From the list, select the Citrix application you are deploying, **XenApp** or **XenDesktop**.

2. **Custom Web Interface URI?**

The next question asks whether you have modified the URI of your Citrix Web Interface deployment. The default for XenApp is **/Citrix/Xenapp**. The default for XenDesktop is **/Citrix/DesktopWeb**.

If you have not changed the default URI, leave the list set to **No**, and then continue with the next section.

If you have changed the default URI, select **Yes** from the list. A new row appears asking for the URI. Type the appropriate URI in the box.

3. **Windows domain**

Type the domain name of your infrastructure. Note this is not the fully qualified domain name. The default is **Citrix**.

Citrix Web Interface virtual server

The next section of the template asks about re-encryption, and for the BIG-IP LTM virtual server address for the Web Interface servers. You created this virtual server when configuring the BIG-IP LTM for XenApp or XenDesktop (not a part of this deployment guide).

1. **Encrypt traffic between APM and LTM?**

As mentioned in the prerequisites, the iApp configures the BIG-IP system to terminate SSL connections on the APM. When you configured the BIG-IP LTM for XenApp or XenDesktop, you may have configured the BIG-IP LTM for offloading SSL. If you want the BIG-IP APM to re-encrypt traffic to the BIG-IP LTM, leave this question set to Yes. This requires no modification to the BIG-IP LTM configuration.

If you want the BIG-IP APM to offload SSL connections, and have previously configured the LTM for offload, select **No** from the list. You must then modify your BIG-IP LTM configuration for XenApp or XenDesktop to listen on port 80 and not port 443. See *Modifying the BIG-IP LTM configuration (optional)* on page 11.

2. **Certificate**

If you chose Yes to the previous question, you must select a certificate. Because the traffic is going from the BIG-IP APM to the BIG-IP LTM, you can use the default (self-signed) certificate. If you imported a certificate for re-encryption, select it from the list. In our example, we leave the default, **default.crt**.

3. **Key**

If you chose Yes to question 1, select the associated key for the certificate. In our example, we leave the default, **default.key**.

4. **IP address of LTM virtual server or Web Interface servers**

The IP address you type here depends on whether your BIG-IP LTM configuration is on the same physical device or a separate device:

a. *Same physical device*

Type the IP address and port of your Citrix Web Interface servers. Click the **Add** button to enter additional Web Interface servers.

b. *Separate physical device*

Type the IP address of the Web Interface virtual server you previously created on the BIG-IP LTM. If necessary, type the appropriate port in the Port box. If re-encrypting traffic, this should be port 443. If you are not re-encrypting traffic, the port should be 80 (and may require modifications to your LTM configuration).

Do not click the Add button, as it simply adds another row for an additional entry. If you leave the additional entry row blank, you will get an error when you complete the iApp.

Authentication Questions

The next section of the iApp asks for information about your Active Directory implementation if it does not support anonymous binds.

1. **Username if anonymous binds are not supported**

If anonymous binds are not supported in your Active Directory deployment, type a user name to bind with Active Directory. This allows APM to offload authentication.

2. **Password**

Type the associated password for the user name you entered (if applicable).

3. **Active Directory FQDN**

Type the fully qualified domain name of your Active Directory implementation

4. **Active Directory domain controller IP address**

Type the IP address of your Active Directory domain controller.

Protocol Optimization Questions

In this section, you configure security and protocol optimizations for Citrix XenApp or XenDesktop.

1. **WAN or LAN**

Specify whether most clients are connecting over a WAN or LAN. The BIG-IP system applies certain optimization profiles depending on your choice.

Finished

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

If you configured the iApp for offloading SSL on the BIG-IP APM, you may need to change your BIG-IP LTM configuration. See *Modifying the BIG-IP LTM configuration (optional)* on page 11.

