Deployment Guide

Deploying F5 with VMware View and Horizon View

Welcome to the F5 and VMware® View® Deployment Guide. This document contains guidance on configuring the BIG-IP system version 11 and later, including BIG-IP Local Traffic Manager™ (LTM) and BIG-IP Access Policy Manager™ (APM) for VMware View and Horizon View resulting in a secure, fast, and highly available deployment.

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

This guide provides instructions on both manually configuring the BIG-IP system and using the iApp™ Application template. iApps, introduced in BIG-IP v11, is an extremely easy and accurate way to configure the BIG-IP system for View.

Why F5?

F5 and VMware have a long-standing relationship that centers on technology integration and solution development. As a result, customers can benefit from leveraging the experience gained by peers from deploying proven, real-world solutions.

F5's products and solutions bring an improved level of reliability, scalability, and security to View deployments. For large View deployments requiring multiple pods or several data centers, F5's products provide the load balancing and traffic management needed to satisfy the requirements of customers around the world.

F5 and VMware continue to work together on providing customers best-of-breed solutions that allow for better and faster deployments as well as being ready for future needs, requirements, and growth of your organization.

Additionally, F5 has achieved full certification with Teradici® for our PCoIP proxy capabilities in BIG-IP APM.

Products and versions tested

Product	Versions
BIG-IP LTM, APM[3]	11.2, 11.3, 11.4, 11.4.1, 11.5, 11.5.1, 11.6
VMware Horizon View	5.2, 5.3, 6.0[1], 6.1[1, 2]
iApp Template version	f5.vmware_view.v1.2.1
Deployment Guide version	1.6 (see *Document Revision History on page 58*)

[1] BIG-IP APM v11.6 HF-3 and earlier does not support publishing and providing remote connectivity to the RDS hosted applications feature in Horizon View 6.0; however v11.6 HF-4 or later enables the View Remote App publishing feature.

[2] BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.

[3] BIG-IP APM does not support proxying the VMware View RDP protocol.

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/vmware-view5-iapp-dg.pdf*

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

Contents

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for VMware View acts as the single-point interface for building, managing, and monitoring VMware View deployments.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network: http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*

Prerequisites and configuration notes

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

- You have the option of configuring the BIG-IP system manually, or using the iApp template.
    - **iApp**
      To use the iApp template, you must download a new template file. Future versions of the product will include this View iApp. See *Configuring the BIG-IP iApp for View on page 13.*
    - **Manual configuration**
      If configuring the BIG-IP system manually, after modifying the VMware Virtual Desktop Manager Global Settings, see *Appendix: Manual configuration tables on page 35.* Because of the complexity of the configuration, we recommend using the iApp template.
- This iApp was written for, and has been tested extensively with VMware View version 5 and 5.1, and Horizon View 5.2, 5.3, 6.0, and 6.1. However, BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.
- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.2 or later. If you are using a previous version of the BIG-IP system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- If you want to use the BIG-IP system as a native PCoIP proxy or want HTML 5 support, you must be running BIG-IP version 11.4 or later and Horizon View 5.2 or later.
  Note the iApp only displays these options when version 11.4 or later has been installed on your BIG-IP system. If using a previous version, you have the option of using the BIG-IP APM as a full PCoIP proxy which enables a secure virtual private tunnel using BIG-IP APM and the BIG-IP Edge Client to create a network access DTLS VPN.
- Because the BIG-IP system is decrypting SSL, you must have an SSL certificate and key installed on the BIG-IP LTM system. If you are offloading SSL onto the BIG-IP system, there are additional steps you need to perform on the View servers. The BIG-IP system can also be configured to re-encrypt the traffic (SSL bridging) before sending it to the View servers.
- This deployment guide is written with the assumption that VMware server(s), Virtual Center and Connection Servers, and Security Servers if applicable, are already configured on the network and are in good working order.

Tip

*Before beginning the iApp template, we recommend you set the **Idle Time Before Automatic Logout** value on the BIG-IP system longer than the default value of 1200 seconds when configuring iApps. This allows more time to configure the iApp and prevent inadvertent logouts which causes you to have to restart the iApp configuration. To modify this value, from the Main tab, expand **System** and then click **Preferences**.*

Configuration examples and traffic flows

In this deployment guide, we show multiple ways of deploying the BIG-IP system with View. Specifically, if View is deployed with View Security Servers, the BIG-IP system can further protect, monitor, and load balance these servers, allowing PCoIP Security Gateway services to be moved out of the DMZ. If only View Connection Servers are used, the BIG-IP LTM can protect, monitor, and load balance those Connection Servers to provide greater reliability and more predictable scaling.

