



## Deploying the BIG-IP Access Policy Manager with Citrix XenApp

**Important:** This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.

For a list of current guides, see <https://f5.com/solutions/deployment-guides>.

# Table of Contents

## Configuring the F5 BIG-IP APM with Citrix XenApp

Prerequisites and configuration notes .....	1-1
Product versions and revision history .....	1-2
Configuration example .....	1-3

## Configuring the F5 BIG-IP APM Secure Proxy with Citrix XenApp

Traffic flow .....	2-1
Configuring the BIG-IP APM secure connection proxy .....	2-3
Citrix Application Server Access control .....	2-3
Creating a Client SSL profile .....	2-4
Creating the HTTP profile .....	2-5
Creating the iRule .....	2-6
Creating the virtual server .....	2-6
Disabling ARP requests .....	2-8
Configuring the BIG-IP LTM for authentication .....	2-10
Configuring the DNS settings on the BIG-IP LTM .....	2-10
Configuring the NTP settings on the BIG-IP LTM .....	2-11
Configuring the BIG-IP APM for Citrix Secure Proxy .....	2-12
Choosing an authentication mechanism .....	2-12
Creating a AAA Server .....	2-13
Creating the SSO configuration .....	2-15
Creating an Access Profile .....	2-16
Creating the profiles .....	2-29
Creating the persistence profile .....	2-30
Creating the iRule .....	2-31
Creating the virtual server .....	2-32
Appendix A: Citrix Receiver Support with BIG-IP APM secure proxy example for iPhone/iPad .....	2-34
Configuring the iPhone for Citrix XenApp Receiver support .....	2-34
Configuring the iPad for Citrix XenApp Receiver support .....	2-39

## Configuring the BIG-IP APM with Citrix XenApp with Remote Network Access

Prerequisites and configuration notes .....	3-1
Configuration example and traffic flow .....	3-1
Configuring the BIG-IP APM .....	3-4
Configuring remote access .....	3-4
Creating a Connectivity Profile .....	3-6
Creating a Webtop .....	3-7
Creating an AAA Server .....	3-8
Creating an Access Profile .....	3-8
Editing the Access Profile with the Visual Policy Editor .....	3-9
Creating the Network Access BIG-IP configuration objects .....	3-10
Creating the profiles .....	3-10
Creating the virtual servers .....	3-13





I

---

## Deploying the BIG-IP APM with Citrix XenApp

---

---

# Configuring the F5 BIG-IP APM with Citrix XenApp

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

While Citrix XenApp provides 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 allows organizations to centralize their applications, this guide describes configuring access and delivering applications as needed with the BIG-IP system.

This guide is broken up into the following chapters:

- *Configuring the F5 BIG-IP APM Secure Proxy with Citrix XenApp*, on page 2-1
- *Configuring the BIG-IP APM with Citrix XenApp with Remote Network Access*, on page 3-1

For more information on the BIG-IP APM, see

[www.f5.com/products/big-ip/product-modules/access-policy-manager.html](http://www.f5.com/products/big-ip/product-modules/access-policy-manager.html)

## Prerequisites and configuration notes

The following are prerequisites for this solution.

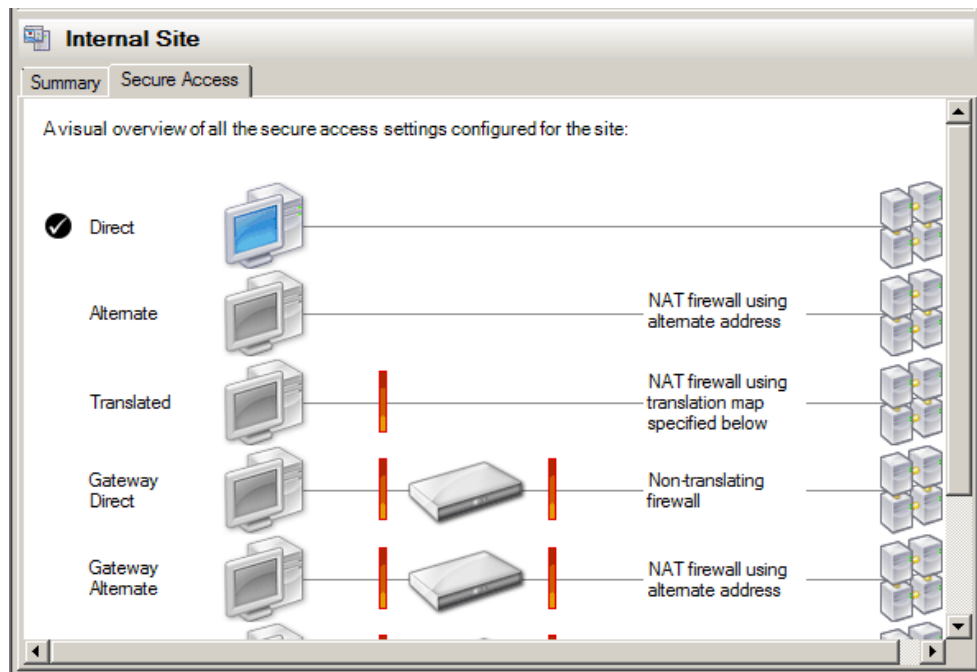
- ◆ For this guide, the Citrix XenApp installation must be running version 5.0 or 6.0.
- ◆ For this deployment guide, the BIG-IP LTM system should be running version 10.2 or later. If you are using a previous version of the BIG-IP LTM system see the [Deployment Guide](#) index.

**Important:** If you are using version 10.2.1, you **must be running version 10.2.1 Hotfix 1** or later for the configuration in this guide.

- ◆ Session Reliability on the Citrix backend servers is supported, but not required. The configuration described in this deployment guide is valid whether Session Reliability is enabled or disabled on the backend servers.
- ◆ We assume you have already configured your BIG-IP Local Traffic Manager (LTM) according to the LTM guide for Citrix XenApp: <http://www.f5.com/pdf/deployment-guides/f5-citrix-xenapp-dg.pdf>

This configuration **requires** the pool and health monitor for the Citrix Web Interface servers that are created by the Template or in the deployment guide.

- ◆ 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 *Creating a Client SSL profile*, on page 2-4.
- ◆ Because the current version of the Application Template is for Presentation Server 4.5, and while the template may work with XenApp 5.0 and 6.0, we recommend you do not use the Application Template for XenApp 5.0. Future versions of the BIG-IP will include the updated template.
- ◆ Citrix Session configuration must be set to Direct mode. For specific information on configuring the Citrix Session mode, see the Citrix documentation.



**Figure 1.1** Citrix Session configuration

## Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP APM/Edge Gateway	v10.2, 10.2.1 HF-1, 10.2.2
Citrix XenApp	5.0 and 6.0

---

Document Version	Description
1.0	New guide
1.1	Added a prerequisite for making sure Session Reliability is enabled on the Citrix Backend servers.
1.2	Modified the TCP profile settings to include an Idle Timeout value set to Indefinite. This prevents idle desktop sessions from being terminated prematurely.
1.3	Changed the guidance for Session Reliability. We had previously stated Session Reliability must be enabled. We have verified the configuration works properly whether Session Reliability is enabled or not.
1.4	Modified TCP profile <b>Idle Timeout</b> guidance from <i>Indefinite</i> to 600-900 seconds.
1.5	<ul style="list-style-type: none"><li>- Removed support for v10.2.1, added support for 10.2.1 HF-1 and 10.2.2.</li><li>- Added note that the Citrix Session configuration must be set to Direct mode.</li><li>- Added additional information on tuning the TCP WAN optimized profiles for users with low bandwidth or high latency connections.</li></ul>

## Configuration example

With BIG-IP APM, a front-end virtual server is created to provide security, compliance and control.

There are two recommended modes where APM can be deployed with Citrix XenApp: secure proxy mode and network access client mode. Both modes have advantages that should be considered.

### ◆ Secure Proxy Mode

Secure Proxy mode is detailed in *Configuring the F5 BIG-IP APM Secure Proxy with Citrix XenApp*, on page 2-1

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.

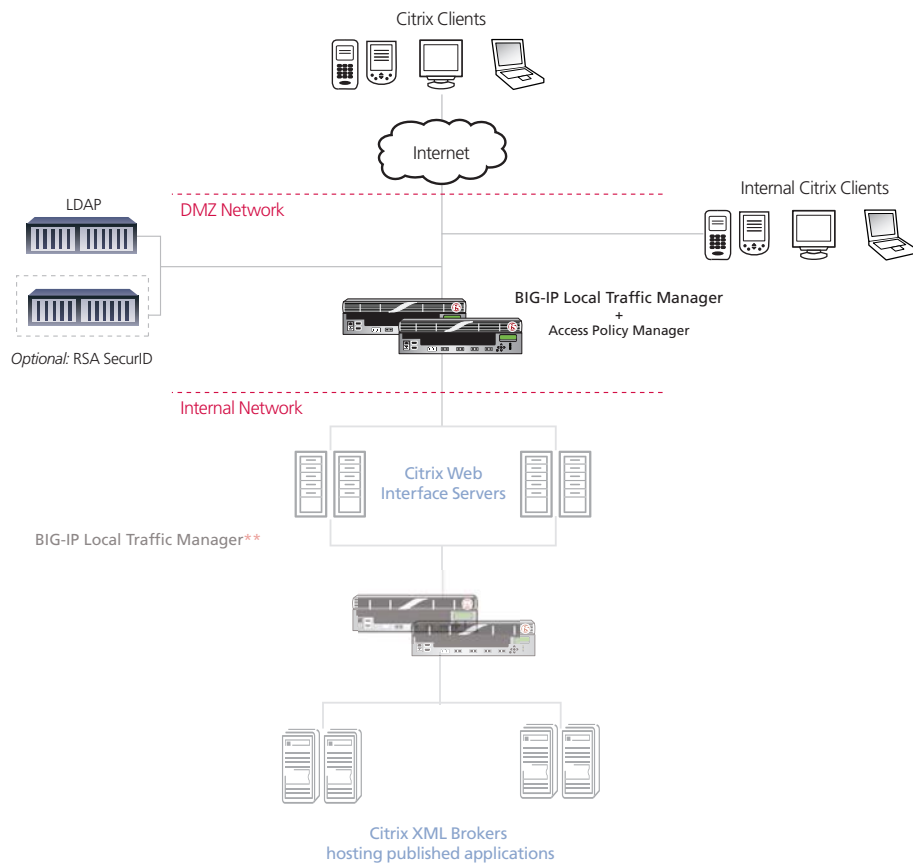
Secure proxy mode has many benefits to both users and administrators. For administrations, APM user authentication is tied directory to Citrix's Active Directory store allowing for compliance and administrative control. For users, TCP optimization and application delivery, plus the need for only the Citrix client, creates a fast and efficient experience.

