



## Deploying the BIG-IP LTM with Citrix XenApp

### What's inside:

- 2 Prerequisites and configuration notes
- 3 Configuration Worksheet
- 4 Using the BIG-IP LTM Application Template for Citrix XenApp
- 8 Modifying the Citrix XenApp Web Interface configuration
- 9 Next steps
- 9 Troubleshooting

Welcome to the F5 deployment guide for Citrix® XenApp® and BIG-IP 10.2.1. This shows how to configure the BIG-IP Local Traffic Manager (LTM) using the Application Template for directing traffic, ensuring application availability, improving performance and providing a flexible layer of security for Citrix XenApp version 5.0 and 6.0

Citrix XenApp provides a run-time environment for applications to be hosted on the server and accessed over the network or by using web protocols, with just keyboard strokes, mouse movements and screen updates being exchanged between the client and the server.

The BIG-IP LTM provides mission critical availability, enhanced security, simple scalability and high operational resiliency to the Citrix XenApp deployment so users can access resources from any device in any location as easily and securely as from within the corporate LAN.

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

For more information on the F5 BIG-IP LTM, see

<http://www.f5.com/products/big-ip/product-modules/local-traffic-manager.html>

Additional information can be found on the DevCentral Citrix forum at

<http://devcentral.f5.com/citrix>

To provide feedback on this deployment guide or other F5 solution documents, contact us at [solutionsfeedback@f5.com](mailto:solutionsfeedback@f5.com).

### Products and versions tested

Product	Version
BIG-IP LTM	10.2.1 HF-1 and later
Citrix XenApp	5.0.1 and 6.0

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

The Current Document Version: **1.2**. See page 12 for the document revision history.

Document Version

1.2

## Prerequisites and configuration notes

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

- For this deployment guide, the Citrix XenApp installation must be running version 5.0 or 6.0.
- For this deployment guide, the BIG-IP LTM system **must be running version 10.2.1 Hotfix 1** or later. If you are using a previous version of the BIG-IP LTM system see the Deployment Guide index.
- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see the online help or product documentation.
- See the *Configuration Worksheet on page 2* to learn what type of information you need to gather before beginning the application template.
- 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.