Next Steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Citrix XenApp or XenDesktop service you just created. To see the list of all the configuration objects created to support the iApp, on the Menu bar, click **Components**. The complete list of all Citrix related objects opens. You can click individual objects to see the settings. Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the Citrix implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the 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 XenApp or XenDesktop Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the Citrix configuration objects.

Object-level statistics

Use the following procedure to view statistics on individual objects.

To view object-level statistics

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.

This completes the configuration. For more information on F5 solutions for Citrix, see <http://www.f5.com/solutions/applications/citrix/xenapp/>.

Modifying the BIG-IP LTM configuration (optional)

If you want the BIG-IP APM to offload SSL connections, and have previously configured the LTM for offload, you must then modify your existing BIG-IP LTM Web Interface configuration for XenApp or XenDesktop to listen on port 80 and not port 443. The procedure for modifying the BIG-IP LTM depends on whether you are using Citrix XenApp or XenDesktop.

Modifying the configuration for Citrix XenApp

Use the appropriate procedure below if you configured the BIG-IP LTM for Citrix XenApp.

If you configured the BIG-IP LTM for Citrix XenApp using the iApp template

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your LTM Citrix XenApp Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. In the **SSL Encryption Questions**, the first question asks whether you want the BIG-IP system to offload SSL. Select **No** from the list.
5. Click the **Finished** button.
The BIG-IP system automatically makes the necessary changes.

If you configured the BIG-IP LTM for Citrix XenApp manually

If you configured the BIG-IP LTM for XenApp manually, you need to delete the redirect virtual server on port 80, modify the port on the Web Interface virtual server and remove the Client SSL profile.

To delete the Web Interface redirect virtual server on port 80

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the **Virtual Server** list, click the name of the Web Interface redirect virtual server you created for Citrix XenApp. This virtual server is on port 80, and should not have any configuration objects other than the built-in redirect iRule.
3. At the bottom of the page, click the **Delete** button, and then confirm the deletion.

To modify the XenApp Web Interface main virtual server

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the **Virtual Server** list, click the name of the Web Interface main virtual server you created for Citrix XenApp. This virtual server is on port 443, and should have all configuration objects you created for XenApp.

3. In the **Service Port** box, type **80** or select **HTTP** from the list.
4. From the **SSL Profile (Client)** list, select **None**.
5. Click the **Update** button.

This completes the necessary modifications for XenApp.

Modifying the configuration for Citrix XenDesktop

Use the following procedures to modify the XenDesktop configuration. You need to delete the redirect virtual server on port 80, modify the port on the Web Interface virtual server and remove the Client SSL profile.

To delete the Web Interface redirect virtual server on port 80

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the **Virtual Server** list, click the name of the Web Interface redirect virtual server you created for Citrix XenDesktop. This virtual server is on port 80, and should not have any configuration objects other than the built-in redirect iRule.
3. At the bottom of the page, click the **Delete** button, and then confirm the deletion.

To modify the XenDesktop Web Interface main virtual server

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the **Virtual Server** list, click the name of the Web Interface main virtual server you created for Citrix XenDesktop. This virtual server is on port 443, and should have all configuration objects you created for XenDesktop.
3. In the **Service Port** box, type **80** or select **HTTP** from the list.
4. From the **SSL Profile (Client)** list, select **None**.
5. Click the **Update** button.

This completes the Citrix modifications.

Manually configuring the BIG-IP APM for XenApp or XenDesktop

While we strongly recommend using the iApp template to configure the BIG-IP APM for Citrix XenApp or XenDesktop, advanced users extremely familiar with the BIG-IP APM can use the following configuration tables for guidance on manually configuring the APM. As with the iApp portion of this guide, you must already have configured the LTM for XenApp or XenDesktop.

The following tables contain any non-default setting you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product documentation. In the *SSO Configurations* section below, use the SSO configuration for XenApp or XenDesktop as applicable for your deployment.