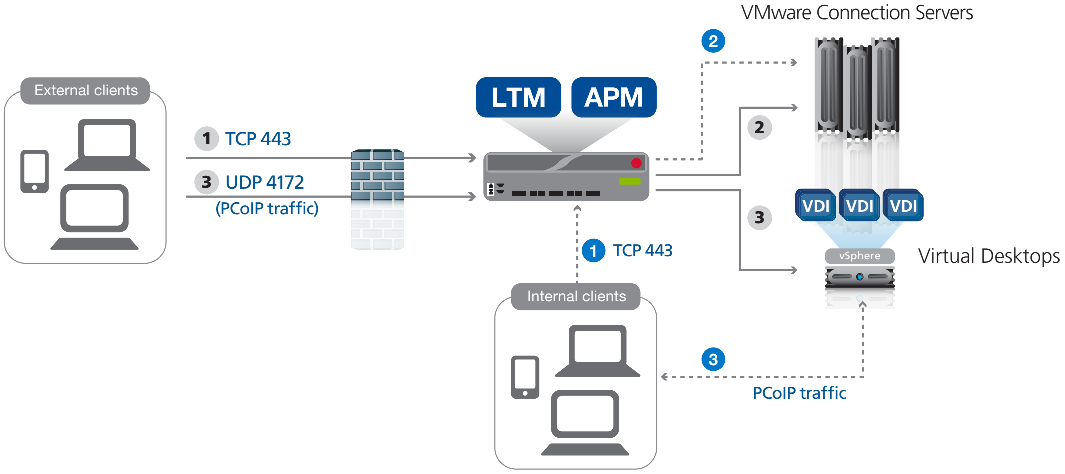
We also show how to configure the BIG-IP APM with the BIG-IP LTM scenarios described above to provide pre-logon checks to the endpoint device and support a broad range of authentication mechanisms, including various back-end directory services. APM can also enforce Active Directory group policies on corporate-owned and non-corporate-owned assets during the duration of the connection. Additionally, once authenticated, BIG-IP APM guarantees the encryption of all View transport protocols, whether natively encrypted or not.

An additional option shows how to use the BIG-IP system to natively proxy PCoIP connections in a reliable and secure manner, thereby removing the need for VMware Security Servers. When using this option, you optionally can support HTML 5 browser based clients for users that are unable to install the Horizon View client.

Traffic Flows

The following diagrams show the traffic flow for the different scenarios described in this guide.

BIG-IP APM/LTM with natively proxied PCoIP connections using Connection Servers only
The following traffic flow diagram shows the BIG-IP LTM and APM running software versions 11.4 or later with a VMware View Horizon 5.2 or later deployment using Connection Servers only and is typically used to support public connections with an option to support internal connections. Use this scenario when load balancing public connections with BIG-IP APM authenticated connections to your Connection Servers. PCoIP connections are fully proxied, providing a secure connection to and from your View Connection servers, thereby eliminating the need for Security Servers. This scenario also supports HTML 5 browser-based clients, as well as RSA SecurID two-factor authentication configurations and View Client disclaimer messages. Note this two-factor solution does not require altering your View environment; the BIG-IP system fully proxies RSA SecurID authentication prior to allowing connections to View Horizon Connection Servers.



For deployments with BIG-IP system fully proxying PCoIP traffic and Horizon View Connection Servers, the traffic flow is (grey callouts):

1. The client device (regardless of Mac, Windows, HTML 5, iPad, Zero Client) makes a connection to the virtual IP address on your BIG-IP system. The BIG-IP establishes a new connection to the Connection Servers and proceeds with authentication.
2. The BIG-IP system persists the TCP 443 XML connection to the same Connection Server.
3. Once desktop availability and entitlement are determined, external PCoIP connections are persisted to the assigned virtual desktop.
4. The BIG-IP system fully proxies the desktop PCoIP connections (UDP 4172) to the user's assigned virtual desktop.

Optional flow for internal clients (blue callouts):

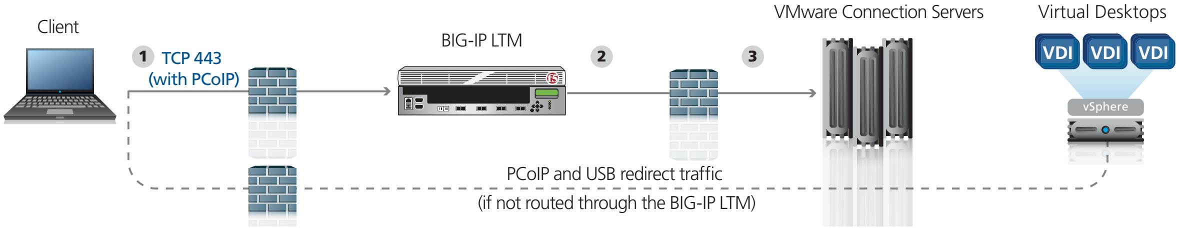
1. The internal client device (regardless of Mac, Windows, HTML 5, iPad, Zero Client) makes a connection to the internal, trusted virtual IP address on the BIG-IP system. The BIG-IP establishes a new connection to the Connection Servers and proceeds with authentication.

2. The BIG-IP system persists the TCP 443 XML connection to the same Connection Server.

3. Once desktop availability and entitlement are determined, PCoIP connections are sent to the assigned virtual desktop (not routed or proxied through the BIG-IP system).

BIG-IP LTM with Connection Servers only (supports trusted internal client connections)

The following traffic flow diagram shows the BIG-IP LTM with a VMware View deployment using Connection Servers only and is typically used to support non-public connections. Use this scenario when load balancing internal connections or with BIG-IP APM using the BIG-IP Edge Client for View.