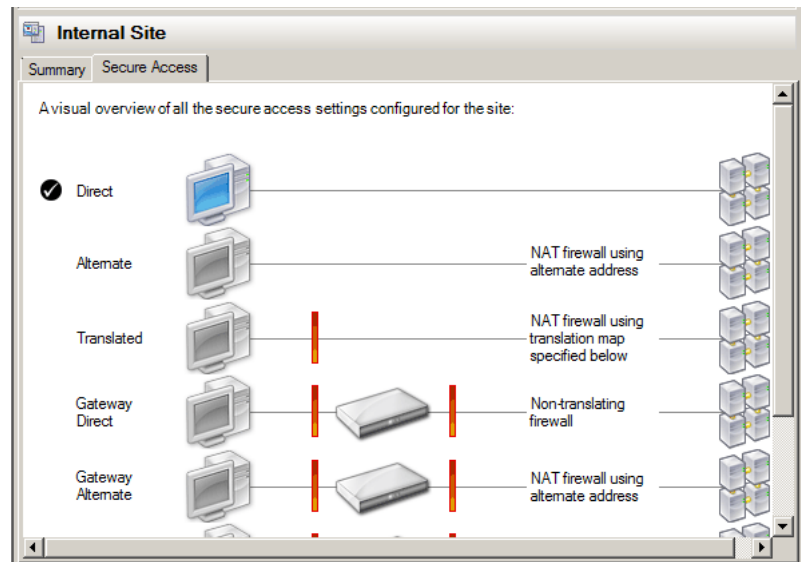


Figure 1: Citrix Session configuration

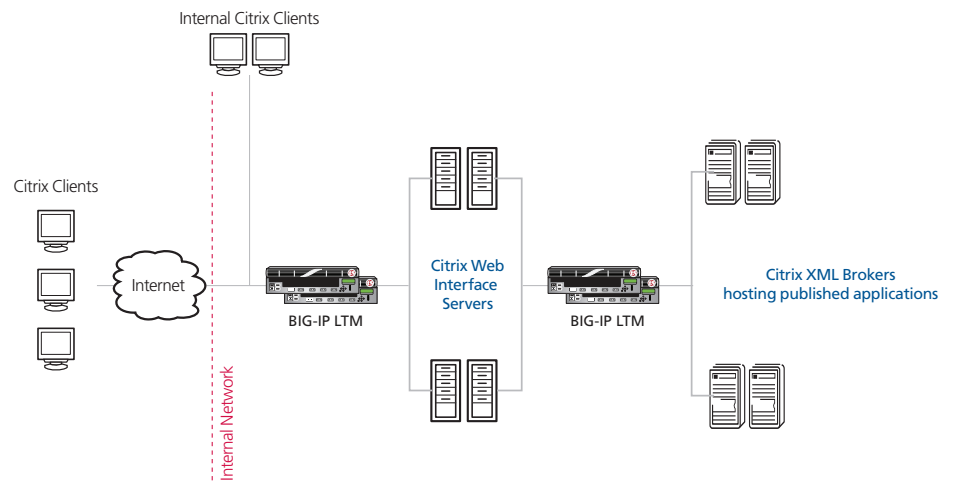
To leave feedback for this or other F5 solution documents, contact us at [solutionsfeedback@f5.com](mailto:solutionsfeedback@f5.com)

## Configuration example

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

In this implementation, traffic to the Citrix Web Interface servers and the Citrix XML Broker servers is managed by the F5 BIG-IP LTM system, and when necessary, ensures that each client connects to the same member of the farm across multiple sessions using persistence on the

BIG-IP LTM. The F5 BIG-IP LTM system is also setup to monitor the Citrix Web Interface servers and Citrix XML Broker servers to ensure availability and automatically mark down servers that are not operating correctly. The ability to terminate SSL sessions in order to offload this processing from the XenApp 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

## Configuration Worksheet

We strongly recommend using the Application Template for Citrix XenApp found in BIG-IP LTM version 10.2.1. In order to run the application template for Citrix XenApp, you need to gather some information, such as Citrix server IP addresses and domain information. You also need to provision two IP addresses that are used for the BIG-IP LTM virtual servers.

Use the following worksheet to prepare the information you will need for the template:

IP Addresses	Certificate and Key?	Pool Members	Health monitor	WAN or LAN
<b>Front-end Web Interface virtual</b>			DNS name clients use to access XenApp:  URI required for accessing XenApp:  XenApp user name with access to applications <i>(we recommend creating a XenApp user account specifically for the monitor):</i>  Associated password:  Domain for the user account:  Name of application XenApp user can retrieve:	Most clients connecting through BIG-IP to XenApp are coming over a:  LAN  WAN
Virtual server IP address:	<i>Optional.</i> Import a certificate and key into the BIG-IP LTM before running the template.  Certificate:  Key:	Web Interface Server IPs: 1: 2: 3: 4: 5: 6: 7:		
<b>Back-end XML Broker virtual</b>			Associated password:  Domain for the user account:  Name of application XenApp user can retrieve:	Most clients connecting through BIG-IP to XenApp are coming over a:  LAN  WAN
Virtual server IP address:	Not Applicable	XML Broker Server IPs: 1: 2: 3: 4: 5: 6: 7:		

In our example, our worksheet looks like the following:

IP Addresses	Certificate and Key?	Pool Members	Health monitor	WAN or LAN
<b>Front-end Web Interface virtual</b>			DNS name clients use to access XenApp: <b>xenapp.example.com</b>  URI required for accessing XenApp: <b>/Citrix/XenApp/</b> (default setting)  XenApp user name with access to applications: <b>xenapp-test-user</b>	Most clients connecting through BIG-IP to XenApp are coming over a:  LAN  <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">WAN</span>
Virtual server IP address: <b>192.0.2.101</b>	<i>Optional.</i> Import a certificate and key into the BIG-IP LTM before running the template.  Certificate: <b>xenapp-cert</b>  Key: <b>xenapp-key</b>	Web Interface Server IPs: 1: <b>10.10.10.101</b> 2: <b>10.10.10.102</b> 3: <b>10.10.10.103</b> 4: <b>10.10.10.104</b> 5: <b>10.10.10.105</b> 6: <b>10.10.10.106</b> 7:		
<b>Back-end XML Broker virtual</b>			Associated password: <b>password</b>  Domain for the user account: <b>example</b>  Name of application XenApp user can retrieve: <b>NOTEPAD</b>	Most clients connecting through BIG-IP to XenApp are coming over a:  LAN  <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">WAN</span>
Virtual server IP address: <b>10.10.10.1</b>	Not Applicable	XML Broker Server IPs: 1: <b>10.10.10.201</b> 2: <b>10.10.10.202</b> 3: <b>10.10.10.203</b> 4: <b>10.10.10.204</b> 5: <b>10.10.10.205</b> 6: 7:		

## Using the BIG-IP LTM Application Template for Citrix XenApp

In this section, we give you guidance on configuring the BIG-IP LTM using the Application Template.

### Virtual Server Questions

The first section of the template asks questions about the BIG-IP virtual servers. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients on an external network can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions.

While the template creates three virtual servers for Citrix XenApp (Web Interface, XML Broker, and XML Broker enumeration), you are only asked for two IP addresses in this section. This is because the enumeration virtual server uses the same IP address as the XML Broker virtual, but on a different port.

In this section, you configure the following:

- **Unique prefix**  
The system attaches this prefix to all of the BIG-IP objects created by the template. You can leave the default or create a prefix specific to your implementation.
- **IP address for the Web Interface virtual server**  
This is the address clients will use to access XenApp (or a FQDN will resolve to this address). You need an available, external IP address to use here.
- **IP address for the XML Broker virtual server**  
This is the address the Web Interface servers will use to communicate with the back-end XML Brokers through the BIG-IP LTM. You need an available IP address to use here.
- **Manual routes or secure network address translation**  
If the XenApp servers do not have a route back to the clients through the BIG-IP (typical and default), the BIG-IP uses Secure Network Address Translation (SNAT) *Automap* to translate the client's source address to an address configured on the BIG-IP. The servers then use this new source address as the destination address.

If the XenApp servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address.

We recommend choosing **No** from the list because it is secure, does not require you to configure routing manually and helps avoid problems like Direct Server Return.

Templates and Wizards » Templates » Citrix XenApp	
<b>Virtual Server Questions</b>	
What unique prefix do you want the BIG-IP system to use when naming objects that this template creates?	<input type="text" value="f5-demo_XenApp_"/>
What IP Address do you want to use for the front-end Citrix XenApp Web Interface virtual server?	<input type="text" value="192.0.2.100"/>
What IP Address do you want to use for the back-end Citrix XenApp XML Broker virtual server?	<input type="text" value="10.10.10.1"/>
Do the Citrix XenApp servers have a route back to application clients via this BIG-IP system?	<input type="button" value="No"/> ▼

Figure 3: Virtual server questions

## SSL Encryption Questions

The next section of the XenApp template is about SSL encryption. With SSL offload, the BIG-IP system decrypts HTTPS traffic before sending it to the Citrix XenApp Web Interface servers as HTTP traffic. Offloading SSL processing onto the BIG-IP LTM saves valuable processing power on the XenApp devices, enabling them to be more efficient. We recommend offloading SSL. .

### Important



*If you are using the BIG-IP LTM to offload SSL, before running the XenApp template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.*

*For 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>.*

In this section, you need to decide the following

#### ➤ SSL offload

- » **No:** If you are not offloading SSL onto the BIG-IP LTM, continue to the following section, leaving the list set to **No**. This is the default.
- » **Yes:** If you are offloading SSL onto the BIG-IP system, select **Yes** from the list.
  - Certificate: Select the Certificate you imported for this implementation.
  - Key: Select the key you imported for this implementation. This is usually the same name as the Certificate.

The BIG-IP template creates an additional virtual server, an iRule to redirect HTTP traffic to HTTPS, and an SSL profile to support SSL offload.