### ◆ Remote Access Mode

Remote Access mode is detailed in *Configuring the BIG-IP APM with Citrix XenApp with Remote Network Access*, on page 3-1

In the Remote Access Mode, the BIG-IP APM client is used to provided a complete tunnel to the environment. The advantages to this mode are

that UDP based Datagram TLS (DTLS) can be used to achieve accelerated connections as well as finer grained control on user interactions with the system. With the remote access client, access to other parts of an organizations network may also be granted instead of a direct one-to-one relationship between in the secure proxy mode.



**Figure 1.2** Logical configuration example

**\*\*** The BIG-IP Local Traffic Manager (LTM) configuration is shown in this diagram for completeness; the step-by-step procedures are not a part of this deployment guide.

See <http://www.f5.com/pdf/deployment-guides/f5-citrix-xenapp-dg.pdf> for the BIG-IP LTM deployment guide.







# 2

---

## Deploying the BIG-IP APM Secure Proxy with Citrix XenApp

---

---

# Configuring the F5 BIG-IP APM Secure Proxy with Citrix XenApp

In this chapter, we configure the BIG-IP APM in Secure Proxy mode for Citrix XenApp.

## Traffic flow

This section shows 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 APM, and enters his or her credentials.
3. The user is logged into Citrix XenApp.
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 F5 BIG-IP APM. The APM module 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 Citrix XenApp's login form and the user is logged in. The user only ever sees the single login page.

4. The BIG-IP APM checks the users 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 APM and LTM to scale, secure, accelerate and optimize the connections from users to Citrix.

---

## Configuring the BIG-IP APM secure connection proxy

The first task in this deployment guide create the BIG-IP objects that the BIG-IP APM uses internally for the connect proxy.

### ◆ Important

*This virtual server must be created before the configuration that begins on **Configuring the BIG-IP APM for Citrix Secure Proxy**, on page 2-12. Otherwise, the iRules in that section do not parse properly.*

## Citrix Application Server Access control

A central component of the APM secure proxy is the ability and requirement to lock-down access control for users from and to XenApp and only XenApp servers. Once a user is authenticated to APM and establish their Secure Proxy connection, a simple conditional mechanism with the HTTPConnectProxy\_help iRule (*Creating the iRule*, on page 2-6) is used to limit the user's internal access. Access control is achieved through the use of iRule Data Groups.

In the following procedure, we create a Data Group list that contains the Application Server and port. For each Application Server IP Address a data group record is created that includes the port number of the server. For example, for the application server 172.16.119.106, two records are created: 172.16.119.106-1494 and 172.16.119.106-2598.

In this example 1494 and 2598 represent the TCP port number of the Citrix Application server and 172.16.119.106 is the IP address of the Application Server.

Figure 2.1 on the following page shows a complete entry with three servers, 172.16.119.106, 172.16.119.107 and 172.16.119.148 listening on 1494 and 2598. While the IP addresses differ from installation to installation, TCP port 1494 (Citrix ICA Protocol) and TCP port 2598 are common to all ICA installations.

### ◆ Note

*If for some reason your environment has customized and changed these ports, adjust the TCP port numbers as well. This is not common.*

### To configure a Data Group

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. On the Menu bar, click **Data Group List**.
3. Click the **Create** button.
4. In the **Name** box, type a name. We type **CitrixAppServers**.
5. From the **Type** list, select **String**.

6. In the **String** box, type the new string records in the following syntax:  
`172.16.119.xxx-1494`  
`172.16.119.xxx-2598`
7. In the **Value** box, type a value. In our example, all values are 1.  
*Note: The Value 1 indicates to the iRule that the destination Citrix server is active.*
8. Repeat steps 6 and 7 for all servers.
9. Click **Finished**.

Local Traffic » iRules : Data Group List » New Data Group...

**General Properties**

Name: CitrixAppServers

Type: String

**Records**

String: 172.16.119.148-1494

Value: 1

Add

String Records

172.16.119.106-1494 := 1

172.16.119.106-2598 := 1

172.16.119.107-1494 := 1

172.16.119.107-2598 := 1

172.16.119.148-2598 := 1

172.16.119.148-1494 := 1

Edit Delete

Cancel Repeat Finished

*Figure 2.1 Creating the Data Group*

## Creating a Client SSL profile

The next task is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. First we import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP system. If you do not have a certificate and key, see the BIG-IP documentation). After the certificate and key have been imported, we create the SSL profile that uses the certificate and key.

### To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
3. In the upper right corner of the screen, click **Import**.

- 
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
  5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
  6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
  7. Click **Import**.
  8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

### To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **xenapp-https**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

## Creating the HTTP profile

The next task is to create an HTTP profile. You must create an HTTP profile for this configuration to function properly.

### To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. Click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **xenapp-http**.
4. From the **Parent Profile** list, leave the default parent profile, **HTTP**.

5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

## Creating the iRule

The next task is to create the APM-Citrix-helper iRule. This iRule identifies whether the client is the Program Neighborhood or Citrix Receiver client and iRule helps direct connections to the appropriate Citrix server and handles authentication credentials and session information. Once created, this iRule requires no ongoing maintenance.

You must copy this iRule from F5's DevCentral at

[http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix\\_APM\\_Helper.html](http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix_APM_Helper.html)

### To create the APM-Citrix-helper iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the Name box, type a name for this rule. In our example, we type **APM-Citrix-helper**.
4. In the **Definition** box, copy and paste the iRule found at [http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix\\_APM\\_Helper.html](http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix_APM_Helper.html).
5. Click **Finished**.

## Creating the virtual server

The next task is to create a virtual server that contains the iRule you just created.

### Important

---

*The name of this virtual server **MUST** be **citrix\_connect\_proxy**, as this name is hard-coded in an iRule you create later in this guide.*

### To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type **citrix\_connect\_proxy**.  
**Important:** You *must* name this virtual server **citrix\_connect\_proxy**.
4. In the **Destination** section, select the **Host** option button.



- 
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.0.1**.

***Note:** This virtual server is internal only and only called from within BIG-IP itself. Later in this section, we describe how to disable Address Resolution Protocol (ARP) requests for this virtual server, to ensure the address does not interfere with your network. We have arbitrarily used 192.168.0.1 as a non-routable, RFC 1918 space IP address, you are free to use any IP address. The important facet of this virtual server is the name **citrix\_connect\_proxy** which must match exactly as described in this rule.*

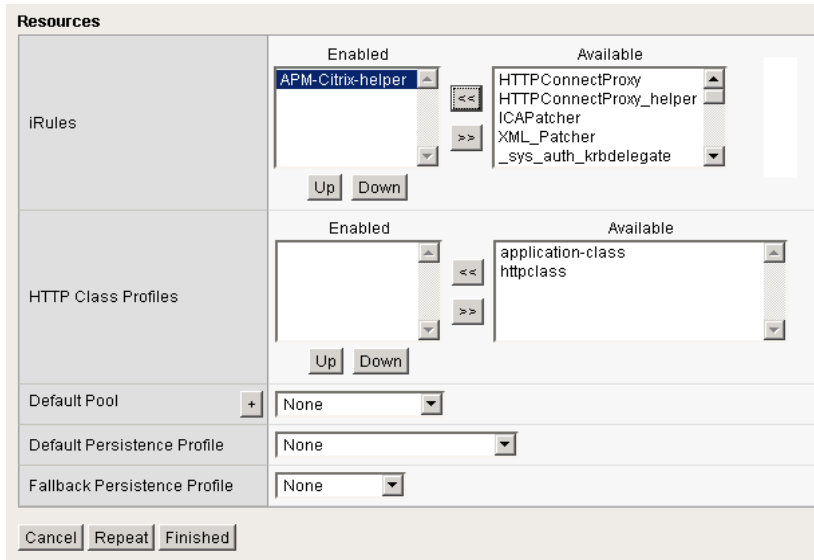
6. In the **Service Port** box, type **443**.

The screenshot shows the 'New Virtual Server' configuration window. The breadcrumb trail at the top is 'Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...'. The 'General Properties' section contains the following fields:

Name	citrix_connect_proxy	
Destination	Type:	<input checked="" type="radio"/> Host <input type="radio"/> Network
	Address:	192.168.0.1
Service Port	443	HTTPS
State	Enabled	

**Figure 2.2** General properties of the virtual server

7. From the **HTTP Profile** list, select the profile you created in *Creating the HTTP profile*, on page 2-5. In our example, we select **xenapp-http**.
8. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*, on page 2-4. In our example, we select **xenapp-https**.
9. In the Resources section, from the **iRule Available** list, select the iRule you created in *Creating the iRule*, on page 6 and click the Add (<<) button (see Figure 2.3).
10. Click the **Finished** button.



*Figure 2.3 Resources section of the virtual server*

## Disabling ARP requests

Address Resolution Protocol (ARP) requests are not needed for this virtual server, and no external requests should reach this virtual server. In this section we disable ARP requests in order to limit any issues with duplication of IPs or broadcast of traffic of this IP address outside of the box.

The Citrix connect proxy is an internal only proxy used to handle portions of the connection traffic.

### To disable ARP replies

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. From the Menu bar, click **Virtual Address List**.
3. In the Address column, click the IP address associated with the virtual server (in our example 192.0.2.102).  
The General Properties page opens.
4. In the Configuration section, from the ARP row, clear the check box to disable ARP (see Figure 2.4).
5. Click the **Update** button.

You have now disabled ARP requests for this virtual.

---

Local Traffic » Virtual Servers : Virtual Address List » 192.0.2.102

⚙️

Properties

Statistics

**General Properties**

Address	192.168.0.1
Partition	Common
Availability	<div></div>
State	Enabled

**Configuration**

Advertise Route	When any virtual server is available
Connection Limit	0
ARP	<input checked="" type="checkbox"/> Enabled
Route Advertisement	<input type="checkbox"/>

Update

**Figure 2.4** Virtual Address properties

## Configuring the BIG-IP LTM for authentication

For Single Sign On authentication to work properly, you must configure BIG-IP LTM authentication. This requires configuring DNS and NTP settings on the BIG-IP LTM.

### Configuring the DNS settings on the BIG-IP LTM

The first task in this section is to configure the DNS settings on the BIG-IP LTM to point to the Active Directory server.

---

◆ **Note**

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

---

◆ **Important**

*The BIG-IP LTM 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 LTM, see the online help or the product documentation.*

#### To configure DNS settings on the BIG-IP LTM

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 (see Figure 2.5).
4. Click **Update**.

---

The screenshot shows a web-based configuration interface for DNS settings. At the top, there is a breadcrumb trail: "System » Configuration : Device : DNS". Below this is a navigation bar with tabs: "Device" (selected), "Local Traffic", and "Global Traffic". The main content area is titled "Properties" and contains four sections:

- DNS Lookup Server List:** Includes an "Address:" input field with "192.0.2.143", an "Add" button, a list box containing "192.0.2.143", and "Edit" and "Delete" buttons.
- BIND Forwarder Server List:** Includes an empty "Address:" input field, an "Add" button, an empty list box, and "Edit" and "Delete" buttons.
- DNS Search Domain List:** Includes an empty "Address:" input field, an "Add" button, an empty list box, and "Edit" and "Delete" buttons.
- DNS Cache:** Includes a checkbox that is currently unchecked.