Client
1 TCP 443 (with PCoIP)
BIG-IP LTM
2
3
VMware Connection Servers
Virtual Desktops
VDI
VDI
VDI
vSphere
PCoIP and USB redirect traffic
(if not routed through the BIG-IP LTM)

For deployments without Security Servers the traffic flow is:

1. The client machine (regardless of Mac, Windows, iPad, or Zero Clients) makes a connection to the BIG-IP virtual IP address for the Connection Servers. Depending on your configuration, PCoIP and USB redirects are routed through or around the BIG-IP LTM.

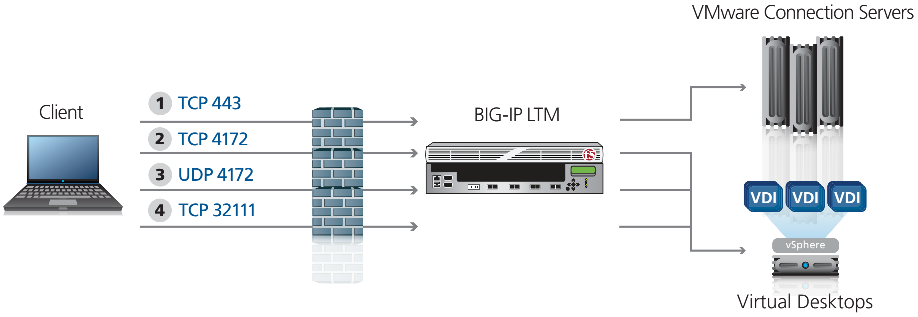
2. The SSL connection terminates on the BIG-IP device. The BIG-IP LTM re-encrypts the traffic, or offloads SSL and establishes a connection to the Connection Servers.

3. After authentication, desktop entitlement, and selection are complete, desktop connections proceed to the appropriate View Desktop.

BIG-IP LTM with Connection Servers only (supports public connections using BIG-IP APM)

The following traffic flow diagram shows the BIG-IP LTM with a VMware View deployment using Connection Servers only and is typically used to support public connections using BIG-IP APM, which handles the public connections with a VPN tunnel. This scenario is only available when you choose to deploy BIG-IP APM. Use this scenario when load balancing public connections and with APM authenticated connections to your Connection servers.

This scenario is typically for use with older versions of the BIG-IP system and View. We recommend using BIG-IP version 11.4 or later with the latest version of the iApp template and View 5.2 or later as described in the first scenario on the previous page.



For deployments with Connection Servers and PCoIP protocol the traffic flow is as follows:

1. The client machine (regardless of Mac, Windows, iPad, Zero Client) makes a connection to the BIG-IP virtual IP address for the Connection Servers. The BIG-IP establishes a new connection to the Connection Servers and proceeds with authentication.

2. The BIG-IP system accepts and forwards client PCoIP TCP 4172 requests to the destination Virtual desktop.

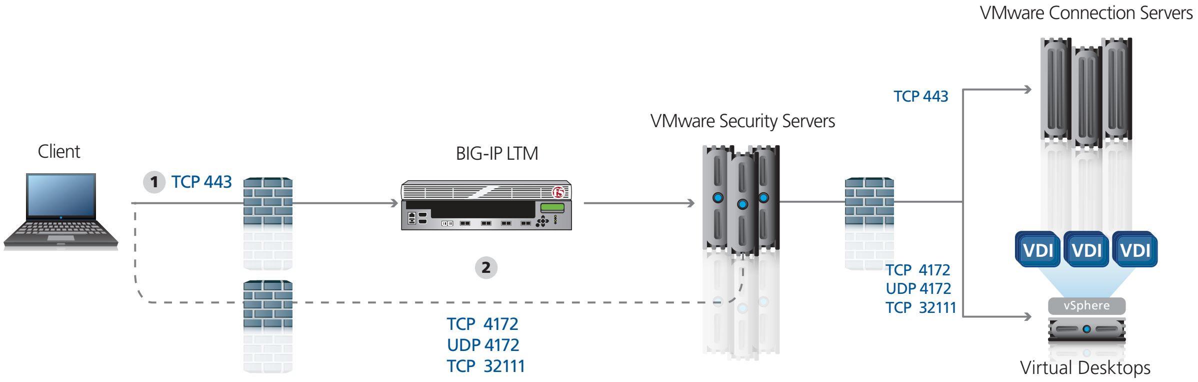
3. Once desktop availability and entitlement are determined, PCoIP connections and USB redirects are persisted to the same target virtual desktop.

4. The BIG-IP system forward proxies the desktop PCoIP connections (UDP 4172) and USB redirects (TCP 32111) to the target View desktop. In View Manager 5.1 and later releases, the USB redirection over port 32111 is tunneled over SSL connection (port 443). This option should only be used if using View 5.0 and supporting USB redirects.

BIG-IP LTM with Security Servers and Connection Servers

This traffic flow diagram shows the BIG-IP LTM with a View deployment using both Security Servers and Connection Servers, and is typically used to support secure public connections. Use this scenario when load balancing public connections without BIG-IP APM. This scenario is typically for use with older versions of the BIG-IP system and View. We recommend using BIG-IP version 11.4 or later with the latest version of the iApp template and View 5.2 or later as described in the first scenario on the previous page.