SSL Encryption Questions	
Do you want the BIG-IP system to offload SSL processing from the Citrix XenApp Web Interface servers?	Yes ▾
Which certificate do you want the BIG-IP system to use to authenticate the server? (You may need to import a certificate before deploying this Template.)	xenapp-SSL-cert ▾
Which key do you want the BIG-IP system to use for encryption? (You may need to import a key before deploying this Template.)	xenapp-SSL-cert ▾

Figure 4: SSL Encryption Questions

## Load Balancing Questions

In the next two sections ask you about load balancing. In these sections, you choose a load balancing method, enter the XenApp server information, and the BIG-IP application template creates load balancing pools.

For both the Web Interface and XML Broker sections, you need the following:

➤ **Preferred load balancing method**

While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

➤ **Address**

Use the IP address for the Web Interface and XML Brokers you entered on the Configuration Worksheet. The template will add the nodes to the appropriate load balancing Pool.

➤ **Service Port**

You should use the default port of 80 for both the Web Interface and XML Broker sections, unless you have changed them in the XenApp configuration. The Template creates an additional pool for XML Broker Enumeration on port 137 behind the scenes, using the addresses you enter for the XML Brokers.

The image shows two configuration panels for load balancing. The top panel is titled "Web Interface Load Balancing Questions" and the bottom panel is titled "XML Broker Load Balancing Questions". Both panels have a similar layout:

- Which load balancing method do you want to use?**: A dropdown menu with "Least Connections (member)" selected.
- Address:**: A text input field containing "10.10.10.106" (for Web Interface) or "10.10.10.205" (for XML Broker).
- Service Port:**: A text input field containing "80" and a "Select..." dropdown menu.
- Which servers do you want this virtual server to reference? (the virtual server will not be available until at least one server is added)**: A list of server entries, each with "Add", "Edit", and "Delete" buttons. The entries are:
  - R:1 P:1 C:0 10.10.10.101 :80
  - R:1 P:1 C:0 10.10.10.102 :80
  - R:1 P:1 C:0 10.10.10.103 :80
  - R:1 P:1 C:0 10.10.10.104 :80
  - R:1 P:1 C:0 10.10.10.105 :80

Figure 5: Load Balancing Questions

## Health monitor questions

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 XenApp 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.

**Tip**



*We recommend you create a XenApp user account specifically for use in this monitor. This user could be restricted to only the application specified in the monitor.*

**Critical**



*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.*

In this section, you need the following:

- **DNS Name**  
This is the Fully Qualified DNS name users employ to access XenApp.
- **URI**  
This is the URI or path representing the XenApp deployment. The default Citrix URI is **/Citrix/XenApp**.
- **User Name**  
The user name that has access to the application specified below. Again, we recommend creating a user account specifically for the monitor.
- **Password**  
The password associated with the user name.
- **Domain**  
The domain for the user account above.
- **Application**  
The name of an application the monitor attempts to retrieve.

Health Monitor Questions	
Specify the DNS name that users are expected to use to access the Citrix XenApp implementation.	<input type="text" value="example.com"/>
Specify the URI required for accessing XenApp.	<input type="text" value="/Citrix/XenApp"/>
Specify a user account that can retrieve applications from XenApp.	<input type="text" value="test-user"/>
What is the password for the above specified user account?	<input type="password" value="....."/>
What is the domain for the above specified user account?	<input type="text" value="example-domain"/>
Specify the name of an application that can be returned by XenApp for the above user. The health of the XenApp will be tested by attempting to retrieve this application using this user account.	<input type="text" value="NOTEPAD"/>

Figure 6: Health Monitor Questions

This completes the Application template.

## Modifying the TCP profiles

After completing the template, there are two changes to the TCP profiles created by the template.

The first change is to the TCP Idle Timeout value. F5 has discovered that if a TCP profile is configured with a **TCP Idle Timeout** set to **Indefinite**, session exhaustion may occur. Currently, the Application Template sets the Idle Timeout value of the TCP profiles to **Indefinite** in the Web Interface servers configuration. Future versions of the template will not include this setting.