At the bottom of the "Properties" section is an "Update" button.

*Figure 2.5 DNS configuration properties*

## Configuring the NTP settings on the BIG-IP LTM

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

### To configure NTP settings on the BIG-IP LTM

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**.

# Configuring the BIG-IP APM for Citrix Secure Proxy

In this section, we configure the Access Policy Manager for the Citrix Secure Proxy. This is the main entry point into the configuration.

## Choosing an authentication mechanism

This guide documents two methods of authentication when integrating BIG-IP APM Secure Proxy mode with your Citrix XenApp environment. The main difference is the ability to support RSA Two-Factor (or token based) authentication, and password-only authentication. We refer to the RSA authentication method in terms of Citrix's terminology as **Access Gateway mode**. For password-only authentication without two factor authentication, we refer to **Non-Access Gateway mode** or simply **standard mode**.

### Important

---

*In this section, there are certain configuration objects that have different procedures depending on which mode you choose. These are clearly marked with **OPTIONAL** in the heading.*

## Standard authentication

Unless you are using Citrix Receiver with RSA SecurID, you configure your authentication with standard, non-access gateway mode authentication. Authentication is carried out through password authentication. In this guide, we demonstrate the configuration of password authentication against Active Directory.

The BIG-IP APM caches users credentials so that users do not have to enter their user name and password twice.

## Access Gateway authentication for Citrix Receiver clients

For Citrix Receiver clients, configuring Access Gateway mode allows administrators to use RSA Two Factor authentication. For Access Gateway mode we use the BIG-IP APM Visual Policy Editor (VPE) to create an access policy that detects which client users are connecting from and authenticates the user to the correct source.

The BIG-IP APM caches users credentials so that users do not have to enter their user name and password twice.

---

## Creating a AAA Server

The BIG-IP APM does not have a built-in authentication store therefore an authentication source must be specified. In the following example, we use Active Directory authentication; you may be using LDAP or another authentication source. Configure as appropriate for your implementation.

### ◆ Important

*If you are using Access Gateway mode, there is an additional AAA server to create, which uses RSA SecurID (however, you still configure the following AAA server).*

### To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Citrix\_domain**.
4. From the **Type** list, select the authentication method appropriate for your implementation. In this example, we select **Active Directory**.
5. In the Configuration section, type the appropriate information relevant to your authentication method. In our Active Directory example, we provide the Domain Controller IP address, the Domain Name, the Admin Name, the Admin Password and we leave the timeout at default.
6. Click **Finished**.

The screenshot shows a configuration window titled "Access Policy » AAA Servers » New Server...". It is divided into two main sections: "General Properties" and "Configuration".

**General Properties**

Name	Citrix_domain
Type	Active Directory

**Configuration**

Domain Controller	192.0.2.145
Domain Name	mydomain.example.com
Admin Name	admin
Admin Password	.....
Verify Admin Password	.....
Timeout	15 seconds

At the bottom, there are two buttons: "Cancel" and "Finished".

**Figure 2.6** AAA server configuration

## OPTIONAL: Configuring an additional AAA server for Access Gateway mode

*If you are using Access Gateway mode for Citrix Receiver, you must configure **an additional** AAA server for RSA SecurID.*

---

### ◆ Note

*If you are **not** using Access Gateway mode, you do not configure this AAA server, continue with **Creating the SSO configuration**, on page 15.*

For RSA SecurID, you need to have the SecurID Configuration file ready to upload from an accessible location, and the RSA device must already be configured to accept connections from the BIG-IP. For additional information about RSA SecurID, see the RSA documentation.

By configuring RSA SecurID as an authentication source, the BIG-IP APM proxies the authentication connection as part of the traffic flow for the Access Gateway connection.

You should already have a self IP address on the BIG-IP system that matches the IP address in the SecurID configuration File. If not, configure the self IP address before beginning this procedure. For specific instructions on configuring a self IP address, see the online help or BIG-IP documentation.

---

### ◆ Important

*You only need to configure this AAA server if you are using Access Gateway mode.*

### To create an AAA server with RSA SecurID

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Citrix\_SecurID**.
4. From the **Type** list, select **SecurID**.
5. In the Agent Host IP Address section, click the **Select from Self IP List** button. From the list, select the appropriate self IP address that matches the IP address in the SecurID configuration file.
6. In the **SecurID Configuration File** box, type the path to the SecurID configuration file, or click **Browse** and locate the file.
7. In the **File Description** box, you can optionally type a description.
8. Click **Finished**.

This is the end of this Optional section for Citrix Receiver Access Gateway mode.



---

## Creating the SSO configuration

The next task is to create a Single Sign-On Configuration that defines the credentials that are cached.

### ◆ Note

*You must complete this section no matter with authentication mechanism you are using.*

### To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **SSO Configurations**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **CitrixSSO**.
4. From the **SSO Method** list, select **Form Based**.
5. In the **Username Source** box, type the user name source. In our example, we leave the default: **session.sso.token.last.username**.
6. In the **Password Source** box, type the user name source. In our example, we leave the default: **session.sso.token.last.password**.
7. In the **Start URI** box, type **/Citrix/XenApp/auth/login.aspx**
8. From the **Form Method** box, select **POST**.
9. In the **Form Action** box, type **/Citrix/XenApp/auth/login.aspx**.
10. In the **Form Parameter For User Name** box, type **user**.
11. In the **Form Parameter For Parameter** box, type **password**.
12. In the **Hidden Form Parameters/Values** box, use the following syntax:

**domain <domain-name>**  
**LoginType Explicit**

***Note:** For domain, you must enter the Active Directory domain name for the users being authenticated.*

In our example, we type

**domain LABDOMAIN**  
**LoginType Explicit**

13. From the **Successful Logon Detection Match Type** list, select **By Resulting Redirect URL**.
14. In the **Successful Logon Detection Match Value** box, type **/Citrix/XenApp/site/default.aspx** (see Figure 2.7).

15. Click **Finished**.

#### ◆ Note

*In this SSO configuration we have documented the default installation for XenApp Web Interface which results in URLs beginning with **/Citrix/XenApp/**. If your default Web Interface is differently named (such as **DesktopWeb**) you have to adjust the URLs in this procedure accordingly.*

Access Policy » SSO Configurations » New SSO Configuration...	
<b>General Properties</b>	
Name	CitrixSSO
SSO Method	Form Based
<b>Configuration</b>	
Username Source	session.sso.token.last.username
Password Source	session.sso.token.last.password
Start URI	/Citrix/XenApp/auth/login.aspx
Form Method	POST
Form Action	/Citrix/XenApp/auth/login.aspx
Form Parameter For User Name	user
Form Parameter For Password	password
Hidden Form Parameters/Values	domain LABDOMAIN LoginType Explicit
Successful Logon Detection Match Type	By Resulting Redirect URL
Successful Logon Detection Match Value	/Citrix/XenApp/site/default.aspx
<input type="button" value="Cancel"/> <input type="button" value="Finished"/>	

**Figure 2.7** New SSO Configuration page

## Creating an Access Profile

The next task in this section is to create an Access profile. How you configure the Access Policy depends on whether you are using Access Gateway mode.

- If you are not using **Access Gateway mode**, use *Creating an Access Profile when not using Access Gateway mode*, on page 2-17

- 
- If you are using **Access Gateway mode**, use *OPTIONAL: Creating an Access Profile in Access Gateway mode*, on page 2-21

---

◆ **Important**

*Only use the section relevant to your configuration.*

## Creating an Access Profile when not using Access Gateway mode

Use the following procedures to create an Access profile *if you are not using Access Gateway mode*.

---

◆ **Important**

*This section is only if you are **not** using Access Gateway mode. If you are using Access Gateway mode, go back to **OPTIONAL: Creating an Access Profile in Access Gateway mode**, on page 2-21, or if you are finished, continue with **Creating the profiles**, on page 2-29.*

### To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Citrix-standard-authentication**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the **SSO Configuration** list, select the SSO configuration you created in *Creating the SSO configuration*, on page 2-15. In our example, we select **CitrixSSO**.
6. Configure the rest of the settings in the Configuration section as applicable to your environment. In our example, we leave **Secure Cookie** checked.
7. In the Language Settings section, if you are deploying in a language other than English, configure as applicable for your language.
8. Click **Finished**

## Editing the Access Profile with the Visual Policy Editor for non Access Gateway mode

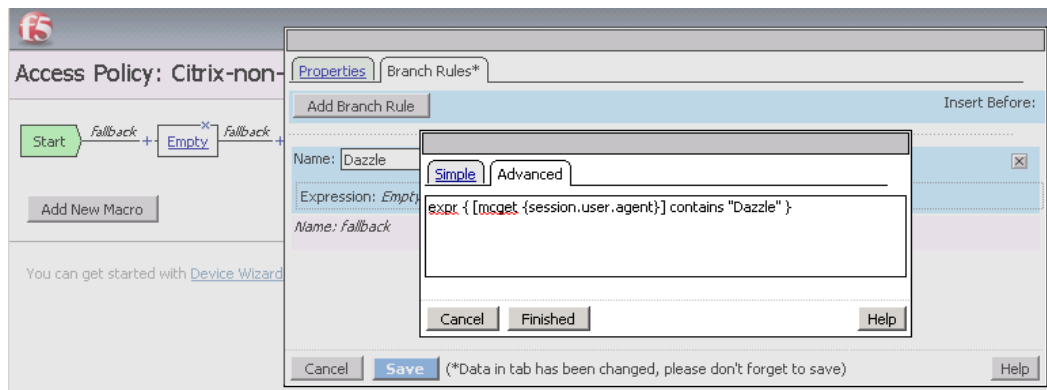
The next task is to edit the Access Policy you just created using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

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 for non-Access Gateway mode

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you just created, and 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 **Empty** option button, and then click **Add Item**. The Properties box opens.
  - a) In the **Name** box, type a name. In our example, we type **User Agent Check**.
  - b) Click the *Branch Rules* tab.
  - c) Click **Add Branch Rule**.
  - d) In the **Name** box, type **Dazzle**.
  - e) Click the **change** link, and then click the *Advanced* tab.
  - f) In the box, copy and paste the following expression:
 

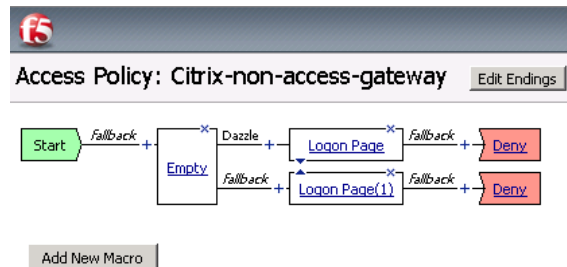
```
expr { [mcget {session.user.agent}] contains "Dazzle" }
```
  - g) Click **Finished**.
  - h) Click **Save**.



