DEPLOYMENT GUIDE
Version 1.1

Deploying the BIG-IP Access Policy Manager and Local Traffic Manager with VMware View 4.5

Table of Contents

Introducing the BIG-IP System 10.2.1 Deployment Guide for VMware View 4.5

Deploying the BIG-IP LTM with VMware View 4.5

Deploying the BIG-IP APM with VMware View 4.5

1

Introducing the BIG-IP System 10.2.1 Deployment Guide for VMware View 4.5

Deploying the BIG-IP 10.2.1 with VMware View 4.5

Welcome to the F5 Deployment Guide for VMware View (formerly Virtual Desktop Infrastructure: VDI). This document provides guidance and configuration procedures for deploying the BIG-IP Local Traffic Manager (LTM) and BIG-IP Access Policy Manager (APM) version 10.2.1 with VMware View 4.5.

The VMware View portfolio of products lets IT run virtual desktops in the datacenter while giving end users a single view of all their applications and data in a familiar, personalized environment on any device at any location.

One of the unique features of this deployment is the ability of the BIG-IP LTM system to persist client to broker connections on a session by session basis. Other implementations commonly use simple/source address persistence, where all the connections from a single IP address are sent to one server. With the iRule described later in this document, the BIG-IP LTM is able to direct traffic with greater precision, resulting in a more uniform load distribution on the connection servers.

The BIG-IP APM provides pre-logon checks to the endpoint device and supports a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. BIG-IP APM can also enforce Active Directory group policies on corporate-owned and non-corporate-owned assets during the duration of the connection. Additionally, once authenticated, BIG-IP APM guarantees the encryption of all VMware View transport protocols, whether natively encrypted or not. With all these features, BIG-IP APM is able to replace the View Security Server.

This guide is broken into two main sections:

- *Configuring the BIG-IP LTM system for VMware View 4.5*, on page 2-1
- *Configuring the BIG-IP APM for View 4.5*, on page 3-1

For more information on the BIG-IP LTM or APM, see ***http://www.f5.com/products/big-ip/.***

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

Using Edge Gateway instead of the APM Module

While this Deployment Guide outlines methods specifically for the APM module on BIG-IP system, the same procedures are applicable to the BIG-IP Edge Gateway. In BIG-IP Edge Gateway deployments, a separate BIG-IP LTM device must be used in order to support advanced persistence for optimal performance and availability of the View environment.

Specifically, if you are deploying this solution on BIG-IP Edge Gateway, follow all of the instructions in this document on your BIG-IP LTM and then follow all of the instructions for deploying BIG-IP APM on your Edge Gateway Device.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	10.2.1
BIG-IP APM	10.2.1
VMware View	4.5

Document Version	Description
1.0	New guide for View 4.5 and 10.2.1
1.1	Added a section on configuring a Webtop for BIG-IP APM. Added a Server SSL profile to the APM virtual server.

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this guide:

- ***Important:*** Do **NOT** run the VMware View Application Template. The current BIG-IP Application Template for View does not support PCoIP in View 4.5. We recommend using this deployment guide for configuring the BIG-IP with VMware View 4.5.
- If you are using or plan to use PC over IP (PCoIP), see the *Special Note about PC over IP*, on page 1-4.
- Because the BIG-IP LTM is offloading SSL for the VMware deployment, this guide does not include VMware Security servers.
- This deployment guide is written with the assumption that VMware server(s), Virtual Center and connection brokers are already configured on the network and are in good working order.
- This deployment guide is written with the assumption that Active Directory is used in your VMware View deployment, according to VMware's installation and administration guidance.
- Your BIG-IP APM device must be configured to point at the Active Directory environment against which your users will be authenticating. The device wizard documented in this guide asks you for this information.
- NTP must be configured on the device. The device wizard documented in this guide will ask you for this information.

- If you are upgrading from VMware View 4.0 to View 4.5, you only need to perform the procedures in *Modifying the VMware configuration*, on page 1-5.
  If you are upgrading from VMware View 4.0 to View 4.5 ***and*** upgrading from BIG-IP version 10.2 to BIG-IP version 10.2.1, we recommend you use this deployment guide to reconfigure the BIG-IP system.
- We recommend you enable direct connections to user's virtual desktops.
- For this deployment guide, the BIG-IP system must be running version 10.2.1. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.

Configuration flow

The following chart for configuring remote access using an Access Policy (read from the bottom to the top) illustrates the setup of Network Access within Access Policy Module. The information about Web Application is included for reference but is not part of the setup for Network Access.

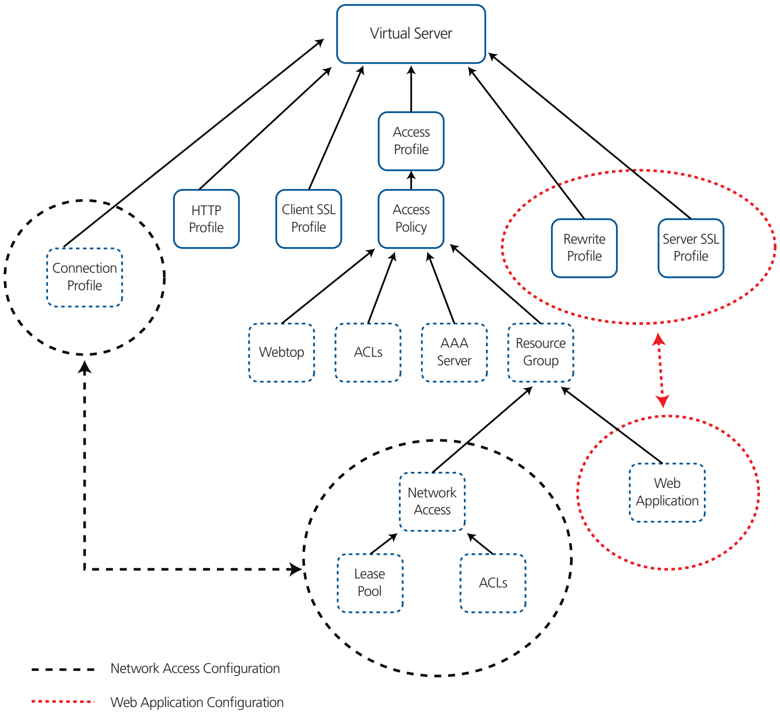


Figure 1.1 *Configuration flow for the Access Policy Module*

Figure 1.2, on page 1-4 is a logical configuration example of this deployment.