The second is a recommended but not required. 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**.

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

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

### To modify the TCP profiles

1. From the Main tab of the BIG-IP Configuration utility, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, select **Protocol**, and then click **TCP** from the drop-down menu.
3. Click the first Web Interface TCP profile. This profile starts with the unique preface you specified on page 4, and includes **\_wi\_**. In our example, we click the LAN optimized profile first: **my\_XenApp\_\_wi\_lan-optimized\_tcp\_profile**.
4. From the **Idle Timeout** list, select **Specify** and then type a number of seconds in the box. We recommend a timeout value of between 600 and 900 seconds.
5. Click the **Update** button.
6. Repeat this procedure to modify the Idle Timeout value for the WAN optimized Web Interface TCP profile.  
For this WAN optimized TCP profile, if you are making any changes to the profile based on the Solutions referenced in the introduction to this section, make those changes as well.
7. If you are making optional changes to the WAN optimized TCP profile for Web Interface as suggested by the Ask F5 solutions, make the same changes on the XML Broker WAN optimized TCP profile. You do not need to modify the Idle Timeout for this profile.

## Modifying the Citrix XenApp Web Interface configuration

The next task is to make important modifications to the Citrix servers.

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

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

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

1. From a Web Interface server, open the Access Management Console.
2. In the Navigation pane, expand **Citrix Resources, Configuration Tools, Web Interface** and then your site name.
3. From the middle column, select **Manage 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 (the address you added in the third bullet on page 8). In our example, we type **10.10.10.1**.
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.

#### ↪ Important

You must make the changes in this section in order for the deployment to function properly.

The last procedure requires editing Java files on the Web Interface servers.

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

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

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

1. Open the file `\\inetpub\\wwwroot\\Citrix\\XenApp\\app_code\\PagesJava\\com\\citrix\\wi\\pageutils\\Include.java` on the Web Interface server, and find the function named `getClientAddress`. In version 5.0, 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.

## Next steps

After completing the Application Template, the BIG-IP system presents a list of all the configuration objects created to support XenApp. Once the objects have been created, you are ready to use the new deployment.

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

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

### Viewing statistics

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

On the Main tab, expand **Overview**, and then click **Statistics**. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.

To see Networking statistics in a graphical format, click **Dashboard**.

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

## Troubleshooting

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

- **Users can't connect to the Web Interface servers**  
Make sure users are trying to connect using the BIG-IP virtual server address (or a FQDN that resolves to the virtual server address).
- **Users can connect to the Web Interface servers, but there are connectivity problems to and from the XML Broker servers.**

This type of problem is usually a routing issue. If you chose Yes when asked if the XenApp servers have a route back to application clients via this BIG-IP system, you must manually configure the proper routes on the XenApp farm servers.

If you mistakenly answered Yes to this question, 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 **Automap**.

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

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

➤ **Citrix XML Broker servers 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.

To see if the issue is coming from the health monitor, you can temporarily disable the health monitor and reattempt the connection. If the connection succeeds with the monitor disabled, we recommend you re-run the template, as the monitor is extremely difficult to manually troubleshoot.

**To disable the monitor**

1. From the Main tab of the BIG-IP Configuration utility, expand **Local Traffic**, and then click **Pools**.
2. From the Pool list, click the Pool the template created for the XML Broker servers. This pool starts with the prefix you specified (my\_XenApp\_ by default) and ends with **\_xmlb\_pool**.
3. In the Health Monitors section, from the **Active** list, select the health monitor and then click Remove (>>) to disable the monitor.
4. Click the **Update** button.
5. When you want to reactivate the monitor, select the XML Broker monitor you previously removed, click the Add (<<) button to reactivate it, and then click **Update**.

### Document Revision History

Version	Description
1.0	New Version
1.1	- Clarified guidance on modifying the Web Interface configuration on page 8. - Added section on page 7 for modifying the TCP profiles created by the template
1.2	- Added note that the Citrix Session configuration must be set to Direct mode. - Added additional information on tuning the TCP WAN optimized profiles for users with low bandwidth or high latency connections.

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