**Figure 2.8** Branch Rule configuration for the Empty VPE object

5. Click the + symbol between **Dazzle** and **Deny**.
6. Click the **Logon Page** option button, and then click **Add Item**.
7. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.

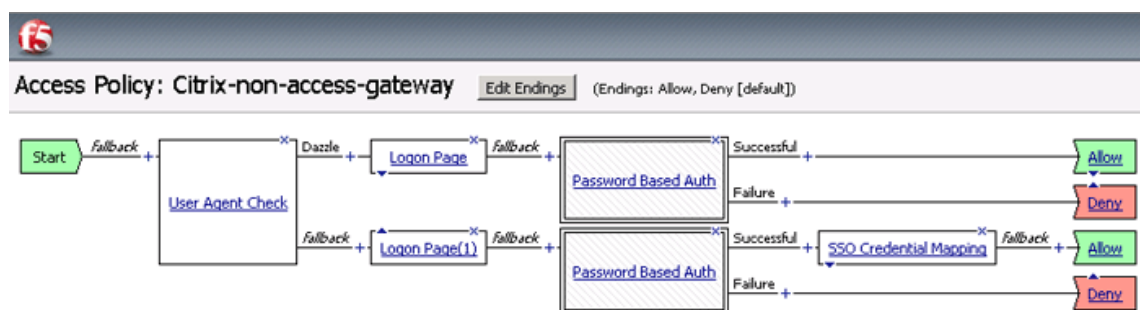
8. Click the **Save** button.
9. Repeat steps 5-7 for the **Fallback** path. After completing this step, your VPE should look like the following.



*Figure 2.9 VPE after configuring the Logon Page options*

10. Click the **Add New Macro** button. The new macro box opens.
  - a) In the **Name** box, type a name for this macro. In our example, we type **Password Based Auth**.
  - b) Click the **Save** button. The Macro appears under the Access Policy.
  - c) Click the Expand (+) button next to **Password Based Auth**.
  - d) Click the + symbol between **In** and **Out**. A box opens with options for different actions.
  - e) Click the **AD Auth** option button, and then click **Add Item**.
  - f) From the **Server** list, select the name of the AAA server you created in *Creating a AAA Server*, on page 2-13. We select **Citrix\_domain**.
  - g) Configure the rest of the Active Directory options as applicable, and then click **Save**. You now see two paths, **Successful** and **Fallback**.
  - h) Click the **Edit Terminals** button to the right of the Macro Name.
  - i) In the **Name** box, type **Successful**. The list to the right should be on a green #1.
  - j) Click **Add Terminal**.
  - k) In the **Name** box, type **Failure**. The list to the right should be on a red #2.
  - l) Click the Up arrow to the right of Successful to move it up.
  - m) Click **Save**.
  - n) Back in the Macro, on the *fallback* path, click the **Successful** box, click **Failure**, and then click **Save**.  
When you are finished, your macro should look like Figure 2.15, on page 2-25.

11. On the *Dazzle* path, click the **+** symbol between **Logon Page** and **Deny**. The box opens with different actions. There is now a section at the top for Macrocalls.
  12. In the Macrocalls section, click the option button for the Macro you just created, and then click the **Add Item** button. In our example, we click **Password Based Auth**.
  13. On the Successful path between **Password Based Auth** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**. This completes the Dazzle path.
  14. Click the **+** symbol on the *fallback* path between **Logon Page** and **Deny**. The options box opens.
  15. In the Macrocalls section, click the option button for the Macro you created, and then click the **Add Item** button. In our example, we click **Password Based Auth**.
  16. Click the **+** symbol on the *Successful* path between **Password Based Auth** and **Deny**. The options box opens
  17. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
  18. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
- Note: The Logon page can be customized to match the look-and-feel of your organization. For further information about this, see the BIG-IP APM Configuration Guide. If you do choose to customize the Logon page, we recommend creating the Logon item as a Macro (using step 10 as a guideline).*
19. Click the **Save** button.
  20. On the *fallback* path between **SSO Credential Mapping** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**. When you are finished, the VPE should look like Figure 2.10, on page 2-20.
  21. 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.
  22. Click the **Close** button on the upper right to close the VPE.



**Figure 2.10** Completed VPE in non-Access Gateway mode

---

This completes the Access Profile and Visual Policy Editor configuration for the Standard/Non-Access Gateway mode. Continue with *Creating the profiles*, on page 2-29.

## OPTIONAL: Creating an Access Profile in Access Gateway mode

Use the following procedure *if you are using Access Gateway mode for Citrix Receiver clients*. This includes creating the Access Profile and editing the profile with the Visual Policy Editor.

### Important

---

*If you are not using Access Gateway mode, go directly to **Creating an Access Profile when not using Access Gateway mode**, on page 2-17.*

#### To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Citrix-ICA-SecureProxy**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the **SSO Configuration** list, select the SSO configuration you created in *Creating the SSO configuration*, on page 2-15. In our example, we select **CitrixSSO**.
6. Configure the rest of the settings in the Configuration section as applicable to your environment. In our example, we leave **Secure Cookie** checked.
7. In the Language Settings section, if you are deploying in a language other than English, configure as applicable for your language.
8. Click **Finished** (see Figure 2.11, on page 2-22).

General Properties		
Name	Citrix-ICA-SecureProxy	
Parent Profile	access	

Settings		
Inactivity Timeout	900	seconds <input type="checkbox"/>
Access Policy Timeout	300	seconds <input type="checkbox"/>
Maximum Session Timeout	0	seconds <input type="checkbox"/>
Max Concurrent Users	0	<input type="checkbox"/>
Max Sessions Per User	0	<input type="checkbox"/>

Configurations	
SSO Configuration	+ CitrixSSO
Domain Cookie	
Secure Cookie	<input checked="" type="checkbox"/> Enabled

**Figure 2.11** New Access Profile (truncated to show relevant settings)

## Editing the Access Profile with the Visual Policy Editor for Access Gateway mode

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

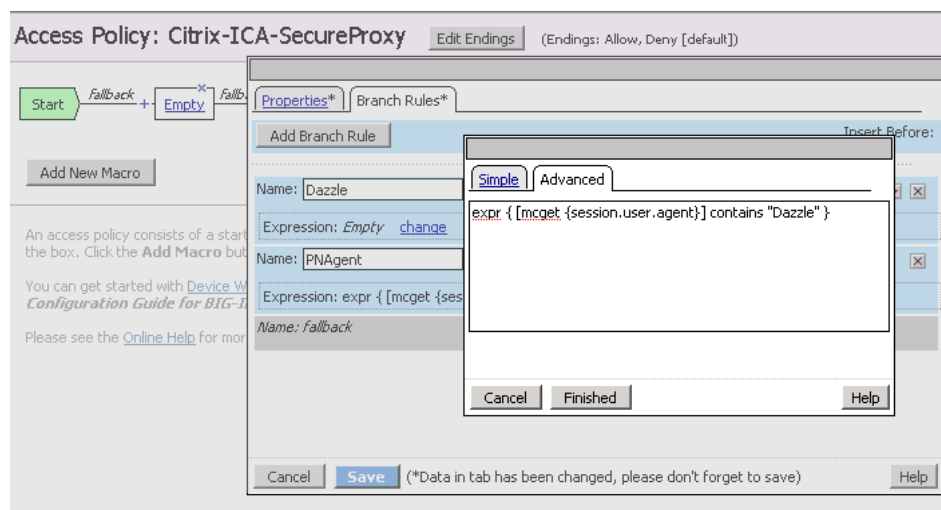
For additional or more sophisticated authentication and policy options, see the *Configuration Guide for BIG-IP Access Policy Manager*, available on Ask F5 (<https://support.f5.com/>).

### To edit the Access Profile for Access Gateway mode

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you just created, and 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 **Empty** option button, and then click **Add Item**. The Properties box opens.
  - a) In the **Name** box, type a name. In our example, we type **User Agent Check**.
  - b) Click the *Branch Rules* tab.
  - c) Click **Add Branch Rule**.
  - d) In the **Name** box, type a name. We type **PNAgent**.

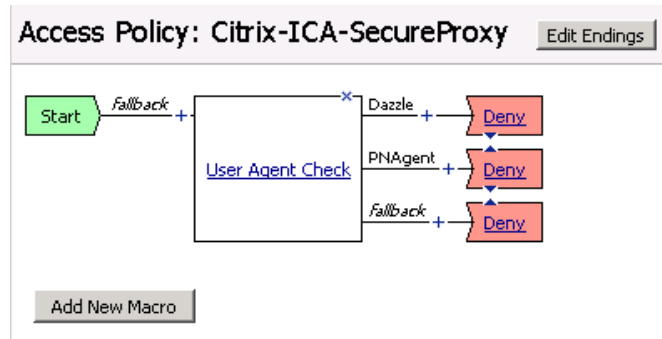


- 
- e) Click the **change** link. The Add Expression box opens.
- f) Click the *Advanced* tab.
- g) In the box, copy and paste the following expression:
- ```
expr { [mcget {session.user.agent}] contains "PNAMAIN" or [mcget {session.user.agent}] contains "PNAMain" }
```
- h) Click **Finished**.
- i) Click **Add Branch Rule** again.
- j) In the new **Name** box (called *Branch Rule 2*), type **Dazzle**.
- k) Click the **change** link, and then click the *Advanced* tab.
- l) In the box, copy and paste the following expression:
- ```
expr { [mcget {session.user.agent}] contains "Dazzle" }
```
- See Figure 2.12.
- m) Click **Finished**.
- n) Click **Save**.



**Figure 2.12** Branch Rule configuration for the Empty VPE object

When you are finished with the Branch rules in the Empty VPE object, your Visual Policy should look like the following.



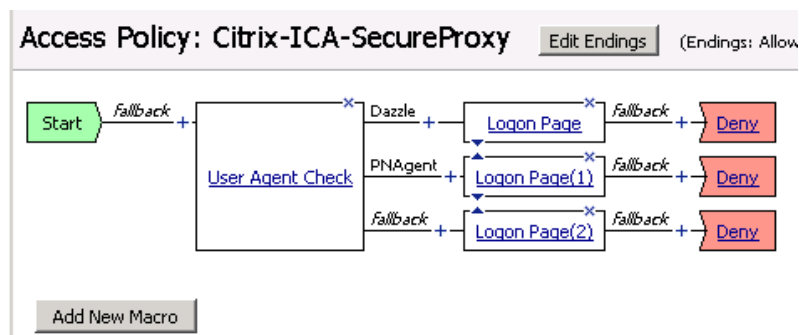
**Figure 2.13** VPE after configuring the Empty object

5. Click the + symbol between **Dazzle** and **Deny**.
6. Click the **Logon Page** option button, and then click **Add Item**.
7. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.