For deployments with Security Servers and PCoIP protocol the traffic flow is as follows:

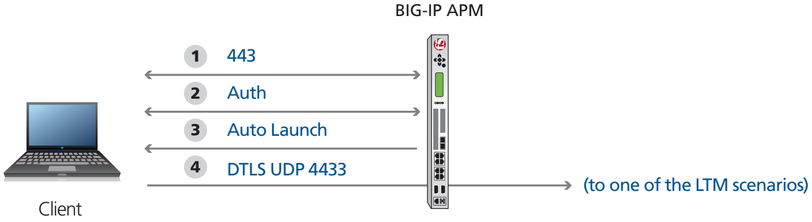


1. The client machine (regardless of Mac, Windows, iPad, Zero Client) makes a connection to the Virtual IP Address for the VMware Security Servers, residing on the BIG-IP LTM.
2. The BIG-IP system establishes a new connection to the Security Servers, which securely forward the request to the Connection Servers and proceeds with authentication.
3. The client establishes remaining PCoIP connections to the View Security servers, which forward requests to the appropriate Virtual desktop. PCoIP connections can go directly to Security Servers (as shown in the diagram), or can be sent to the BIG-IP virtual server, and then persisted to same Security server to which the client initially connected.

BIG-IP APM using the Edge Client with View

This traffic flow diagram shows the BIG-IP APM using the BIG-IP Edge Client in front of the View deployment. After the Auto Launch, traffic continues to one of the BIG-IP LTM scenarios described previously.

This scenario is typically for use with older versions of the BIG-IP system and View. We recommend using BIG-IP version 11.4 or later with the latest version of the iApp template and View 5.2 or later as described in the first scenario on the previous page.



When BIG-IP APM is added to the deployment, the APM performs pre-authentication, as well as additional security and client detection.

1. The client machine launches the BIG-IP Edge Client, which makes a connection to the BIG-IP virtual IP address for either the VMware Connection Servers or Security Servers (depending on your configuration). The BIG-IP system establishes a new connection to the VMware Active Directory Servers.
2. Authentication is performed directly from the BIG-IP APM. User credentials are securely cached on the BIG-IP system.
3. The BIG-IP Edge Client checks for the availability of the View Client and either downloads the client or launches it on Microsoft Windows or Mac clients only.
4. Once the secured network tunnel is setup between the client and the BIG-IP APM, the client is automatically logged in using one of the LTM scenarios (either connecting to the Security or Connection Servers). The BIG-IP system uses DTLS for platforms that support the BIG-IP Edge Clients and SSL for platforms that do not.

Modifying the View configuration

Before starting the BIG-IP system configuration, we modify the View configuration to allow the BIG-IP system to load balance View Client connections. If you are planning on configuring the BIG-IP system to support HTML 5, you must also modify the Connection Server configuration (see *Modifying your Connection Servers to support HTML 5 clients on page 10*).

VMware Virtual Desktop Manager Global Settings

Before configuring the BIG-IP LTM, we modify the View configuration to allow the BIG-IP LTM to load balance View Client connections. The modifications depend on whether you are configuring View with Connection Servers only or Security and Connection Servers.

Refer to the VMware documentation if you need further instruction on configuring the View servers.

Modifying the View implementation if using Connection Servers only

Use the following procedures if you are using Connection Servers only. Make sure to check each of the procedures to see if they are applicable to your configuration.

Modifying the VMware configuration to allow SSL termination

Use this procedure only if using the Connection Servers and not Security Servers. The following procedure allows the BIG-IP system to terminate SSL transactions and send encrypted (SSL Bridging) or unencrypted (SSL Offload) web traffic directly to the View Connection Servers.

To modify the VMware configuration for Connection Servers only

1. Log on to the View Manager Administrator tool.
2. From the navigation pane, click to expand **View Configuration** and then click **Servers**.
   The Servers Settings opens in the main pane.
3. For each View Connection Server, perform the following:
   a. From the *View Connection Servers* pane, click to select a Connection Server.
   b. Click the **Edit...** button. The Edit View Connection Server settings box opens.
   c. On the General tab, clear the **Use secure tunnel connection to desktop** check box if selected.
   d. Clear the **Use PCoIP Secure Gateway for PCoIP connections to desktop** check box if selected.
   e. Click **OK** to close the window.

Note

When using Connection Servers only, and not using BIG-IP APM, make sure you have internal routes set up to point to the BIG-IP system for your View desktop network if you choose to route PCoIP and/or USB redirect traffic through the BIG-IP system.

Configuring Connection servers for SSL offload by the BIG-IP system (optional; requires server reboot)

When SSL is offloaded to the BIG-IP system, you can configure View Connection Server instances to allow HTTP connections from the BIG-IP system. The BIG-IP system must accept HTTPS for View Client connections.

To allow HTTP connections between View servers and BIG-IP system, you must configure the **locked.properties** file on each View Connection Server instance on which HTTP connections are allowed.

Even when HTTP connections between View servers and the BIG-IP system are allowed, you cannot disable SSL in View. View servers continue to accept HTTPS connections as well as HTTP connections.

➡ ***Note***

If your View Clients use smart card authentication, the clients must make HTTPS connections directly to View Connection Servers. SSL offloading is not supported with smart card authentication.