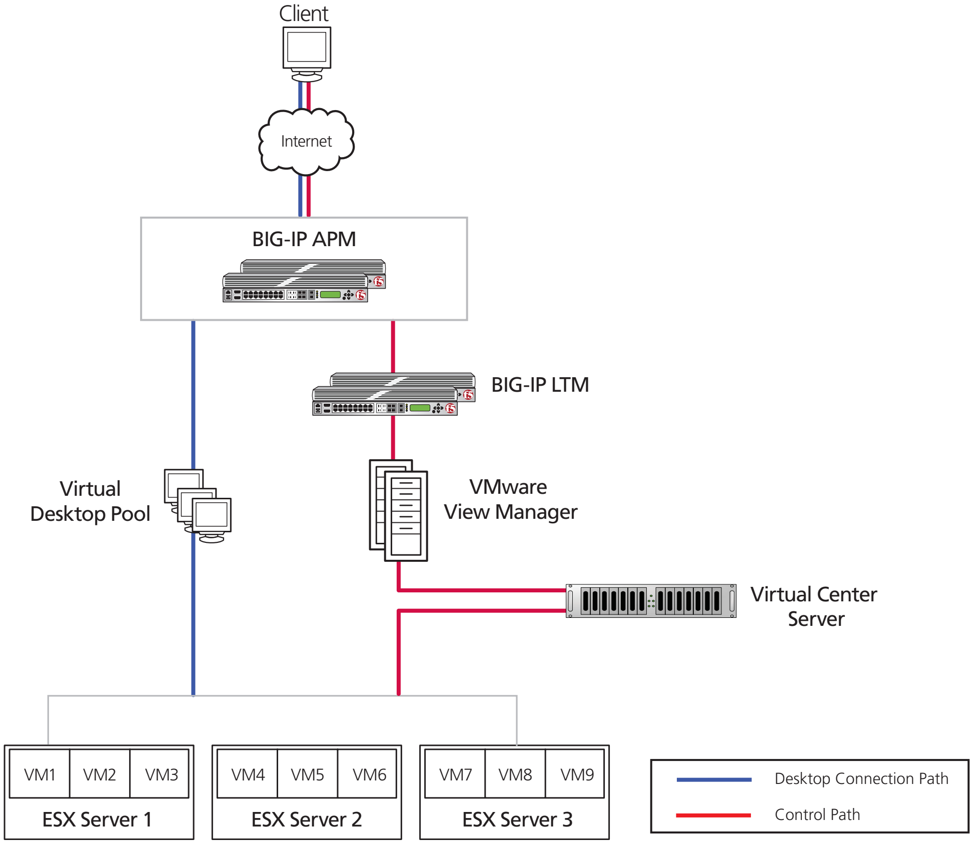


Figure 1.2 *Logical configuration example*

◆ **Note**

APM and LTM may be running on the same device in your environment.

Special Note about PC over IP

Beginning with VMware View 4, VMware supports PC Over IP as a display protocol. PCoIP is an application encrypted UDP protocol, so the BIG-IP system cannot offload encryption for it.

If you want to use PCoIP, we recommend you enable direct connections to the desktop using PCoIP. This means the View client connects to the View Manager server for authentication, authorization and obtaining desktop information. Then, when the users choose a desktop to connect to, the view client opens a new connection directly to the desktop, bypassing the BIG-IP and connection manager. If you are deploying an environment with mixed display protocols, we recommend enabling direct access for all protocols. Refer to the VMware View administrators guide for details.

Modifying the VMware Virtual Desktop Manager global settings

Before starting the BIG-IP LTM configuration, we modify the View configuration to allow the BIG-IP LTM to load balance View client connections and offload SSL transactions. In the following procedure, we disable the SSL requirement for client connections in the Virtual Desktop Manager Administrator tool.

The modifications depend on which version of View you are using. Use the procedure applicable for your deployment.

Modifying the VMware configuration

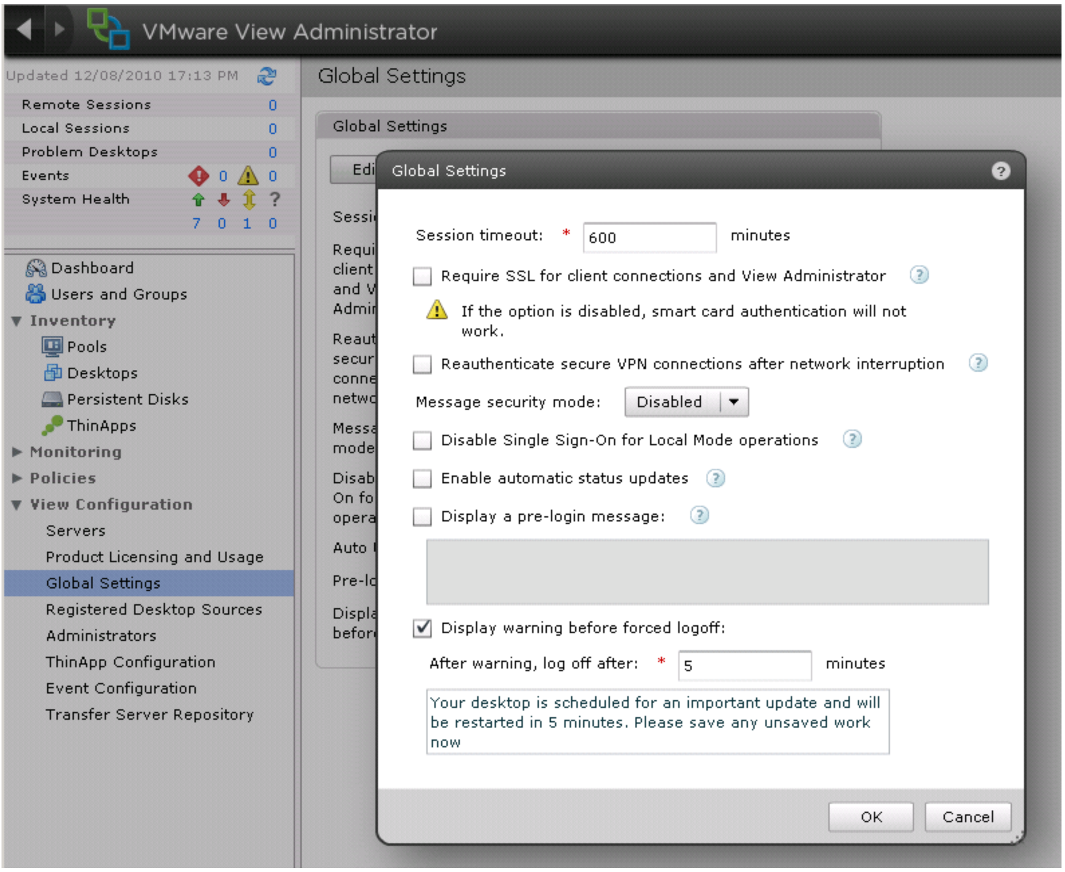
The first task is to modify the View configuration.

◆ **Note**

The following SSL setting applies only to Connection Manager servers, Security servers always require SSL.

To modify the VMware configuration for View 4.5

1. Log on to the View Manager Administrator tool.
2. From the left Navigation pane, click to expand **View Configuration**, and then click **Global Settings**.
   Global Settings page opens in the main pane.
3. Click the **Edit** button.
4. Clear the check from the **Require SSL for client connections** box.
5. Click the **OK** button (see Figure 1.3, on page 1-6).
6. You must reboot or restart the server after making this change. We strongly recommend rebooting.



Session timeout: * 600 minutes

□ Require SSL for client connections and View Administrator

If the option is disabled, smart card authentication will not work.

□ Reauthenticate secure VPN connections after network interruption

Message security mode: Disabled

□ Disable Single Sign-On for Local Mode operations

□ Enable automatic status updates

□ Display a pre-login message:

☑ Display warning before forced logoff:

After warning, log off after: * 5 minutes

Your desktop is scheduled for an important update and will be restarted in 5 minutes. Please save any unsaved work now