BIG-IP Object	Non-default settings/Notes	
DNS and NTP settings	See <i>Configuring the DNS settings on page 5</i> and <i>Configuring the NTP settings on page 6</i> for instructions.	
AAA Servers (Main tab-->Access Policy -->AAA Servers)	Name	Specify a unique name. We use citrix-domain
	Type	Active Directory
	Domain Controller	Type the IP address of the Domain Controller
	Domain Name	Type the FQDN of the Windows Domain name
	Admin Name¹	Type the Administrator name
	Admin Password¹	Type the associated password
SSO Configurations (Main tab-->Access Policy -->SSO Configurations)	XenApp SSO Configuration	
	Name	Type a unique name. We use XenApp-SSO .
	SSO Method	Form Based
	Form Method	POST
	Form Action	/Citrix/XenApp/auth/login.aspx²
	Form Parameter for User Name	user
	Form Parameter for Password	password
	Hidden Form Parameters/Values	domain <domain-name>³ LoginType Explicit
	Successful Logon Detection Match Type	By Resulting Redirect URL
	Successful Logon Detection Match Value	/Citrix/XenApp/site/default.aspx²
	XenDesktop SSO Configuration	
	Name	Type a unique name. We use XenDesktop-SSO .
	SSO Method	Form Based
	Form Method	POST
Form Action	/Citrix/DesktopWeb/auth/login.aspx⁴	
Form Parameter for User Name	user	
Form Parameter for Password	password	
Hidden Form Parameters/Values	domain <domain-name>³ LoginType Explicit	
Successful Logon Detection Match Type	By Resulting Redirect URL	
Successful Logon Detection Match Value	/Citrix/DesktopWeb/site/default.aspx²	
Connectivity Profile (Main tab-->Access Policy -->Secure Connectivity)	Name	Type a unique name
	Parent Profile	connectivity
Access Profile (Main tab-->Access Policy -->Access Profiles)	Name	Type a unique name
	SSO Configuration	Select the SSO Configuration you created above

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

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. In our example, **domain LABDOMAIN**

⁴ You may need to adjust these URLs to match your configuration

Configuration table, continued

BIG-IP Object	Non-default settings/Notes	
Access Policy (Main tab-->Access Policy -->Access Profiles)	Edit	Edit the Access Profile you created using the VPE. See <i>Editing the Access Profile with the Visual Policy Editor</i> on page 15 for instructions.
Profiles (Main tab-->Local Traffic -->Profiles)	HTTP (Profiles-->Services)	Name Type a unique name Parent Profile http Redirect Rewrite All
	TCP WAN (Profiles-->Protocol)	Name Type a unique name Parent Profile tcp-wan-optimized (see note on left) Idle Timeout ¹ We recommend between 600-900 ¹
	TCP LAN (Profiles-->Protocol)	Name Type a unique name Parent Profile tcp-lan-optimized (see note on left) Idle Timeout ¹ We recommend between 600-900 ¹
	Persistence (Profiles-->Persistence)	Name Type a unique name Persistence Type Source Address Affinity
	Client SSL (Profiles-->SSL)	Name Type a unique name Parent Profile clientssl Certificate and Key Select the Citrix Certificate and Key
	Server SSL² (Profiles-->SSL)	Name Type a unique name Parent Profile serverssl-insecure-compatible
Pool (Main tab-->Local Traffic -->Pools)	Name	Type a unique name.
	Health Monitor³	TCP³
	Load Balancing Method	Choose your preferred load balancing method.
Virtual Server (Main tab-->Local Traffic -->Virtual Servers)	Address and Service Port	If this APM is on a <i>separate</i> physical device from the LTM, type the IP address and port of the LTM Web Interface virtual server. If this APM is on the <i>same</i> device as the LTM, type the IP address and port of each of your Web Interface servers.
	Name	Type a unique name.
	IP Address⁴	Type the IP address for this virtual server.
	Service Port	443
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	Persistence Profile	Select the Persistence profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SSL Profile (Server)	Select the Server SSL profile you created above (if applicable)
SNAT Pool	Auto Map (if you expect more than 64,000 concurrent connections, create a SNAT Pool)	
Access Profile	Select the Access Profile you created above	
Connectivity Profile	Select the Connectivity profile you created	
Citrix Support	Check the box to enable Citrix support	