To configure the locked.properties file

1. Create or edit the **locked.properties** file in the SSL gateway configuration folder on the View Connection Server host. For example: *install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties*
2. To configure the View server's protocol, add the **serverProtocol** property and set it to **http**.   The value **http** must be typed in lower case.
3. *Optional*: Add properties to configure a non-default HTTP listening port and a network interface on the View server.
   - To change the HTTP listening port from 80, set **serverPortNonSSL** to another port number to which the intermediate device is configured to connect.
   - If the View server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set **serverHost** to the IP address of that network interface.
4. Save the **locked.properties** file.
5. Restart the View Connection Server service to make your changes take effect.

For example, the following locked.properties file allows non-SSL HTTP connections to a View server. The IP address of the View server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value http must be lower case.

```
serverProtocol=http

serverHost=10.20.30.40
```

Modifying the Global Policy to allow USB redirects (Optional)

Use the following procedure if you plan on supporting USB redirects though the BIG-IP system.

➡ ***Note***

USB redirects through the BIG-IP system are not supported when using Native PCoIP proxy. USB redirects are supported when forward proxying PCoIP traffic using the Edge Client, or if not using the BIG-IP APM.

To modify the Global Policy to allow USB redirects

1. From the View Manager Administrator tool, in the left pane, expand **Policies** and then highlight **Global Policies**.
2. Click **Edit Policies**.
3. Set **USB access: Allow**.
4. Click **OK**.

This completes the modifications for implementations without the Security Server.

Modifying the View implementation if using Security Servers and Connection Servers

Use the following procedures if using both Security Servers and Connections Servers.

Modifying the VMware View configuration if using Security and Connection Servers

In this scenario, the BIG-IP system is used to load balance Security Servers and to act as a gateway for PCoIP connections. This procedure allows PCoIP servers to be moved off the DMZ if desired.

To modify the VMware configuration for View using Security Server

1. Log on to the View Manager Administrator tool.
2. From the navigation pane, click to expand **View Configuration** and then click **Servers**. The Servers Settings opens.
3. For each View Connection Server, perform the following:
   a. In the main pane, from the *View Connection Servers* section, click to select a Connection Server.
   b. Click the **Edit...** button. The Edit View Connection Server settings box opens.
   c. On the General tab, in the HTTP(S) Secure Tunnel **External URL** box, type the IP address you will associate with the BIG-IP LTM virtual IP address for the Security Server, followed by a colon and the port. For example we type: https://192.0.2.123:443
   d. Click **OK** to close the window.
   e. Repeat these steps for each Connection Server.
4. For each View Security Server object located in the Administers console of your Connection server:
   a. From the View Security Servers section, click to select a Security Server.
   b. Click the **Edit...** button. The Edit Security Server box opens.
   c. In the HTTP(S) Secure Tunnel **External URL** box, type the IP address you will associate with the BIG-IP LTM virtual IP address for the Security Servers, followed by a colon and the port. In our example, we type: **https://192.0.2.123:443**.
   d. If you are using PCoIP, in the **PCoIP External URL** box, type the appropriate IP address followed by a colon and the port. In our example, we use **192.0.2.123:4172**.
   e. Click **OK** to close the window.
   f. Repeat these steps for each Security Server.

Configuring Connection servers for SSL offload by the BIG-IP system (optional; requires server reboot)

When SSL is offloaded to the BIG-IP system, you can configure View Connection Server instances to allow HTTP connections from the BIG-IP system. The BIG-IP system must accept HTTPS for View Client connections.

To allow HTTP connections between View servers and BIG-IP system, you must configure the **locked.properties** file on each View Connection Server instance on which HTTP connections are allowed.

Even when HTTP connections between View servers and the BIG-IP system are allowed, you cannot disable SSL in View. View servers continue to accept HTTPS connections as well as HTTP connections.

Note

If your View Clients use smart card authentication, the clients must make HTTPS connections directly to View Connection Servers or Security Servers. SSL offloading is not supported with smart card authentication.

To configure the locked.properties file

1. Create or edit the **locked.properties** file in the SSL gateway configuration folder on the View Connection Server or Security Server host. For example: *install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties*.
2. To configure the View server's protocol, add the **serverProtocol** property and set it to **http**. The value **http** must be in lower case.

3. *Optional*: Add properties to configure a non-default HTTP listening port and a network interface on the View server.
    - To change the HTTP listening port from 80, set **serverPortNonSSL** to another port number to which the intermediate device is configured to connect.
    - If the View server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set **serverHost** to the IP address of that network interface.
4. Save the **locked.properties** file.
5. Restart the View Connection Server or Security service to make your changes take effect.

For example, the following locked.properties file allows non-SSL HTTP connections to a View server. The IP address of the View server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value http must be lower case.

```
serverProtocol=http
serverHost=10.20.30.40
```

Modifying the Global Policy to allow USB redirects (Optional)

Use the following procedure if you plan on supporting USB redirects though the BIG-IP system.

➡ ***Note***

USB redirects through the BIG-IP system are not supported when using Native PCoIP proxy. USB redirects are supported when forward proxying PCoIP traffic using the Edge Client, or if not using the BIG-IP APM.

To modify the Global Policy to allow USB redirects

1. From the View Manager Administrator tool, in the left pane, expand **Policies** and then highlight **Global Policies**.
2. Click **Edit Policies**.
3. Set **USB access: Allow**.
4. Click **OK**.

This completes the modifications.