Figure 1.3 *View Administrator 4.5 Global Settings*

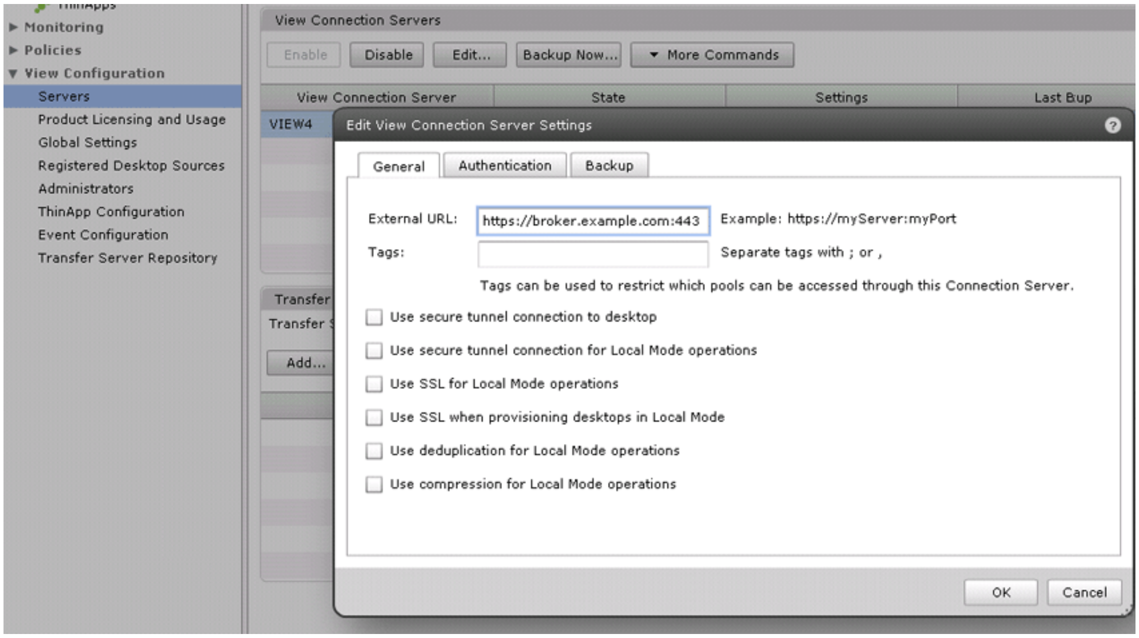
Configuring the External URL

The final modification to the VMware configuration is to configure the server External URL field with the FQDN of the BIG-IP virtual server. This is the server name that clients use to connect to the View Manager pool. Refer to the VMware View Administrator guide for more information. The following procedure must be performed on each VMware View Manager device.

To configure the External URL in View 4.5

1. Log on to the View Manager Administrator tool.
2. From the left Navigation pane, click to expand **View Configuration**, and then click **Servers**.
   The Servers page opens in the main pane.
3. In the *View Connection Servers* box, select a View Connection Server and then click the **Edit** button.

4. In the **External URL** box, type the DNS name you will associate with the BIG-IP LTM virtual IP address, followed by a colon and the port. In our example, we type **https://broker.example.com:443**.
5. Clear the **Use Secure tunnel connection to desktop** box if it is checked.
6. Click the **Ok** button.



Edit View Connection Server Settings

External URL: https://broker.example.com:443 Example: https://myServer:myPort

Tags: Separate tags with ; or ,

Tags can be used to restrict which pools can be accessed through this Connection Server.

□ Use secure tunnel connection to desktop

□ Use secure tunnel connection for Local Mode operations

□ Use SSL for Local Mode operations

□ Use SSL when provisioning desktops in Local Mode

□ Use deduplication for Local Mode operations

□ Use compression for Local Mode operations

Figure 1.4 *View Connection Server configuration*

This completes the modifications to VMware View, continue with the following chapter to configure the BIG-IP LTM.

2

Deploying the BIG-IP LTM with VMware View 4.5

Configuring the BIG-IP LTM system for VMware View 4.5

In this chapter, we configure the BIG-IP LTM for the VMware View Connection Broker devices.

Creating the health monitor

The first task is to set up a health monitor for the VMware View Manager devices. This procedure is optional, but very strongly recommended. For this configuration, we create a simple HTTP health monitor. In this example, the advanced fields are not required, and we recommend you use the default values for the send and receive strings.

To configure a HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
   The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **view-manager-http**.
4. From the **Type** list, select **HTTP**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. Click the **Finished** button.
   The new monitor is added to the Monitor list.

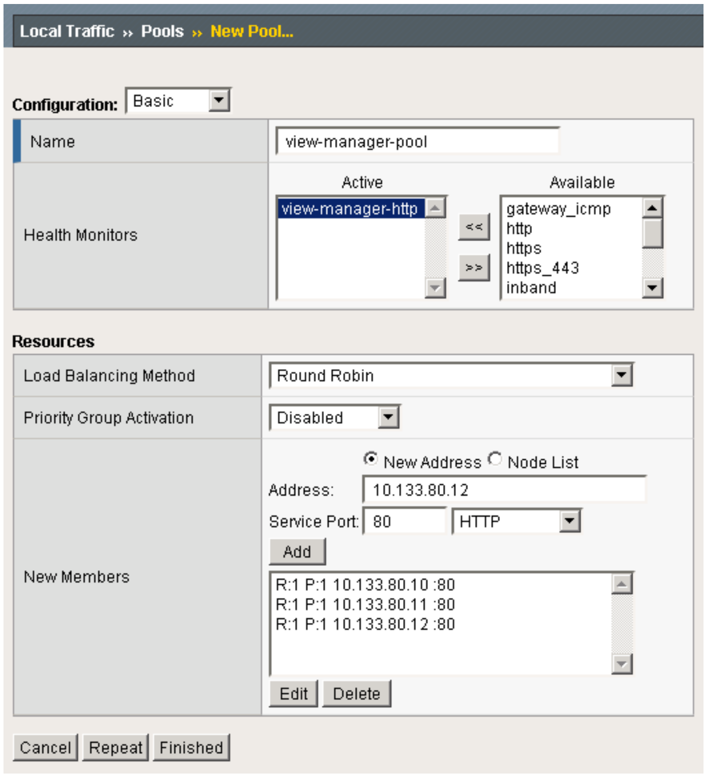
Creating the View Manager server pool

The next step is to create a pool on the BIG-IP LTM system for the View Manager systems. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method.

To create the pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
   The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, enter a name for your pool.
   In our example, we use **view-manager-pool**.

4. In the **Health Monitors** section, select the name of the monitor you created in *Creating the health monitor*, on page 2-1, and click the Add (**<<**) button. In our example, we select **view-manager-http**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Round Robin**.
6. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the View Manager to the pool. In our example, we type **10.133.80.10**
9. In the **Service Port** box, type **80**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each View Manager you want to add to the pool.
12. Click the **Finished** button.


Local Traffic » Pools » New Pool...

Configuration: Basic

Name: view-manager-pool

Health Monitors
Active: view-manager-http
Available: gateway_icmp, http, https, https_443, inband

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members: ● New Address ○ Node List
Address: 10.133.80.12
Service Port: 80 HTTP

R:1 P:1 10.133.80.10 :80
R:1 P:1 10.133.80.11 :80
R:1 P:1 10.133.80.12 :80

Figure 2.1 Configuring the BIG-IP LTM pool

Creating the Universal Inspection Engine persistence iRule

Using the following iRule, the BIG-IP LTM is able to direct traffic with greater precision resulting in a more uniform load distribution on the connection servers. Using the Universal Inspection Engine (UIE), the iRule looks for session information so that the BIG-IP LTM can persist the connections to the proper nodes. The View clients first use the session information in a cookie, and then use it as an URI argument when the tunnel is opened. The first response from the server contains a JSESSIONID cookie. The iRule enters that session ID into the connection table and upon further client requests looks for the information in a cookie or in the URI.

◆ **Important**

For the following iRule to function correctly, you must be using the BIG-IP LTM system to offload SSL transactions from the View implementation, as described in this deployment guide.