***Note:** The Logon page can be customized to match the look-and-feel of your organization. For further information about this, see the BIG-IP APM Configuration Guide. If you do choose to customize the Logon page, we recommend creating the Logon item as a Macro (using step 10 as a guideline).*

8. Click the **Save** button.
9. Repeat steps 5-7 for the **PNAgent** and **Fallback** paths.

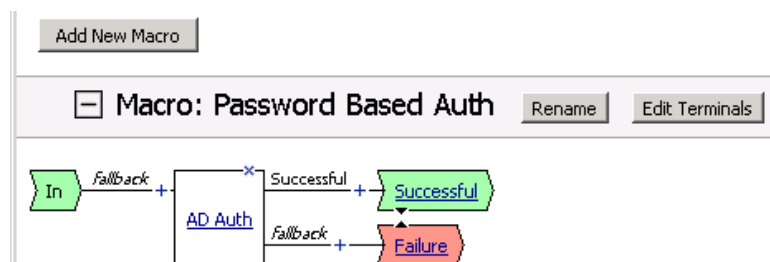
Your VPE should now look like the following:



**Figure 2.14** VPE after adding the Logon Pages

10. Click the **Add New Macro** button. The new macro box opens.
  - a) Leave the **Select macro template** list set to **Empty**.

- b) In the **Name** box, type a name for this macro. In our example, we type **Password Based Auth**.
  - c) Click the **Save** button. The Macro appears under the Access Policy.
  - d) Click the Expand (+) button next to **Password Based Auth**.
  - e) Click the + symbol between **In** and **Out**. A box opens with options for different actions.
  - f) Click the **AD Auth** option button, and then click **Add Item**.
  - g) From the **Server** list, select the name of the AAA server you created in *Creating a AAA Server*, on page 2-13. We select **Citrix\_domain**.
  - h) Configure the rest of the Active Directory options as applicable, and then click **Save**. You now see two paths, **Successful** and **Fallback**.
  - i) Click the **Edit Terminals** button to the right of the Macro Name.
  - j) In the **Name** box, type **Successful**. The list to the right should be on a green #1.
  - k) Click **Add Terminal**.
  - l) In the **Name** box, type **Failure**. The list to the right should be on a red #2.
  - m) Click the Up arrow to the right of Successful to move it up.
  - n) Click **Save**.
  - o) Back in the Macro, on the *fallback* path, click the **Successful** box, click **Failure**, and then click **Save**.
- When you are finished, your macro should look like the following:



**Figure 2.15** Completed Macro configuration

11. Click the + symbol on the *Dazzle* path between **Logon Page** and **Deny**. The box opens with different actions. There is now a section at the top for Macrocalls.

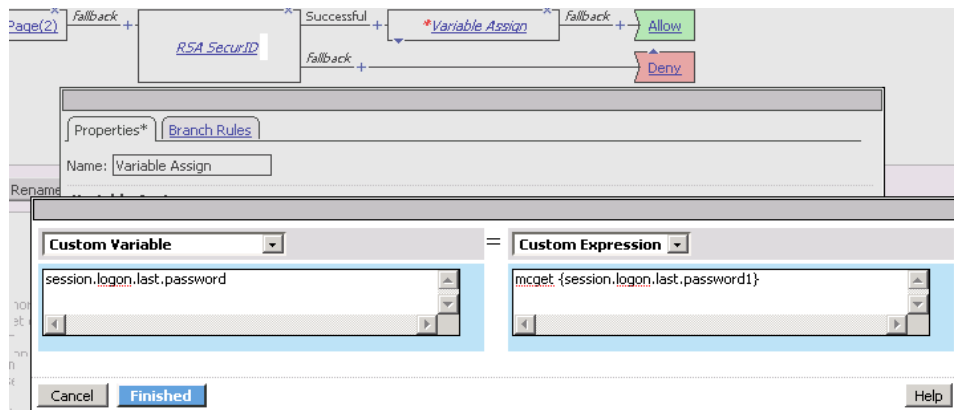
12. In the Macrocalls section, click the option button for the Macro you just created, and then click **Add Item**. In our example, we click **Password Based Auth**.
13. On the *Dazzle* Successful path after Password Based Auth, click the **Deny** box. In the **Select Ending** box, click **Allow** and then click the **Save** button.  
This completes the Dazzle path.
14. On the *PNAgent* path between **Logon Page(1)** and **Deny**, click the + symbol.
15. In the Macrocalls section, click the option button for the Macro you just created, and then click **Add Item**. In our example, we click **Password Based Auth**.
16. Click **Save**.
17. On the *PNAgent* Successful path, click the + symbol between **Password Based Auth** and **Deny**.
18. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
19. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
20. Click the **Save** button.
21. On the *PNAgent* Successful path after SSO Credential Mapping, click the **Deny** box, click **Allow**, and then click **Save**.  
This completes the PNAgent path.
22. Click the + symbol on the *fallback* path between **Logon Page(2)** and **Deny**.
23. Click **RSA SecurID**, and then click **Add Item**.
  - a) From the **AAA Server** list, select the AAA server for RSA SecurID you created in *OPTIONAL: Configuring an additional AAA server for Access Gateway mode*, on page 2-14.
  - b) From the **Max Logon Attempts Allowed** list, select a number of attempts. In our example, we leave the list at **3**.
  - c) Click **Save**.
24. On the *fallback* Successful path after RSA SecurID, click the **Deny** box, click **Allow**, and then click **Save**.
25. On the Successful path between **RSA SecurID** and **Allow**, click the + symbol.
26. Click the **Variable Assign** button and then click **Add Item**.
27. Click the **Add new entry** button.
28. On the left side, select **Custom Variable** from the list, and then type the following:

`session.logon.last.password`

29. On the right side, select Custom Expression from the list, and then type the following:

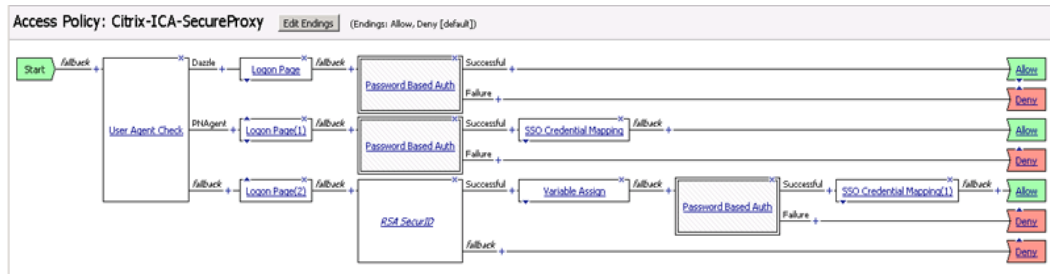
`mcget {session.logon.last.password1}`

30. Click the **Finished** button.



**Figure 2.16** Variable Assign configuration

31. On the Successful path between **Variable Assign** and **Allow**, click the + symbol.
32. In the Macrocalls section, click the option button for the Macro you created, and then click **Add Item**. In our example, we click **Password Based Auth**.
33. On the Successful path between **Password Based Auth** and **Allow**, click the + symbol.
34. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
35. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
36. Click the **Save** button. When you are finished, your VPE should look like Figure 2.17, on page 2-28.
37. 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.
38. Click the **Close** button on the upper right to close the VPE.



**Figure 2.17** Completed VPE for Access Gateway mode

This completes the Optional procedure for Access Gateway mode for Citrix Receiver clients. The remainder of this guide applies to both authentication mechanisms; there are no more optional procedures for Access Gateway mode.

---

## Creating the profiles

You have now created a Visual Policy for either Access Gateway mode or Standard mode. The next task is to create the profiles for this configuration.

### Creating the TCP profiles

The next profiles we create are the TCP profiles. With regard to the TCP profiles and XenApp, 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.

#### Important

*Setting TCP timeout to **Indefinite** may lead to session exhaustion and should be used with care.*

*Optional:* 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>

### Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile. We recommend creating **tcp-lan-optimized** profile, with an additional **tcp-wan-optimized** profile, if you have you have remote users coming in.

#### To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens by default.
2. On the Menu bar, from the **Protocol** menu, select **TCP**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **citrix\_tcp\_lan**.
5. In the **Idle Timeout** row, click the **Custom** box, and then type a number between 600 and 900, depending on your configuration.

6. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

## Creating the WAN optimized TCP profile

The next task is to create the WAN optimized profile. Again, we set the Idle Timeout value to Indefinite to prevent idle desktop sessions from being terminated prematurely.

### To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **Protocol** menu, select **TCP**.
2. Click the **Create** button. The New TCP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **citrix\_tcp\_wan**.
4. In the **Idle Timeout** row, click the **Custom** box, and then type a number between 600 and 900, depending on your configuration.
5. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

## Creating the persistence profile

The next profile we create is a Persistence profile.

### To create a new persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Persistence**.
3. Click the **Create** button. The New Persistence Profile screen opens.
4. In the **Name** box, type a name. In our example, we type **citrix-persistence**.
5. From the **Persistence Type** list, select **Source Address Affinity**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.



---

## Creating an HTTP profile

The next task is to create an HTTP profile. To create the HTTP profile, use the procedure *Creating the HTTP profile*, on page 2-5, using a unique name (we use **xenapp-secureproxy-http**), and with the following exception:

5) From the **Redirect Rewrite** row, check the **Custom** box, and then select **All** from the list.

## Creating the iRule

In this section, we create the iRule for this deployment. The iRule performs three main functions:

- ◆ Intercepts **.ica** files served by Citrix Web Interface servers and patches them to add entries to point Citrix clients to the CitrixICAPatcher virtual server as their HTTPS Proxy. This also injects APM login credentials so there is no need for the Citrix client to request the user to authenticate to the proxy.
- ◆ Identifies Secure Proxy connections and begins to process them. Once the user is authenticated, it sets APM session information and passes the user to the connect proxy virtual server you created in *Creating the virtual server*, on page 2-6.
- ◆ Identifies whether the client is a Program Neighborhood, Citrix Receiver, or Mac Dazzle client. The connection is then handled appropriately because the connection is not a standard Web Interface user.

### ◆ Note

*Because the iRule would span more than a page in this guide, the copy and paste operation would be complicated. Therefore, the source for the iRule can be found on DevCentral:*

[http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix\\_APM.html](http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix_APM.html)

### To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the Name box, type a name for this rule. In our example, we type **APM-XenApp**.
4. In the **Definition** box, copy and paste the iRule source from the following DevCentral link:  
[http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix\\_APM.html](http://devcentral.f5.com/wiki/default.aspx/iRules/Citrix_APM.html)
5. Click **Finished**.

## Creating the virtual server

The next task is to create the virtual server that serves as the **main entry point into the deployment**.