Modifying your Connection Servers to support HTML 5 clients

VMware Horizon View HTML Access is required to support HTML 5 View clients. Use the following guidance to modify the Connection Servers. For specific information,

1. Download the **HTML Access Web Portal installer** from the downloads section of the VMware website.
    a. Note the HTML Access software is listed under the "Feature Packs" section of their downloads.
    b. Install the software onto all Connection Servers supporting HTML 5 clients.
2. Download **Remote Experience Agent**.
    a. Note the software is listed under the "Feature Packs" section
    b. Install software onto all your Virtual Desktops master images which will support HTML 5 clients
3. Modify the Connection Servers to remove the Use Secure Tunnel connection to desktop and use Blast Secure Gateway for HTML
    a. From the View Configuration tab, select **Servers**, and then click **Connection Servers**.
    b. Highlight one of the Connections servers and then click **Edit**.
    c. Modify the HTTP External URL and BLAST External URL to match the URL of your SSL certificates.
    d. **Important:** Clear the check from **Use Secure Tunnel connection to desktop** and **Use Blast Secure Gateway for HTML access to desktop** after modifying the External URLs.
    e. Repeat for each Connection server.

4. Check the option to enable HTML Access in the pool(s) settings for which HTML 5 client connections are supported.
    a. Make sure pool template used has Remote Experience Agent in addition to the standard View Agent installed.
5. Use a browser that supports HTML 5 when connecting to the BIG-IP system.

Once you have finished installing all of the VMware HTML Access components, and before configuring the BIG-IP system, we recommend connecting directly to a Connection server using a supported HTML 5 browser to verify View HTML Access is properly functioning without the BIG-IP system proxying connections. This makes future troubleshooting much easier.

Configuring BIG-IP LTM DNS and NTP settings

If you are using BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP to point to the appropriate DNS servers.

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

➲ **Important:** *The BIG-IP system must have a Route to the DNS server. The Route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a Route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
   a. In the **Address** box, type the IP address of the DNS server.
   b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

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

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the BIG-IP command line, run `ntpq -np`.

See *http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html* for more information on this command.

Configuring the BIG-IP iApp for View

Use the following guidance to help configure the BIG-IP system for VMware View using the BIG-IP iApp template.

Downloading and importing the View iApp

The first task is to download the iApp for View and import it onto the BIG-IP system. Ensure you download the file with the latest version number.

To download and import the iApp

1. Open a browser and go to: *http://support.f5.com/kb/en-us/solutions/public/15000/000/sol15041.html*.
2. Follow the instructions to download the VMware View iApp to a location accessible from your BIG-IP system.
3. Extract (unzip) the **f5.vmware_view.v1.2.1** file (or a newer version if applicable).
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Select the **Overwrite Existing Templates** check box.
8. Click the **Choose File** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use. If you are configuring the BIG-IP system manually, see *Appendix: Manual configuration tables on page 35.*

Getting started with the iApp for View

To begin the View iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **VMware-View_.**
5. From the **Template** list, select **f5.vmware_view.v1.2.1** (or a newer version if applicable).
   The View iApp template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.

2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template options

This section of the template asks about your View and BIG-IP implementation.

1. ***Do you want to see inline help?***
   Select whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Show inline help text**. Important and critical notes are always shown, no matter which selection you make.

   - **Yes, show inline help text**
     This selection causes inline help to be shown for most questions in the template.

   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.

   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method, parent profiles, and settings are all set automatically. The F5 recommended settings come as a result of extensive testing with VMware View, so if you are unsure, choose Basic.

   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options like Slow Ramp Time and Priority Group Activation. You can also choose to attach iRules you have previously created to the VMware View application service. This option provides more flexibility for advanced users.

     Advanced options in the template are marked with the Advanced icon: **Advanced** If you are using Basic/F5 recommended settings, you can skip the questions with this icon.

BIG-IP Access Policy Manager

In this section, you have the option of using the BIG-IP Access Policy Manager (APM) to provide proxy authentication (pre-authentication) for your View implementation (see *Configuration examples and traffic flows on page 4* for details). For specific information on BIG-IP APM, see http://www.f5.com/products/big-ip/big-ip-access-policy-manager/overview/.

You must have the BIG-IP APM module fully licensed and provisioned on your BIG-IP system to use these features. Additionally, if you are not using the BIG-IP system as a native PCoIP proxy (11.4 and later only) using BIG-IP APM requires a browser plugin, or the BIG-IP Edge Client must be installed on the remote user's computer.

1. ***Do you want to deploy BIG-IP Access Policy Manager?***
   You can use BIG-IP APM to provide pre-authentication for your View implementation. The BIG-IP APM enables a secure virtual private tunnel using BIG-IP APM and the BIG-IP Edge Client to create a network access DTLS VPN, or if you are using BIG-IP v11.4 or later and View Clients are using Horizon View 5.2 or later, the BIG-IP APM can act as a native PCoIP secure gateway proxy.

   - **No, do not deploy BIG-IP Access Policy Manager**
     Select this option if you do not want to use the BIG-IP APM at this time. You can always re-enter the template at a later date should you decide to add BIG-IP APM functionality. Continue with *Virtual Servers and Pools on page 21.*

- **Yes, deploy BIG-IP Access Policy Manager**
  Select this option to use the BIG-IP APM, either to natively or forward PCoIP proxy or as a DTLS Network Access VPN.