To create the persistence iRule

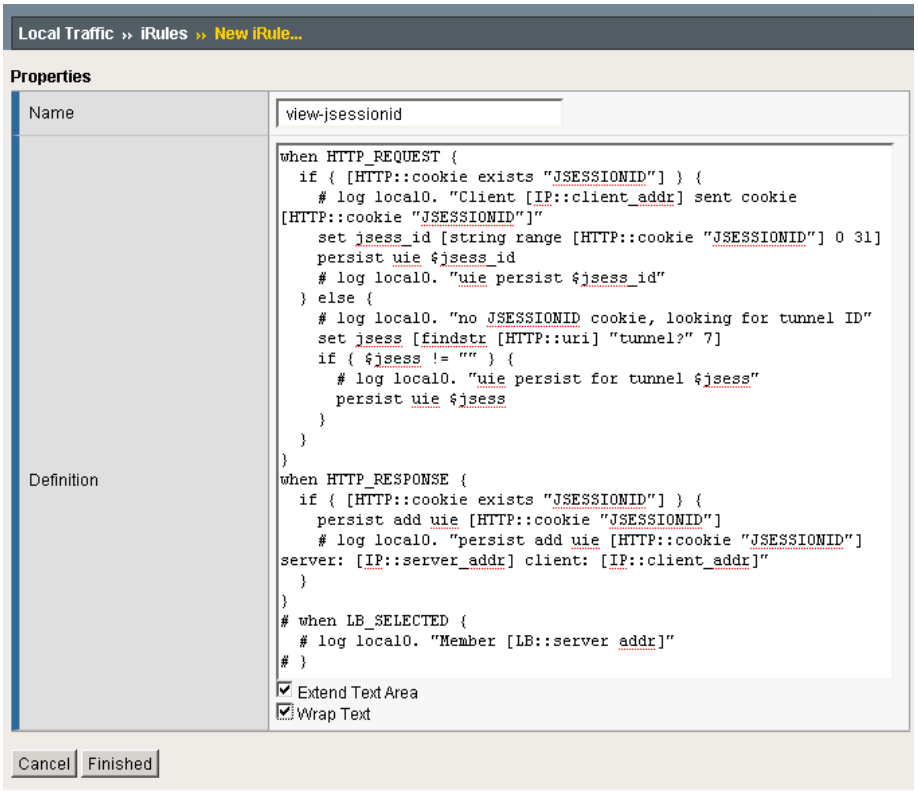
1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the Name box, type a name for this rule. In our example, we type **view-jsessionid**.
4. In the Definition box, type the following iRule, omitting the line numbers.

```
when HTTP_REQUEST {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    # log local0. "Client [IP::client_addr] sent cookie [HTTP::cookie "JSESSIONID"]"
    set jsess_id [string range [HTTP::cookie "JSESSIONID"] 0 31]
    persist uie $jsess_id
    # log local0. "uie persist $jsess_id"
  } else {
    # log local0. "no JSESSIONID cookie, looking for tunnel ID"
    set jsess [findstr [HTTP::uri] "tunnel?" 7]
    if { $jsess != "" } {
      # log local0. "uie persist for tunnel $jsess"
      persist uie $jsess
    }
  }
 }
 when HTTP_RESPONSE {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    persist add uie [HTTP::cookie "JSESSIONID"]
    # log local0. "persist add uie [HTTP::cookie "JSESSIONID"] server: [IP::server_addr] client: [IP::client_addr]"
  }
 }
 # when LB_SELECTED {
 # log local0. "Member [LB::server addr]"
 # }
```

5. Click the **Finished** button.

◆ **Tip**

The preceding iRule contains logging statements that are commented out. If you want to enable logging, simply remove the comment (#) from the code.



Name: view-jsessionid

Definition:

```
when HTTP_REQUEST {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    # log local0. "Client [IP::client_addr] sent cookie
[HTTP::cookie "JSESSIONID"]"
    set jsess_id [string range [HTTP::cookie "JSESSIONID"] 0 31]
    persist uie $jsess_id
    # log local0. "uie persist $jsess_id"
  } else {
    # log local0. "no JSESSIONID cookie, looking for tunnel ID"
    set jsess [findstr [HTTP::uri] "tunnel?" 7]
    if { $jsess != "" } {
      # log local0. "uie persist for tunnel $jsess"
      persist uie $jsess
    }
  }
}
when HTTP_RESPONSE {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    persist add uie [HTTP::cookie "JSESSIONID"]
    # log local0. "persist add uie [HTTP::cookie "JSESSIONID"]
server: [IP::server_addr] client: [IP::client_addr]"
  }
}
# when LB_SELECTED {
  # log local0. "Member [LB::server addr]"
# }
```

☑ Extend Text Area
☑ Wrap Text

Figure 2.2 *Configuring the persistence iRule on the BIG-IP LTM system*

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for client connections to the BIG-IP LTM device. For this deployment guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the ***Configuration Guide for Local Traffic Management***.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.
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.

Creating BIG-IP LTM profiles

The next task is to create the profiles. A ***profile*** is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In this example, we use the **http-lan-optimized-caching** parent profile.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

2. In the upper right portion of the screen, 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 **view-http**.
4. From the **Parent Profile** list, select **http-lan-optimized-caching**. The profile settings appear.
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 TCP profiles

The next task is to create the TCP profiles. We recommend creating one TCP profile using the **tcp-lan-optimized** parent. If your configuration uses various WAN links and your users are widely distributed, you should also create a second profile that uses **tcp-wan-optimized** as the parent profile. If all of your users are accessing the BIG-IP LTM over a LAN, you only need to create the LAN optimized profile.

Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **view-lan-opt**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
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 the WAN optimized TCP profile

Now we create is the WAN optimized TCP profile.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button.

4. In the **Name** box, type a name. We type **view-wan-opt**.

5. From the **Parent Profile** list, select **tcp-wan-optimized**.

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 the UIE persistence profile

The next profile we create is the persistence profile. This profile references the Universal Inspection Engine iRule you created earlier in this guide.

To create a 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.

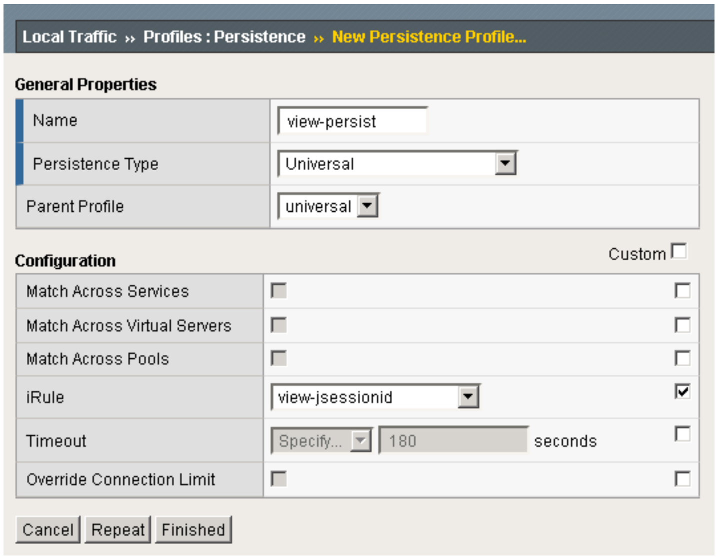
4. In the **Name** box, type a name for this profile. In our example, we type **view-persist**.

5. From the **Persistence Type** list, select **Universal**.

6. In the **iRule** row, check the **Custom** box. From the iRule list, select the name of the iRule you created in *Creating the Universal Inspection Engine persistence iRule*, on page 2-3. In our example, we select **view-jsessionid**.

7. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

8. Click the **Finished** button.



Local Traffic » Profiles : Persistence » New Persistence Profile...

General Properties

Name	view-persist
Persistence Type	Universal
Parent Profile	universal

Configuration

		Custom □
Match Across Services	□	□
Match Across Virtual Servers	□	□
Match Across Pools	□	□
iRule	view-jsessionid	☑
Timeout	Specify... 180 seconds	□
Override Connection Limit	□	□

Figure 2.3 Creating the persistence profile

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can use existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **view-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating a Client SSL profile

The next step in this configuration is to create a Client SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**. The HTTP Profiles screen opens.
3. On the Menu bar, from the SSL menu, select **Client**. The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **view-clientssl**.
6. In the Configuration section, check the **Certificate** and **Key Custom** boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.

8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.

9. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profiles and pool you created in the preceding procedures.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
   The Virtual Servers screen opens.

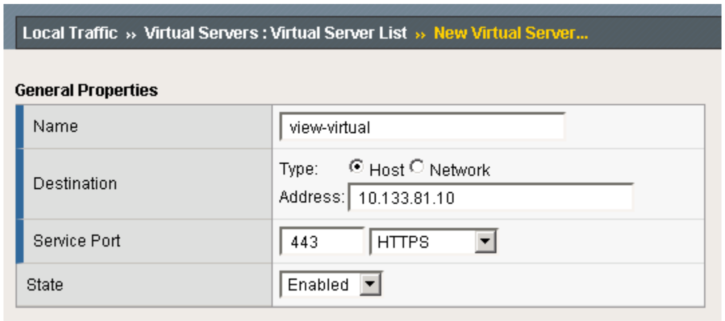
2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **view-virtual**.

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 **10.133.81.10**.

6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.



Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	view-virtual
Destination	Type: ● Host ○ Network Address: 10.133.81.10
Service Port	443 HTTPS
State	Enabled

Figure 2.4 Configuring the virtual server properties

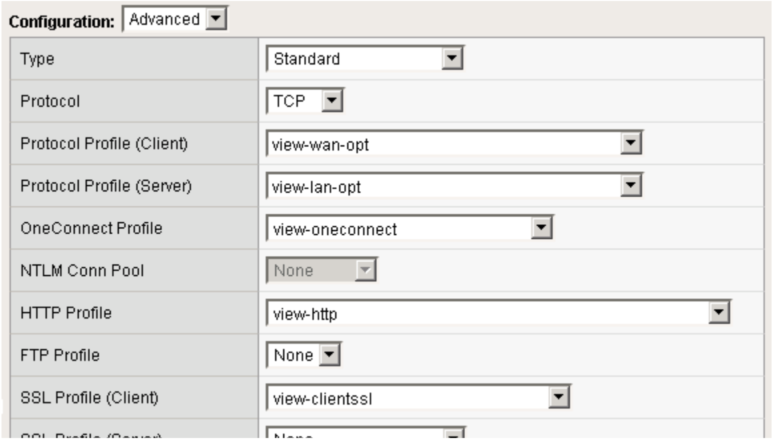
7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.

8. Leave the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list select the profile you created in *Creating the WAN optimized TCP profile*, on page 2-6. In our example, we select **view-wan-opt**.

10. From the **Protocol Profile (Server)** list, select the profile you created in *Creating the UIE persistence profile*, on page 2-7. In our example, we select **view-lan-opt**.

11. From the **OneConnect Profile** list, select the profile you created in *Creating a OneConnect profile*, on page 2-8. In our example, we select **view-oneconnect**.
12. From the **HTTP Profile** list, select the profile you created in *Creating an HTTP profile*, on page 2-5. In our example, we select **view-http**.
13. From the SSL Profile (Client) list, select the profile you created in *Creating a Client SSL profile*, on page 2-8. In our example, we select **view-clientssl**.

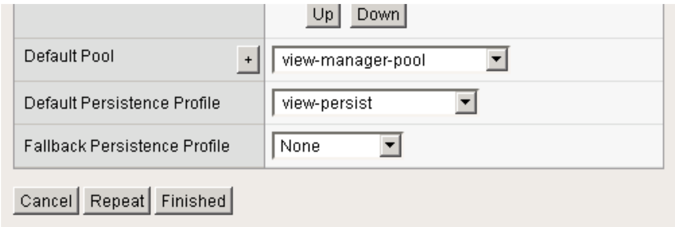


Configuration: Advanced

Type	Standard
Protocol	TCP
Protocol Profile (Client)	view-wan-opt
Protocol Profile (Server)	view-lan-opt
OneConnect Profile	view-oneconnect
NTLM Conn Pool	None
HTTP Profile	view-http
FTP Profile	None
SSL Profile (Client)	view-clientssl
SSL Profile (Server)	None

Figure 2.5 *Adding the profiles to the virtual server*

14. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the View Manager server pool*, on page 2-1. In our example, we select **view-manager-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating the UIE persistence profile*, on page 2-7. In our example, we select **view-persist**.



Default Pool	view-manager-pool
Default Persistence Profile	view-persist
Fallback Persistence Profile	None

Figure 2.6 *Adding the pool and persistence profile to the virtual server*

16. Click the **Finished** button.

The BIG-IP LTM configuration for VMware View is now complete.

3

Deploying the BIG-IP APM with VMware View 4.5

Configuring the BIG-IP APM for View 4.5

In this chapter, we configure the BIG-IP APM for VMware View 4.5.

Configuring remote access

To configure Remote Access, we use the Network Access Setup Wizard for Remote access.

To configure remote access using the wizard

1. On the Main tab, expand **Templates and Wizards**, and then click **Device Wizards**.
2. In the *Access Policy Manager Configuration* row, click the **Network Access Setup Wizard for Remote Access**, and then click the **Next** button.
3. On the Basic Properties page, configure the following:

    a) In the **Policy Name** box, type a name. In our example, we type **View-access**.

    b) From the **Default Language** list, select a language. We leave **en** selected.

    c) In the *Client Side Checks* row, leave the **Enable Antivirus Check in Access Policy** box checked.

    d) Click **Next**.

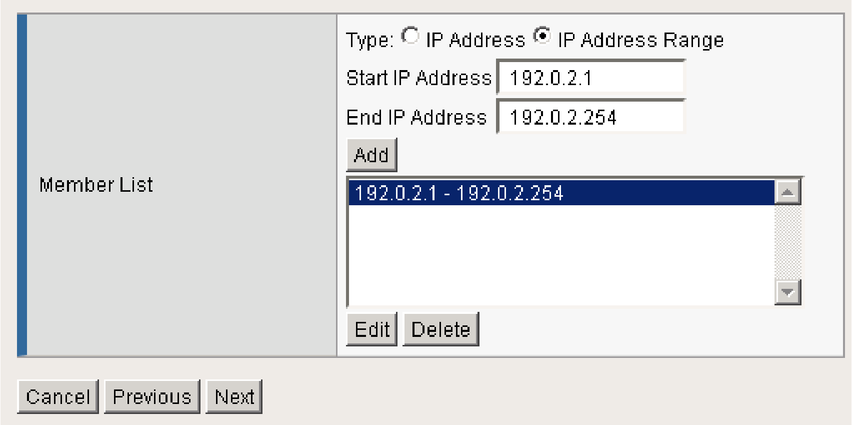
4. On the Select Authentication page, click the **Active Directory** option button, and then click **Next**.
5. On the Configure AAA Server page, configure the properties as appropriate for your installation (you must type a **Domain Name** at the minimum), and then click the **Next** button.
6. On the **Configure Lease Pool** page, you can either enter individual IP addresses, or define a range of IP addresses. In our example, we use an IP address range, so we perform the following:

    a) In the Type section, click **IP Address Range**.

    b) In the **Start IP Address** box, type the appropriate IP address. In our example, we type **192.0.2.1**.

    c) In the **End IP Address** box, type the appropriate IP address. In our example, we type **192.0.2.254**.

    d) Click the **Add** button, and then click the **Next** button.


Member List

Type: ○ IP Address ● IP Address Range

Start IP Address 192.0.2.1

End IP Address 192.0.2.254

192.0.2.1 - 192.0.2.254

Figure 3.1 *Lease Pool configuration*

7. On the Configure Network Access page, configure the following:

   a) From the Compression list, select GZIP.
   Note: *If Datagram TLS (DTLS) is configured (UDP based communication between client and Remote Access Server) GZIP compression is automatically disabled. DTLS and GZIP compression are incompatible with one another. If you enable GZIP compression it will be used for TCP connections. DTLS clients will use compression for network access tunnels.*

   b) In the *Traffic Options* row, 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.