As mentioned in the prerequisites section, we assume you have already configured your BIG-IP LTM as described in the Citrix XenApp deployment guide (<http://www.f5.com/pdf/deployment-guides/f5-citrix-xenapp-dg.pdf>). This virtual server references the Citrix Web Interface pool you created in that guide. If you have not configured the pool (and associated health monitor), see the BIG-IP LTM deployment guide for XenApp.

### To create the HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name. We type **CitrixICASecureProxy**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.0.2.101**.

***Note:** 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.*

6. In the **Service Port** box, type **443**.
7. From the **Protocol Profile (Client)** list, select the name of the profile you created in *Creating the WAN optimized TCP profile*. In our example, we select **citrix\_tcp\_wan**. This is optional.
8. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the TCP profiles* section. In our example, we select **citrix\_tcp\_lan**.
9. From the **HTTP Profile** list, select the profile you created in *Creating an HTTP profile*, on page 2-31. We select **xenapp-secureproxy-http**.
10. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*, on page 2-4. We select **xenapp\_https**.
11. From the **SNAT Pool** list, select **Automap**.
12. In the Access Policy section, from the **Access Profile** list, select the appropriate Access Profile you created:

- If you used Standard/Non-Access Gateway mode, select the Access Profile you created in *Creating an Access Profile when not using Access Gateway mode*, on page 2-17.
  - If you used Access Gateway mode for Citrix Receiver clients, select the Access Profile you created in *OPTIONAL: Creating an Access Profile in Access Gateway mode*, on page 2-21.
13. In the Resources section, from the **iRule Available** list, select the iRule you created in *Creating the iRule*, on page 2-31 and click the Add (<<) button.
  14. From the **Default Pool** list, select the pool you created for the Citrix Web Interface devices (in the LTM deployment guide or in Appendix B). In our example, we select **citrix-web\_pool**.
  15. From the **Default Persistence Profile** list, select the profile you created in *Creating the persistence profile*, on page 2-30.
  16. Click the **Finished** button (see Figure 2.18).

Access Policy	
Access Profile	Citrix-ICA-SecurePolicy
Connectivity Profile	None
Rewrite Profile	None

WAN Optimization	
iSession Profile	None Context: server
CIFS Profile	None
MAPI Profile	None

Resources	
iRules	<div> <div>Enabled</div> <div>APM-XenApp</div> <div>Up Down</div> </div> <div> <div>Available</div> <div> APM-Citrix-helper  HTTPConnectProxy  HTTPConnectProxy_helper  ICAPatcher  XML_Patcher </div> <div>&lt;&lt; &gt;&gt;</div> </div>
HTTP Class Profiles	<div> <div>Enabled</div> <div></div> <div>Up Down</div> </div> <div> <div>Available</div> <div> DELETEALL_application_httpclass  application-class  httpclass </div> <div>&lt;&lt; &gt;&gt;</div> </div>
Default Pool	+ citrix-web_pool
Default Persistence Profile	citrix-persistence
Fallback Persistence Profile	None

Cancel Repeat Finished

**Figure 2.18** Virtual server configuration

## Appendix A: Citrix Receiver Support with BIG-IP APM secure proxy example for iPhone/iPad

In this Appendix, we provide a sample client application configuration for Apple® iPhone® and iPad™ devices. Citrix Receiver allows users access to applications on their mobile devices such as iPhone, Microsoft® Windows® Mobile, Android™ and Blackberry®. For each device, users install an application that then allows access to installed applications in your XenApp environment.

With BIG-IP Access Policy Module and Local Traffic Module in Secure Proxy mode, control, compliance and acceleration are all possible for mobile device users. The following instructions are intended to show how to configure Apple devices using the Citrix Receiver client and should be similar to the configuration of other devices, although the range of devices used in any organization (and the specific Citrix client configuration) is beyond the scope of this deployment guide.

**No changes are required to your configuration for Citrix Receiver support if all instructions for Secure Proxy in this guide were followed.**

For a complete list of supported devices, visit the Citrix Receiver website.

This Appendix is broken in to the following sections:

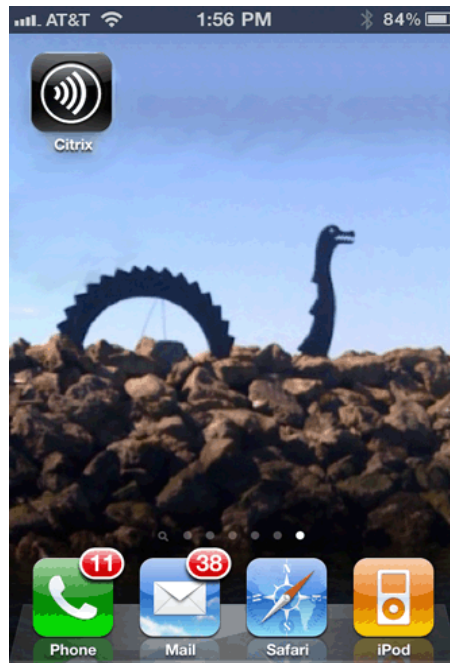
- *Configuring the iPhone for Citrix XenApp Receiver support*
- *Configuring the iPad for Citrix XenApp Receiver support*, on page 2-39

### Configuring the iPhone for Citrix XenApp Receiver support

Use the following procedure to configure the Apple iPhone for XenApp Receiver support.

#### **To configure the iPhone for Citrix XenApp Receiver Support**

1. Download and install the free Citrix Receiver application from the Apple Store for your iPhone.
2. Launch the application by pressing the **Citrix** icon.  
See the following example.



**Figure 2.19** Citrix icon on the Apple iPhone

3. Once you open the Application, you are prompted to create an account or request a trial account. Select **Create an Account**, and then press the plus (+) sign.
4. Complete the General Settings as applicable for your implementation, noting the following:

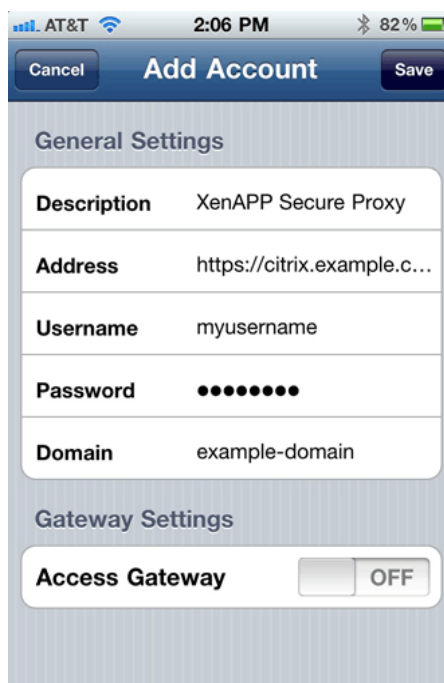
- **Address:** The address should start with **https://** and the URI should resolve to the BIG-IP APM HTTPS virtual server you created in *Creating the virtual server*, on page 2-32.

As an administrator, this is the address you will provide your users.

As a user, be sure to have the correct address from your administrator.

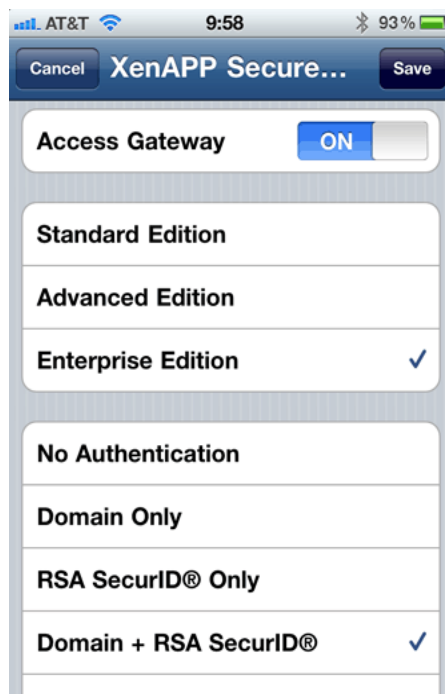
- **Access Gateway:** If you are not using Access Gateway, the setting should be **Off**. If you are using Access Gateway, see Step 5.

Press **Save**.



**Figure 2.20** Add Account page on the iPhone

5. *Optional:* If you are using Access Gateway mode, you need to configure the Access Gateway. Perform the following:
  - a) On the Add Account page, turn the Access Gateway **ON** by swiping the switch.
  - b) In the Edition section, touch **Enterprise Edition**.
  - c) In the Authentication section, touch **Domain + RSA SecurID** (see Figure 2.21).
  - d) Press **Save**.



*Figure 2.21 Optional Access Gateway configuration*

6. Once the account has been created, you see it in the Account list. Press **XenAPP Secure Proxy** to launch the connection.



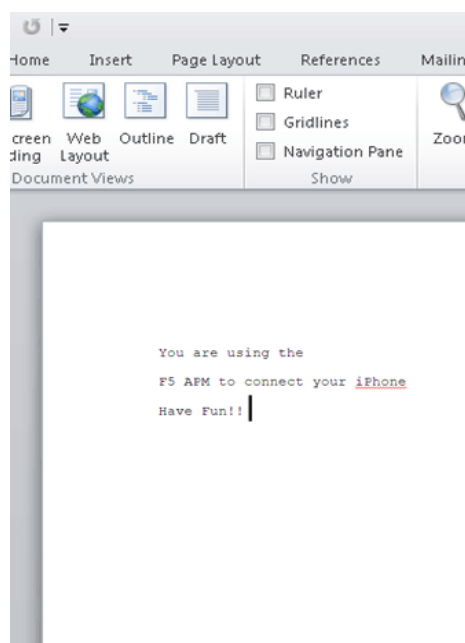
*Figure 2.22 XenApp Secure Proxy Account*

7. You are now logged in and able to see the applications that have been shared. In the following example, Microsoft Word 2010 and Notepad are available.



**Figure 2.23** Available applications

8. To launch an application, press the appropriate line for the application you would like to use. In the following example, we launch Microsoft Word.



**Figure 2.24** Microsoft Word on the iPhone via BIG-IP APM



---

## Configuring the iPad for Citrix XenApp Receiver support

Use the following procedure to configure the Apple iPhone for XenApp Receiver support.

### To configure the iPad for Citrix XenApp Receiver Support

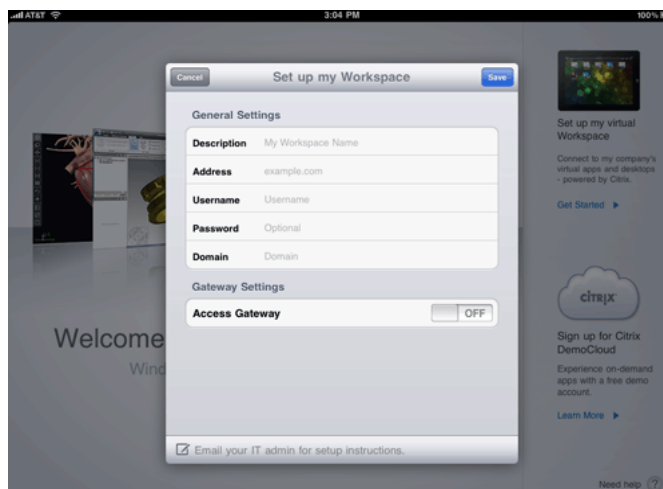
1. Download and install the free Citrix Receiver application from the Apple Store for your iPad.
2. Launch the application by pressing the **Citrix** icon. You see the Welcome screen shown in Figure 2.25.