  If you are using BIG-IP version 11.2 - 11.3, continue with step *i). What IP address do you want to use for the APM virtual server? on page 16*.

  If you are using BIG-IP version 11.4 or later ***only***, the following questions appear.

  a. *How should the BIG-IP system handle PCoIP traffic?*
  Select how you want the BIG-IP system to handle PCoIP traffic.

  - **Securely proxy PCoIP traffic using APM as a PCoIP gateway (recommended)**
    This option (and the sub-options) requires Horizon View 5.2 or newer View Clients and Servers. Check the BIG-IP APM Client Compatibility Matrix for your version to ensure compatibility. For 11.4, you can find the matrix here.

    Select this option if you want to securely proxy PCoIP traffic through the BIG-IP system. In this case, the BIG-IP system fully proxies PCoIP traffic without the use of a BIG-IP client-side plugin or the F5 Edge Client. Selecting this option also enables the ability to support two-factor authentication.

    i). *Do you want to support browser based connections, including the View HTML 5 client?*
    Select whether you want the BIG-IP system to support browser-based connections, including the View HTML 5 client.

    - **No, only support View Client connections**
      Select this option if you only need to support View Client connections and do not need to support browser based connections, including the View HTML 5 client. No further information is necessary.
    - **Yes, support HTML 5 View clientless browser connections**
      Select this option if you want the system to support both HTML 5 clientless browser connections and View client connections. The system adds this information to the APM configuration and no further information is necessary.

    ii). *Should the BIG-IP system support RSA SecurID for two-factor authentication?*
    Select this option if you want the BIG-IP APM to support two-factor authentication using RSA SecurID.

    Important

    You must have already created a SecurID AAA Server object on the BIG-IP APM to use this feature. If you have not created the AAA Server, exit the template and create the AAA Server. See Access Policy > AAA Servers > SecurID to create the AAA Server.

    - **Yes, configure the BIG-IP system for two-factor authentication**
      Select this option if you want to configure two-factor authentication using SecurID on the BIG-IP system.

      1). *Which AAA Server object do you want to use for SecurID?*
      Select the SecurID AAA Server object you created on the BIG-IP APM for RSA SecurID.
    - **No, do not support RSA SecurID two-factor authentication**
      Select this option do not require two-factor authentication at this time. You can always reconfigure the template at a later time to add two-factor authentication.

    ii). *Should the BIG-IP system show a message to View users during logon?*
    The BIG-IP system can display a message to View users before they log on. This can be a warning that only authorized users can attempt to access the system, or any other type of message. The BIG-IP APM refers to this as a disclaimer message.
    Select whether you want to create a custom message for View users during the log on process.

    - **Yes, add a message during logon**
      Select this option if you want users to see a message during logon. The following question appears.

      1). *What message should be displayed to users?*
      Type the message you want users to see during the logon process.

- **No, do not add a message during logon**
  Select this option if you do not want to display a message to users during logon.

iii). *If external clients use a network translated address to access View, what is the public-facing IP address?*
If there is a device between the View Clients and the BIG-IP system that is translating the public IP address to which View Clients are resolving for initial connections, you must enter the public NAT IP address here. If you are not translating this address, this can remain blank.

iv). *What is the NetBIOS domain name for your environment?*
Specify the NetBIOS domains for this View environment. For example, if the FQDN is 'my.example.com', the NetBIOS domain is 'my'. Continue with #2.

- **Forward proxy PCoIP traffic using the BIG-IP Edge Client**
  Select this option if you want the BIG-IP system to act as a forward proxy for PCoIP traffic using the BIG-IP Edge Client. Choosing this option enables the option of client side antivirus enforcement, and requires concurrent connection user licensing.

i). *What IP address do you want to use for the APM virtual server?*
Specify an available IP address to use for the BIG-IP APM virtual server. This virtual server address is used by clients to establish initial connections to the network via the BIG-IP system.

ii). *Which certificate do you want to use to authenticate access?*
Select the SSL certificate you imported for this View deployment.

If you have not yet imported a trusted certificate, you must import one before it appears in the list. You can either complete the template using the default certificate and key, import the trusted certificate and key, use the Reconfigure option to re-enter the template, and then select them from the lists; or exit the template to import the certificate and key, and then start the configuration over from the beginning.

⚠ ***Warning***

The default certificate and key on the BIG-IP system is not secure and should never be used in production environments. The trusted certificate must be valid for all fully qualified domain names used to access the application. For more information on importing certificates and keys, see the BIG-IP documentation.

iii). *Which associated key do you want to use?*
Select the associated key from the list.

iv). *What is the directory path to the View Client for Windows?*
Specify the full path to the View Client. The default path is
C:\Program Files\VMware\VMware View\Client\bin\wswc.exe
If you have a different path to the View Client, make sure to use the same format as the default.