   - If you want all traffic to go through the tunnel, click **Force all traffic through tunnel**, and continue with Step 8. We use this option in our example.

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

     1)In the *LAN Address Space* section, in the **IP address** and **Mask** boxes, type the IP address and Mask of the LAN Address space that should go through the tunnel, and then click the **Add** button. For example, **192.168.0.0/16**.

     2)In the *DNS Address Space* section, in the **DNS** box, type the DNS suffixes that are used in the target LAN and then click the **Add** button.

   c) The **Allow Local Subnet** and **Client Side Security** settings are optional, configure as applicable. See the online help for more information.

d) In the *DTLS* row, check the box to enable DTLS. If necessary, in the **DTLS Port** box, update the port.
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.
If clients cannot connect with DTLS, they fall back to TCP based SSL.

e) Click **Next**.

8. On the Configure DNS Hosts for Network Access page, complete the following:

   a) In the **Primary Name Server** box, type the IP address of the Active Directory Server in the network. In our example, we type **10.133.84.60**.

   b) All other settings are optional, configure as applicable for your implementation.

   c) Click **Next**.

9. On the Virtual Server (HTTPS connection) page, complete the following:

   a) In the **Virtual Server IP Address** box, type the IP address to use for this virtual server. This is the virtual server for Network Access connectivity. In our example, we type 10.133.20.200.

   b) In the *Redirect Server* row, we leave the Create redirect Virtual Server (HTTP to HTTPS) box checked. This will create a virtual server that only redirects requests from HTTP to HTTPS.

   c) Click **Next**.

10. Review the Configuration Summary, and then click **Next** to complete the configuration and apply the settings. If you notice any mistakes, use the Previous button to go back to specific pages.

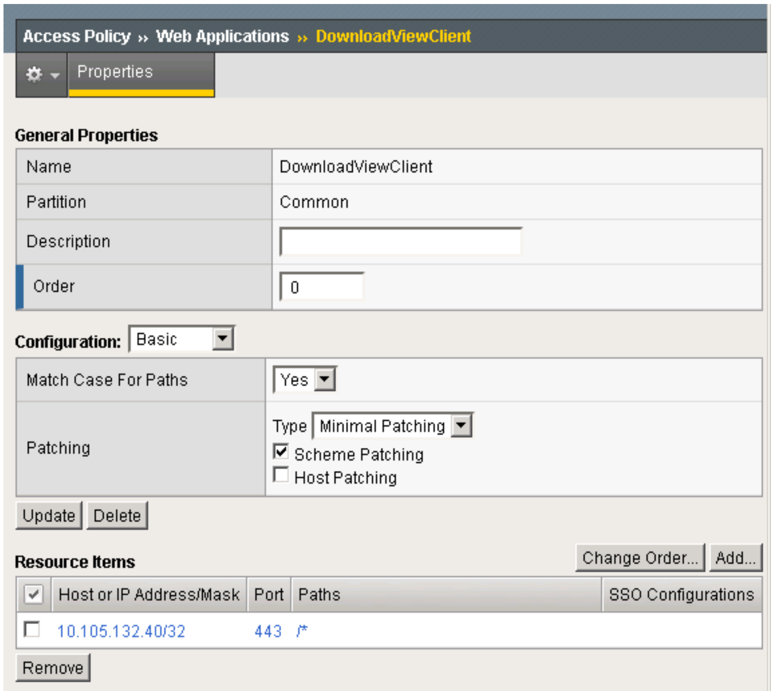
Creating a Web Application

The next task is to create a Web Application. This Web Application contains the IP address of the BIG-IP LTM virtual server for the Connection Broker servers, where users are directed if the prelogon policy cannot detect the View client.

To create a Web Application

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.

3. In the **Name** box, type a name. In our example, we type **DownloadViewClient**.
4. In the **Patching** section, from the **Type** list, select **Minimal Patching**, and then click the **Scheme Patching** box.
5. Click the **Create** button. The Resource Items appear.
6. Click the **Add** button to the right of Resource Items.
7. In the Destination row, click the **IP Address** option button, and then in the **IP Address** box, type the IP address of the BIG-IP LTM virtual server you created for the Connection Broker servers in *Creating the virtual server*, on page 2-9.
8. In the **Port** box, type **443**.
9. From the **Scheme** list, select **HTTPS**.
10. In the **Paths** box, type `/*`
11. From the **Compression** list, select **GZIP Compression**.
12. Leave the other settings at their defaults.
13. Click the **Finished** button.



General Properties

Name	DownloadViewClient
Partition	Common
Description	
Order	0

Configuration: Basic

Match Case For Paths	Yes
Patching	Type Minimal Patching ☑ Scheme Patching □ Host Patching

Resource Items

☑	Host or IP Address/Mask	Port	Paths	SSO Configurations
□	10.105.132.40/32	443	/*	

Figure 3.2 *Web Application configuration*

Creating a Webtop

The next task is to create a Webtop. The Webtop also contains the IP address of the BIG-IP LTM virtual server for the Connection Broker servers.

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, give the Webtop a unique name. In our example, we type **view-webtop**.
4. From the **Type** list, select **Web Applications**.
5. In the Web Application Start URI box, type the FQDN or IP address of the BIG-IP LTM virtual server you created for the Connection Broker servers in *Creating the virtual server*, on page 2-9.
   Be sure to use HTTP or HTTPS as appropriate.
6. Click the **Finished** button.

Creating the Profiles

In this section, we configure BIG-IP profiles that are not created by the Wizard. 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 a Rewrite profile

In this procedure, we create a Rewrite profile. The Client Caching Type for this profile must be CSS and Java Script.

To create a Rewrite profile

1. On the Main tab, expand **Access Policy**, and then click **Rewrite Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **viewRewriteProfile**.
4. Leave the **Client Caching Type** list set to **CSS and Java Script**.
5. Click the **Finished** button.

Creating TCP profiles

The next task is to create the TCP profiles. We recommend creating **tcp-lan-optimized** and **tcp-wan-optimized** profiles.

Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile.

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 **View-access-tcp-lan**.
5. Modify any of the 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 WAN optimized TCP profile

The next task is to create the WAN optimized profile.

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 **View-access-tcp-wan**.
4. Modify any of the 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.
5. 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. We type **View-access-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. 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 **View-access-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 a Server SSL profile

The next task is to create a Server SSL profile.

To create the Server SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Server**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **View-server-ssl**.
4. Leave all the settings at the defaults, and then click **Finished**.

Modifying the APM virtual server to use the objects you just created

The next task is to associate the objects you just created with the APM virtual server that was created by the Wizard.

To associate the Rewrite profile with the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Server list opens.
2. From the **Virtual Server** list, select the name of the virtual server that was created by the Remote Access Wizard. This virtual server will start with the prefix you specified in Step 3a of *Configuring remote access*, on page 3-1. In our example, we select **View-Access_Vs**.
3. From the **Protocol Profile (Client)** list, select the profile you created in *Creating the WAN optimized TCP profile*, on page 3-6.
4. From the **Protocol Profile (Server)** list, select the profile you created in *Creating the LAN optimized TCP profile*, on page 3-6.
5. From the **HTTP Profile** list, select the profile you created in *Creating the HTTP profile*, on page 3-6.
6. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*, on page 3-7.

7. From the **SSL Profile (Server)** list, select the profile you created in *Creating a Server SSL profile*, on page 3-8.

   Note: If your download source is an SSL protected server, a Server SSL profile is required. Your download source was defined in both the Web Application and Webtop you created earlier in this chapter. For example, if you are pointing to the Connection Broker LTM virtual server as recommended in this guide, you will need this Server SSL profile.
   If you are pointing directly at a Connection Broker listening on port 80, this Server SSL profile is not required.