Note about TCP profiles:
Certain WAN conditions such as users connecting over low bandwidth or high latency can be optimized further by using different options for the TCP WAN profile. We recommend that you review the following solutions for environments where users are connecting from more challenging WAN conditions. Significant improvements are possible. Specifically, we recommend setting Nagle's Algorithm to Disabled and setting Congestion Control to Scalable. See

<http://support.f5.com/kb/en-us/solutions/public/7000/400/sol7402.html> and <http://support.f5.com/kb/en-us/solutions/public/7000/400/sol7405.html>

¹ Citrix maintains keepalives using its own clients. This keepalive is configurable on a per client basis (see Citrix documentation instructions on adjusting this timeout). As an alternate approach, if premature session termination is a concern, we recommend setting the Idle Timeout value to a longer time period to prevent idle desktop sessions from being terminated prematurely

² You only need a Server SSL profile if you are re-encrypting traffic to send to the BIG-IP LTM. See #1 in *Citrix Web Interface virtual server* on page 8 for more details.

³ If this APM is on the same device as the LTM, you can optionally create the advanced monitor for the Web Interface servers as described in the manual configuration tables of the XenApp or XenDesktop deployment guide. See the Prerequisites for the URLs.

⁴ The address here will most likely be an external address, the main entry point for users into the network. For example, the IP address might translate to a well understood DNS entry "Citrix.MyCompany.com." The use of a NAT'ed address which is translated somewhere else in the network (firewall, for example) is also supported with this configuration.

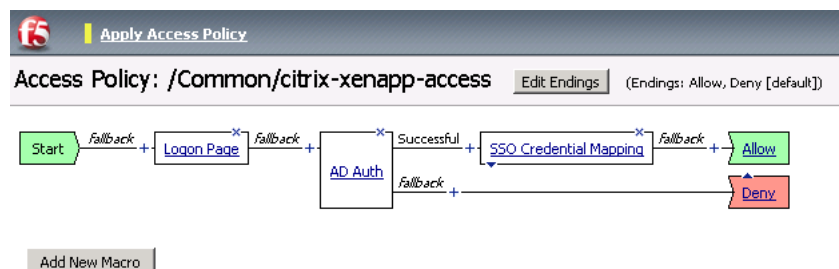
Editing the Access Profile with the Visual Policy Editor

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/>).

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you created, and then in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click **Add Item**.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
6. Click the **Save** button.
7. Click the **+** symbol between **Logon Page** and **Deny**. The options box opens.
8. Click the **AD Auth** option button, and then click **Add Item**.
9. From the **Server** list, select the name of the AAA server you created in the table above. In our example, we select **Citrix_domain**.
10. Configure the rest of the Active Directory options as applicable, and then click **Save**. You now see two paths, **Successful** and **Fallback**.
11. Click the **+** symbol on the Successful path between **AD Auth** and **Deny**. The options box opens.
12. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
13. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
14. Click the **Save** button.
15. On the fallback path between **SSO Credential Mapping** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**. When complete, it should look like the example below.
16. 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.
17. Click the Close button on the upper right to close the VPE.



Document Revision History

Version	Description
1.0	New Version
1.1	Added manual configuration details
1.2	<p>Updated the link to the downloadable iApp to point to the newest version</p> <p>Updated the guide to reflect the ability in the new iApp to use either the existing LTM virtual server (if on a separate physical device) or IP addresses of the Web Interface servers (if on the same physical device).</p> <p>Updated the manual configuration table to include a BIG-IP pool that includes either the IP address of the LTM virtual server or the Web Interface servers</p>

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