*Figure 2.25 Citrix Receiver for iPad Welcome screen*

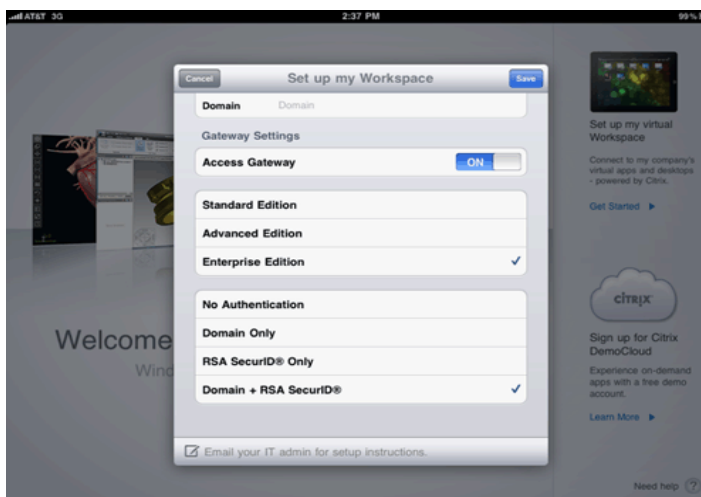
3. In the Right pane, under Set up my virtual Workspace, click **Get Started**. The Set up my Workspace dialog box opens.
4. Complete the General Settings as applicable for your implementation, noting the following:
  - **Address:** The address should start with **https://** and the URI should resolve to the BIG-IP APM HTTPS virtual server you created in *Creating the virtual server*, on page 2-32. As an administrator, this is the address you will provide your users. As a user, be sure to have the correct address from your administrator.
  - **Access Gateway:** If you are not using Access Gateway, the setting should be **Off**. If you are using Access Gateway, see Step 5.

Press **Save**.



*Figure 2.26 Set up my Workspace page on the iPad*

5. *Optional:* If you are using Access Gateway mode, you need to configure the Access Gateway. Perform the following:
  - a) Turn the Access Gateway ON by swiping the switch to ON.
  - b) In the Edition section, touch **Enterprise Edition**.
  - c) In the Authentication section, touch **Domain + RSA SecurID** (see Figure 2.21).
  - d) Click **Save**.



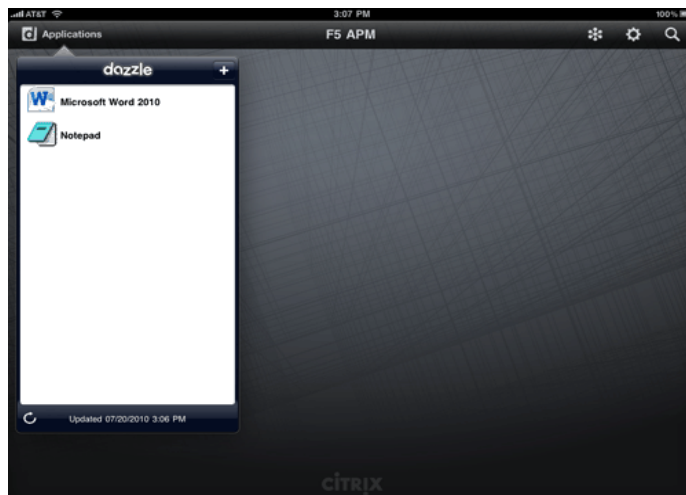
*Figure 2.27 Optional Access Gateway configuration*

- 
6. Once the account has been created, you see a black screen titled F5 APM as shown in the following.



*Figure 2.28 F5 APM page*

7. Click **Applications**. You see the applications that have been shared. In the following example, Microsoft Word 2010 and Notepad are available.



*Figure 2.29 Available applications*

8. To launch an application, press the appropriate line for the application you would like to use.

This completes this appendix.



# 3

---

## Deploying the BIG-IP APM and Citrix XenApp with Remote Network Access

---

---

# Configuring the BIG-IP APM with Citrix XenApp with Remote Network Access

In this chapter, we configure the BIG-IP APM with Citrix XenApp for Remote Network Access. In the Remote Network Access mode, the administrator has total control over the compliance, security, scalability and TCP connections of the Citrix session.

For more detail on the Remote Network Access configuration scenario, see *Configuration example and traffic flow*, on page 3-1.

## Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- ◆ You must have already configured the BIG-IP LTM according to the Deploying the BIG-IP LTM System with Citrix XenApp deployment guide, available at <http://www.f5.com/pdf/deployment-guides/f5-citrix-xenapp-dg.pdf>
- ◆ For this deployment guide, the Citrix XenApp installation must be running version 5.0.
- ◆ For this deployment guide, the BIG-IP LTM system must be running version 10.0 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 *Creating a Client SSL profile*, on page 3-12.
- ◆ Because the current version of the Application Template is for Presentation Server 4.5, **do not** use the Application Template for XenApp 5.0.
- ◆ You must configure DNS and NTP on the BIG-IP LTM system. See *Configuring the BIG-IP LTM system to authenticate against the Active Directory server*, on page 1-12 for specific instructions.

## Configuration example and traffic flow

In the Remote Network Access mode, the user experience takes the following path:

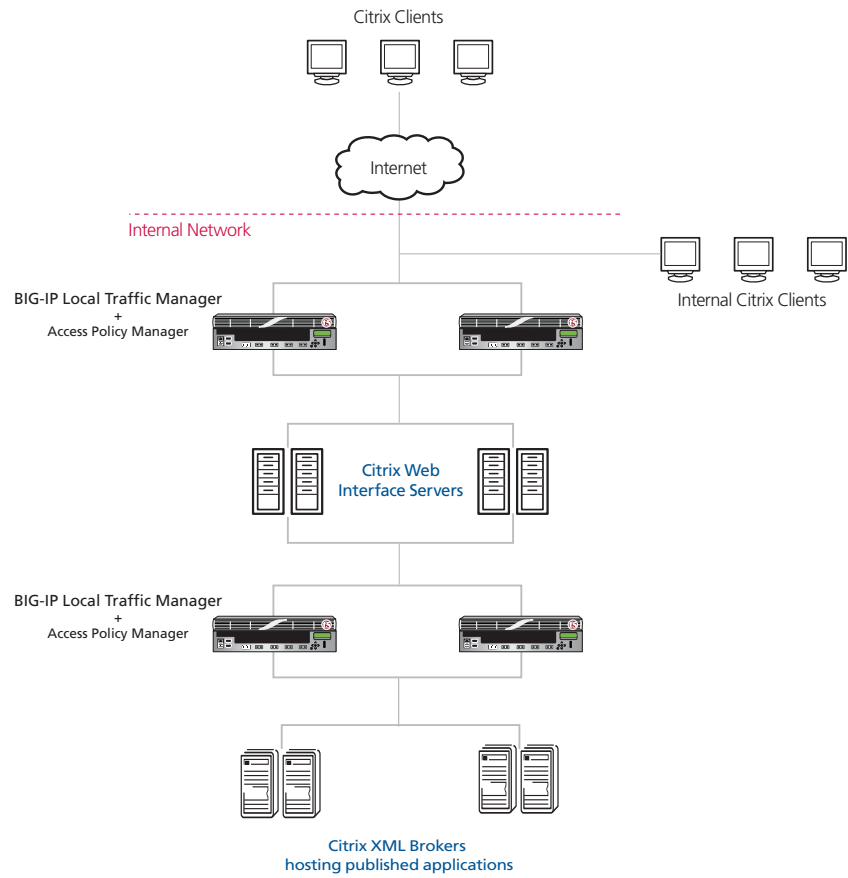
1. The user enters a Virtual Address for Remote Access such as <https://remoteaccess.example.com> into the browser or the user launches the BIG-IP Remote Network Access Edge client.

***Note:** The Edge client needs to be distributed by an administrator ahead of time, or a download link needs to be provided. Otherwise, the user can use any supported browser on all common operating system platforms (Windows, Linux, Mac).*

2. The user is prompted for a user name and password by a customizable login screen on the APM and enters his or her credentials, or the BIG-IP Edge client requests the user name and password.
3. The user is now entered into the internal network and launches a new browser or Citrix ICA client and connects to the Citrix server.
4. The user is asked for the credentials and is logged into Citrix XenApp.

In the Remote Network Access 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://remoteaccess.example.com>. This request is answered by the F5 BIG-IP APM. The APM module creates a secure remote access tunnel using TCP or UDP after authenticating the user against Active Directory or other authentication mechanism. The BIG-IP Client also can be configured to ensure compliance of the user's machine, including whether anti-virus software is installed, the operating system is up-to-date and other compliance criteria such as the country of origin.
2. Once the user enters credentials, the BIG-IP APM contacts Active Directory and authenticates the user's credentials. Once the user is authenticated, a network address lease is provided for the client's machine and a new network interface is setup. The client's routing table is updated to indicate where traffic should flow to for "internal" connections.
3. The administrator now has total control with APM to which internal networks the client can access, at what traffic rates (for example, traffic rate and QOS shaping) and other compliance criteria.



**Figure 1** Logical configuration example

## Configuring the BIG-IP APM

In this configuration, the BIG-IP APM Remote Access virtual server creates the secure remote access tunnel for the users. The Citrix XenApp servers should be configured as recommended in the Citrix XenApp Deployment Guide

(<http://www.f5.com/pdf/deployment-guides/f5-citrix-xenapp-dg.pdf>).

After the secure network access tunnel is established, users then separately launch a browser or Citrix ICA client and connect to the BIG-IP LTM virtual server. Part of this BIG-IP APM configuration is to allow access to the network hosting this BIG-IP LTM virtual server.

## Configuring remote access

To configure Remote Access, a Device Wizard is included in the product that assists in the setup of Network Access. In this guide, we describe the steps to complete the configuration manually.

### To configure remote access

1. On the Main tab, expand **Access Policy**, and then click **Network Access**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this Network Access Profile. In our example, we type **London\_Remote\_Access**. You can optionally type a description.
4. In the General Settings section, next to **Lease Pool**, click the Add (+) button. The Lease Pool is the pool of IP Addresses that clients receive when they connect to the VPN.
  - a) In the **Name** box, type a name for the Lease pool. In our example, we type **London\_Lease\_Pool**.
  - b) Click the **IP Address Range** button.
  - c) In the **Start IP Address** and **End IP Address** boxes, type the appropriate IP addresses. In our example, we allow addresses from **10.0.1.1** to **10.0.1.255**.
  - d) Click the **Add** button.



e) Click the **Finished** button. You return to the Network Access list.