8. In the *Access Policy* section, from the **Rewrite Profile** list, select the name of the profile you created in the preceding procedure. In our example, we select **viewRewriteProfile**.
9. Click the **Update** button.

Modifying the APM log level

The next task is to adjust the APM log level to a lower setting. For maximum security, lowering the log level ensures no user information is ever written to the logs. If troubleshooting is needed, this log level can be increased.

To modify the APM log level

1. On the Main tab, expand **System**, select **Logs** and then click **Options**.
2. In the Access Policy Logging section, from the **Access Policy** list, select **Alert**.
3. Click the **Update** button.

Editing the Access Profile with the Visual Policy Editor

In this section, we modify the Access Policy that was created by Remote Access wizard using the Visual Policy Editor (VPE).

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile that was created by the Wizard (this Access Profile starts with the prefix you specified in Step 3a of *Configuring remote access*, on page 3-1), and then in the Access Policy column, click **Edit**.
   The Visual Policy Editor opens in a new window.

3. Click the **+** symbol between **Start** and **Antivirus Check**. A box opens with options for different actions.
4. In the Server Side Checks section at the bottom of the box, click the **Client OS** option button, and then click the **Add Item** button at the bottom of the box, and then perform the following:

    a) From the **Name** field, you can optionally type a new name.

    b) Click the Branch Rules tab.

    c) In the **Windows 7** row, change the name to **Windows 7, Vista and XP**.

    d) Click the **change** link.

    e) Under OR, click the **Add Expression** button.
    Important: You must click the button under OR and ***not*** next to AND.

    f) From the **Agent Sel**: list, select **Client OS**.

    g) From the **Client OS is** list, select **Windows Vista**.

    h) Click the **Add Expression** button.

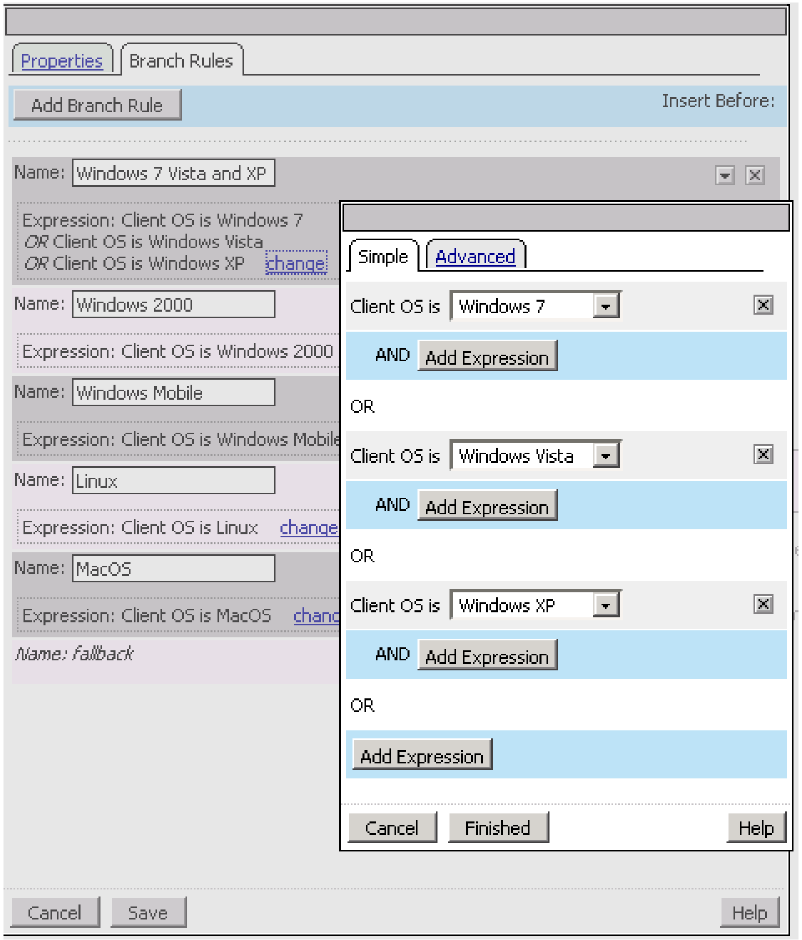
    i) Below Windows Vista and under OR, click the **Add Expression** button.

    j) Repeat Steps f - h, but in step g, select **Windows XP**.

    k) Click **Finished**. You return to the Branch rules tab.

    l) From the Windows Vista and Windows XP rows, click the delete button (x).

    m) Click the **Save** button (see Figure 3.3, on page 3-11).



Name: Windows 7 Vista and XP

Expression: Client OS is Windows 7
OR Client OS is Windows Vista
OR Client OS is Windows XP change

Name: Windows 2000

Expression: Client OS is Windows 2000

Name: Windows Mobile

Expression: Client OS is Windows Mobile

Name: Linux

Expression: Client OS is Linux change

Name: MacOS

Expression: Client OS is MacOS chanc

Name: fallback

Client OS is Windows 7
AND
OR
Client OS is Windows Vista
AND
OR
Client OS is Windows XP
AND
OR

Figure 3.3 VPE Client OS Branch rule changes

5. 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 **UnsupportedOSMessage**.

   b) Click the **Save** button. The Macro appears under the Access Policy.

   c) Click the Expand (+) button next to UnsupportedOSMessage.

   d) Click the **+** symbol between **In** and **Out**. A box opens with options for different actions.

   e) Click the **Message box** option button, and then click **Add Item**.

   f) In the **Name** box, type a unique name for this box. In our example, we type **serviceNotAvailableforThisOS**.

   g) In the **Message** box, type the message you want users to see. In our example, we type **This service is available for Windows 7, Vista or XP clients only**.

h) You can optionally modify the Link text. Clicking the link sends the user to the next object in the path, Deny in our example.

i) Click the **Save** button. The macro is now ready to use in the following step.

6. Click the **+** symbol between **Windows 2000** and **Deny**. A box opens with options for different actions.
7. 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 **UnsupportedOSMessage**.
8. Repeat steps 7 and 8 for each of the operating systems you want to deny.

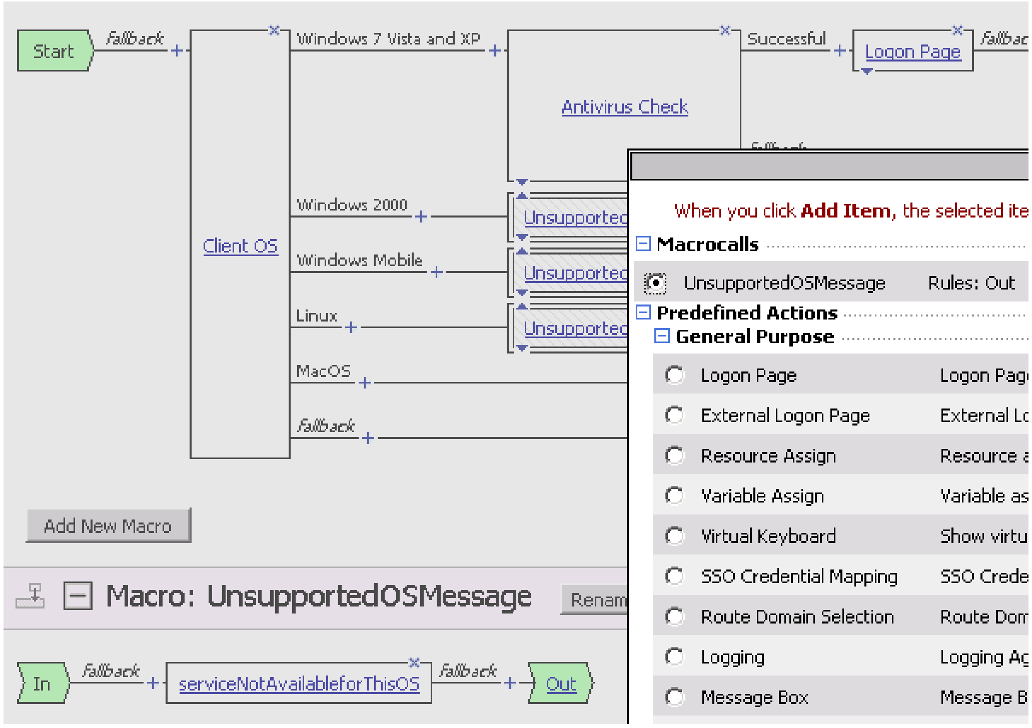


Figure 3.4 Visual Policy Editor: Adding the Macro to the Operating Systems (MacOS in this image)

9. On the Fallback path between **Antivirus check** and **Deny,** click the **+** symbol.
10. In the General Purpose section, click the click the **Message box** option button, and then click **Add Item**.

a) In the **Name** box, type a unique name for this box. In our example, we type **antiVirusNotFound**.

b) In the **Message** box, type the message you want users to see. In our example, we type **You do not have the proper AntiVirus software installed on your machine. Please install or update your Antivirus software**.

c) You can optionally modify the Link text. Clicking the link sends the user to the next object in the path, Deny in our example.

d) Click the **Save** button.

11. On the Successful path between **AD Auth** and **Resource Assign**, click the **+** symbol.

12. In the Client Side Check section, click the **Windows File Check** option button, and then click the **Add Item** button. The Windows File Checker page opens. Complete the following:

a) In the **Name** box, you can optionally type a new name. In our example, we type **checkForViewClient**.

a) Click the **Add new entry** button.

b) In the **FileName** box, type the path to the View client as appropriate for your View deployment. In our example, we type:

```
C:\\Program Files\\VMware\\VMware View\\Client\\bin\\wswc.exe
```

Note: *The double backslashes are required for the inspector to check for the file. If your View client is installed in a custom location be sure to set the correct path to the executable.*

c) Leave the rest of the settings at their default levels.

d) Click the **Save** button.

13. On the Fallback path between **Resource Assign** and **Allow**, click the **+** symbol.

14. In the General Purpose section, click the **Variable Assign** option button, and then click the **Add Item** button. The Resource Assignment page opens. Complete the following:

a) In the **Name** box, you can optionally type a new name. In our example, we type **configureViewSSO**.

b) Click the **Add new entry** button.

c) Click the **change** button.

d) From the list on the left, select **Configuration Variable** and then select **Unsecure** from the adjacent list.

e) From the **Property** list, select **application launch**.

f) In the **Custom Expression** box on the right, use the following syntax for the expression, replacing the red text with information from your implementation (see note following).
IMPORTANT: *The second line of following code must be*

entered as a single line. If you copy and paste from this document, you will likely pick up unnecessary spaces or line breaks that will cause a syntax error in the code. We present the code below for your information; we strongly recommend you copy and paste the code from the following text file: ***http://www.f5.com/solutions/resources/deployment-guides/files/vmware-view-vpe-expression.txt****. And then carefully replace the values in red below with values from your implementation.*

```
expr {"<application_launch><item><path>C:\\Program Files\\VMware\\VMware
    View\\Client\\bin\\wswc.exe</path><parameter>-username [mcget {session.logon.last.username}]
    -password [mcget -secure {session.logon.last.password}] -domainName BD -serverURL
    https://broker.example.com:443</parameter><os_type>WINDOWS</os_type></item></application_lau
    nch>"}
```

Note: *If your View client is installed in a custom location be sure to set the correct* ***path*** *to the executable. Our* ***domainName*** *is BD; insert the correct name of your domain. The* ***serverURL*** *parameter indicates where clients should connect to for accessing the View Connection Servers (the BIG-IP LTM virtual server); replace the value of this parameter with the Connection Server virtual server IP address or Domain Name. Additional parameters are available in the client and can be set here. Refer to VMware View client documentation for more information.*

g) Click the **Finished** button.

h) On the Variable Assign page, click the **Save** button.

15. On the Fallback path between **checkForViewClient** and **Deny**, click the **+** symbol.

16. In the General Purpose section, click the **Decision Box** option button, and then click the **Add Item** button. The Decision box page opens. Complete the following:

    a) In the **Name** box, you can optionally type a name. In our example, we type **askUserDownload**.

    b) In the **Message** box, type a message for users to see when the View client is not found. In our example, we type **View client not found**.

    c) In the **Option 1** box, type something similar to **Download client now**.

    d) In the **Option 2** box, type something similar to **Disconnect**.

    e) Click the **Save** button.

17. On the Option 1 path between **askUserDownload** and **Deny**, click the **+** symbol.

18. In the General Purpose section, click the **Resource Assign** option button, and then click **Add Item**. The Resource Assign page opens. Complete the following:

    a) In the **Name** box, you can optionally type a new name. In our example, we type **downloadViewClient**.

    b) Click the **Add new entry** button.

    c) Click the **Add/Delete Web Application Resources** link.

    d) Check the box for the Web Application you created in *Creating a Web Application*, on page 3-3. In our example, we check the **DownloadViewClient** box. Click **Update**.

    e) Click the **Set Webtop** link.

    f) Click the option button for the Webtop you created in *Creating a Webtop*, on page 3-5. In our example, we click the **view-webtop** button. Click **Update**.

    g) Click the **Save** button.

19. On the Fallback path after **downloadViewClient**, click the **Deny** box.

20. Under Select Ending, click the **Allow** button, and then click **Save**.

21. 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.

22. Click the **Close** button on the upper right to close the VPE.
    Your policy should look similar to the following.

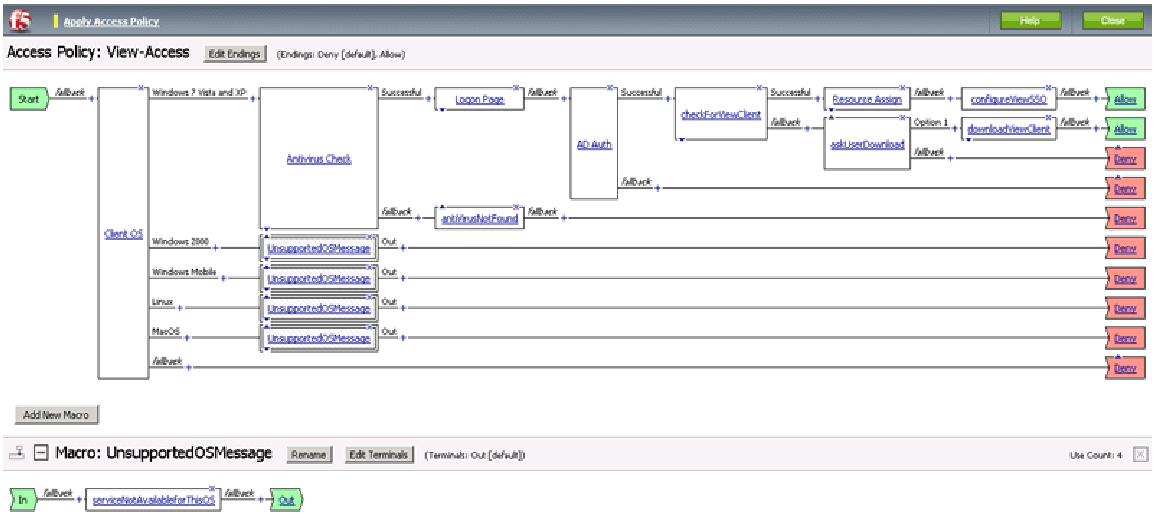


Figure 3.5 Completed Access Policy in the Visual Policy Editor

This completes the configuration.