Access Policy >> Network Access : Lease Pools >> New Lease Pool...

**General Properties**

Name: London\_Lease\_Pool

**Configuration**

Type: ☐ IP Address ☒ IP Address Range

Start IP Address: 10.0.1.1

End IP Address: 10.0.1.255

Add

Member List: 10.0.1.1 - 10.0.1.255

Edit Delete

Cancel Finished

**Figure 2** Configuring the Lease Pool

5. If necessary, from the **Lease Pool** list, select the lease pool you just created. In our example, we select **London\_Lease\_Pool**.
6. From the **Compression** list, select **GZIP Compression**. This allows both the web browser client and the thick client to take advantage of compression between the client and the remote access server.

***Note:** If DTLS is configured (UDP based communication between client and Remote Access Server) GZIP compression is automatically disabled. DTLS and GZIP for SSL VPN access is not currently supported.*

Access Policy >> Network Access : Network Access List >> New Resource...

**General Properties**

Name: London\_Remote\_Access

Description:

**General Settings:** Advanced

Lease Pool: London\_Lease\_Pool

Compression: GZIP Compression

SNAT Pool: Auto Map

Session Update Threshold: 0

Session Update Window: 0

**Figure 3** Configuring Network Access

7. From the **Client Settings** list, select **Advanced**.

8. In the Traffic Options section, you can choose to Force all traffic through the tunnel, or use split tunneling. With Split Tunneling enabled, the administrator needs to indicate which subnets should be routed through the VPN tunnel. If Split tunneling is not allowed, all traffic will go through the tunnel.

a) If you want all traffic to go through the tunnel, click **Force all traffic through tunnel**, and continue with Step 8.

b) If you want to use split tunneling, click **Use split tunneling** for traffic. The split tunneling options appear.

- In the LAN Address Space section, type the IP address and Mask of the LAN Address space that should go through the tunnel. In our example we indicate that 192.168.0.0/16 is all LAN space.

***Note:** In this example the BIG-IP LTM Virtual Server front-ending the Citrix ICA server would be located on the 192.168.0.0/16 LAN space.*

- In the DNS Address Space section, type the DNS name(s) that are used in the target LAN.
- In the Exclude Address Space section, type the IP address and Mask of any address space that should be excluded. For example, if a portion of 192.168.0.0/16 should be excluded, it can be entered here. In our example, we indicate that 192.168.10.0/24 is excluded.

9. The remaining options are also administrative, configure the settings as applicable to your configuration. In our testing and architecture we generally recommend the following settings:

a) In the Client Side Security section, we select **Prohibit routing table changes during Network Access Connection**.

b) In the Reconnect To Domain section, we select **Synchronize with Active Directory policies on connection establishment**.

c) In the DTLS section, check the box to enable DTLS. We recommend using DTLS protocol for optimum performance.

***Note:** DTLS uses UDP port 4433 by default. Arrange to open this port on firewalls as needed.  
For DTLS, a UDP Virtual Server is required (described in *Creating the virtual servers, on page 3-13*).*

10. Click **Finished**.

## Creating a Connectivity Profile

The next task is to create a connectivity profile.

---

### To create a connectivity profile

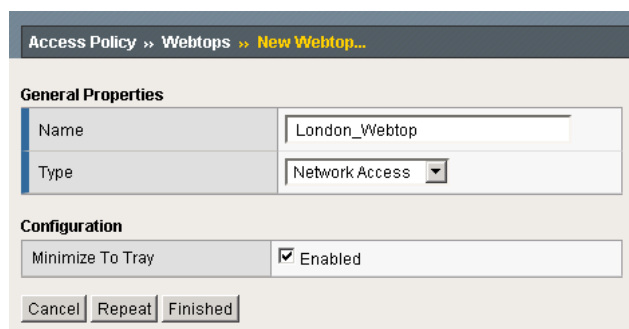
1. On the Main tab, expand **Access Policy**, and then click **Connectivity Profile**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **London\_Connectivity**.
4. Configure the rest of the options as applicable to your configuration. In our example, we leave all settings at the default.
5. Click **Finished**.

## Creating a Webtop

In the BIG-IP Edge, a Network Webtop is used to deliver the BIG-IP Edge client components to the user's web browser session.

### To create a Webtop

1. On the Main tab, expand **Access Policy**, and then click **Webtops**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this webtop. In our example, we type **London\_Webtop**.
4. From the **Type** list, select **Network Access**.
5. If you want the browser window to be minimized to the system tray for Windows hosts, check the **Enabled** box.
6. Click **Finished**.



*Figure 3.1 Webtop configuration*

## Creating an AAA Server

The BIG-IP APM does not have a built-in authentication store therefore an authentication source must be specified. In this procedure, we create an AAA server.

### To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Seattle\_LDAP\_server**.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **LDAP**.
5. In the Configuration section, type the appropriate information relevant to your authentication method. In our LDAP example, we provide the Host name for the LDAP server, the Admin DN, the Admin Password and we leave the timeout at default.
6. Click **Finished**.

## Creating an Access Profile

The Access Profile ties together all of the other pieces in order to create a Network Connection VPN Tunnel. The Access Profile is also where the Visual Policy Editor (VPE) is located, which allows for complex workflows to be designed.

### To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **London\_Access\_Policy**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, configure the settings as applicable to your environment. In our example, we accept all of the defaults.
6. In the Language Settings section, if you are configuring the BIG-IP APM in a language other than English, configure as applicable for your language. In our example, we accept English as the default language.

- 
7. Click **Finished**.

## Editing the Access Profile with the Visual Policy Editor

The next task is to open the London Access Policy and edit the Access Policy 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 detailed information on the VPE please see the product documentation.

In the following procedure, we configure a policy using the Visual Policy Editor. However, Device Wizards provide an easy way to create more interesting policies, including ones that check for Virus Software and other prerequisites before allowing a user to logon. In this guide, it is our goal to get you oriented with the concepts of the Visual Policy Editor. In this example, we create a Login Page, an LDAP auth, and assign the resources allowed.

### To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you just created, and in the Access Policy column, click **Edit**. The Visual Policy Editor opens.
3. Click the + symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.
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**.
8. In the Authentication section, click the **LDAP Auth** option button, and then click the **Add Item** button.
9. From the **Server** list, select the AAA Source you created in *Creating an AAA Server*, on page 3-8.
10. Add **SearchDN** and **SearchFilter** items as applicable.
11. Click the **Save** button. You now see two paths, **Successful** and **Fall Back**.
12. Click the **Deny** box from the path leading from Successful. The Select Ending box opens.
13. Click the **Allow** button, and then click **Save**. In our example, we leave the fallback as Deny.
14. Click the + symbol between **LDAP Auth** and **Allow**.

15. In the General Purpose section, click the **Resource Assign** option button, and then click **Add Item**.
16. Click the **Add new entry** button.
17. Click **Set Network Access Source**, and then click the option button for the Network Access Source you created in *Configuring remote access*, on page 3-4. In our example, we click **London\_Remote\_Access**. This associates the Lease Pool and other settings.  
Click the **Update** button. You return to the Resource Assign page.
18. Click **Set Webtop**, and then click the option button for the Webtop you created in *Creating a Webtop*, on page 3-7. In our example, we click **London\_Webtop**. Click the **Update** button.
19. Click the **Save** button. The Resource Assignment window closes and you return to the Visual Policy Editor main page.  
At this point you have the basics for a functional access policy.
20. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.
21. Click the **Close** button on the upper right to close the VPE.

## Creating the Network Access BIG-IP configuration objects

The next task is to create the external Virtual Server that allows users to initiate their connection to the SSL VPN from either the web browser or the BIG-IP Edge Client for Windows. In our example, we have chosen to allow DTLS as a connection method and we will create two virtual servers, one for TCP 443 and one for UDP 4433.

The first task is to create profiles that are used by the virtual servers.

## Creating the profiles

The next step is to create the profiles. Although you may use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. By creating new profiles, you may easily modify the profile settings specific to your deployment without altering default global behaviors.

## Creating the TCP profiles

The next profiles we create are the TCP profiles. With regard to the TCP profiles and XenApp, 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.

◆ **Important**

*Setting TCP timeout to **Indefinite** may lead to session exhaustion and should be used with care.*

*Optional:* 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>

## Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile. We recommend creating **tcp-lan-optimized** profile, with an additional **tcp-wan-optimized** profile, if you have you have remote users coming in.

### To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens by default.
2. On the Menu bar, from the **Protocol** menu, select **TCP**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **edge\_tcp\_lan**.
5. In the **Idle Timeout** row, click the **Custom** box, and then type a number between 600 and 900, depending on your configuration.
6. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

## Creating the WAN optimized TCP profile

The next task is to create the WAN optimized profile. Again, we set the Idle Timeout value to Indefinite to prevent idle desktop sessions from being terminated prematurely.

### To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **Protocol** menu, select **TCP**.
2. Click the **Create** button. The New TCP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **edge\_tcp\_wan**.
4. In the **Idle Timeout** row, click the **Custom** box, and then type a number between 600 and 900, depending on your configuration.
5. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

## Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required for the VPN to function. This should be a simple HTTP profile with no optimization (compression or caching).

### To create the HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name for this profile. In our example, we type **edge-http**.
3. Modify any of the settings as applicable for your network, but **do not** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
4. Click the **Finished** button.

## Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

### To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
3. In the upper right corner of the screen, click **Import**.



- 
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
  5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
  6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
  7. Click **Import**.
  8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

### To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **edge\_https**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

## Creating the virtual servers

The next task is to create the virtual servers for TCP 443 and UDP 4433.

### To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **edge-tcp-443**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.20.200**.

6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. In the Configuration section, select **Advanced** from the list. The Advanced configuration options appear.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **edge\_tcp\_wan**. This is optional.
9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **edge\_tcp\_lan**.
10. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **edge-http**.
11. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **edge\_https**.
12. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 8. In our example, we select **London\_Access\_Policy**.
13. From the **Connectivity Profile** list, select the profile you created in *Creating a Connectivity Profile*, on page 3-6. In our example, we select **London\_Connectivity\_Profile**.
14. Leave the **Rewrite Profile** list set to **None**.
15. **Do not** configure any of the options in the WAN Optimization section.
16. Click the **Finished** button (this virtual server does not have any Resources).
17. Repeat this entire procedure for the UDP virtual server with the following exceptions.
  - In Step 3, give this virtual server a unique name.
  - In Step 5, use the appropriate IP address.
  - In Step 6, in the **Service Port** box, type **4433**.
  - After Step 7, from the **Protocol** list, select **UDP**.
  - All other settings are the same.

This concludes the configuration.