ⓘ ***Important***

Auto-Launch only works in Microsoft Windows, Mac, and LINUX client environments.

v). *What is the directory path to the View Client for Mac?*
Specify the full path to the View Client for Apple Mac devices. The default installation path for Mac is **/Applications/VMware View Client.app**.

vi). *To which server (IP or FQDN) should users be sent when the View Client is not present?*
Specify the IP address or domain name of a server from which clients can acquire the View Client software when it is not present. If the View environment is only accessible via BIG-IP APM authenticated network access, you must ensure this link points to a resource that is available without BIG-IP APM authenticated network access.

vii). *What is the NetBIOS domain name for your environment?*
Specify the NetBIOS domains for this View environment. For example, if the FQDN is 'my.example.com', the NetBIOS domain is 'my'.

viii). *What IP address should start the lease pool range?*
Specify an available IP address to being the lease pool range. The BIG-IP APM uses the IP addresses in the range you specify to assign to clients connecting through the APM. The IP address range you specify must have routes to View Connection Servers or Security Servers, and a route to the View Virtual Desktop network.

ix). *What IP address should end the lease pool range?*
Specify the end of the IP address range.

x). *What is the IP address of the DNS server used for remote client lookups?*
Specify the IP address of the primary DNS server that is used when clients are connected to BIG-IP system. Clients will use this server to resolve addresses while connected to the BIG-IP system.

xi). *What is the IP address of the second DNS server?*
You can optionally specify the IP address of a second DNS server the system can use for remote client lookups.

xii). *Should BIG-IP APM perform a check for antivirus software?*
The BIG-IP Edge Client can perform client-side checks to determine if antivirus software is installed, enabled, and up to date before allowing users to connect to the BIG-IP system. Specify whether you want the system to perform an antivirus software check.

- **No, do not perform an antivirus software check**
  Select this option if you do not want the system to perform a check for antivirus software on the client devices.
- **Yes, perform an antivirus software check**
  Select this option if you want the system to perform an antivirus software check on

  1). *On which operating systems do you want to enable antivirus software checks?*
  Select the operating systems for which you want to enable antivirus software checks. You can enable or disable the check for Windows, Mac, and UNIX operating systems.

  2). *What message do you want clients to see after failing an antivirus software check?*
  Specify the message you want to present to your users who fail the antivirus software check.

2. ***Create a new AAA Server object or select an existing one?***
The AAA Server contains the authentication mechanism for the BIG-IP APM Access Policy. This question appears no matter which way you answered the PCoIP traffic question.

The iApp can create a new Active Directory AAA Server object, or if you have previously created an AAA Server for your View implementation, you can select it from the list.

▶ *Select an existing AAA Server object*
If you manually created an AAA Server for View, select it from the list. All of the rest of the questions in this section disappear. Continue with the following section.

▶ Create a new AAA Server object
If you want the iApp to create an AAA Server continue with the following.

a. *Which Active Directory servers (IP and host name) are used for user credential authentication?*
Specify each of your Active Directory domain controllers, both FQDN and associated IP address, used for this View environment. Click the **Add** button for additional rows.

b. *What is your Active Directory domain name?*
Specify the fully qualified domain name (FQDN) used for this View environment, for example, my.example.com

c. *Does your Active Directory domain require credentials?*
Select whether anonymous binding is allowed in your Active Directory environment.

▸ **Yes, anonymous binding is allowed**
Select this option if anonymous binding is allowed. No further information is required.

▸ **No, credentials are required for binding**
If credentials are required for binding, you must specify an Active Directory user name and password for use in the AAA Server.

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

ii). *What is the password associated with that account?*
Type the associated password.

d. *Create a new monitor for the Active Directory servers?*
The iApp can create a new monitor for the Active Directory servers (either an Active Directory-specific monitor or a simple ICMP ping monitor), or if you have already created a health monitor for the Active Directory servers, you can select it from the list.

- *Select the monitor you created from the list*
If you created a monitor for the Active Directory servers, select it from the list. Continue with the next section.

- **No, do not monitor Active Directory**
Select this option if you do not want the BIG-IP system to monitor the Active Directory servers.

- **Yes, create a simple ICMP monitor**
Select this option to have the system create a simple ICMP monitor for the Active Directory server. The ICMP monitor sends a ping to each server in the pool, and marks the server as up if the ping is successful. Continue with the next section.

- **Yes, create a new Active Directory Monitor**
Select this option to have the system create a new LDAP monitor for the Active Directory servers. This health monitor is much more sophisticated than the ICMP monitor and includes a user account (that you specify in the following questions) which the system uses to attempt to log into Active Directory as a part of the health check.

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

ii). *What is the associated password?*
Specify the password associated with the Active Directory user name.
These credentials are stored in plaintext on your BIG-IP system.

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

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

v). *How many seconds between Active Directory health checks?* **Advanced**
Specify how many seconds the system should use as the health check Interval for the Active Directory servers. We recommend the default of 10 seconds.

vi). *Which port is used for Active Directory communication?* **Advanced**
Specify the port being used for communication with your Active Directory implementation. The default port when using the TLS security protocol, or no security, is port 389. The default port used when using the SSL security protocol is 636. The port that appears by default changes depending on your answer to the secure protocol question above.

SSL Encryption

In this section, you configure the SSL encryption options for the View deployment.

1. ***How should the BIG-IP system handle encrypted traffic?***
Select whether you want to configure the BIG-IP system for SSL offload or SSL bridging.

If your application requires encryption and session persistence (which ensures requests from a single user are always distributed to the server on which they started), we recommend you configure the BIG-IP system for SSL offload. This allows the system to more accurately persist connections based on granular protocol or application-specific variables.

Because encryption and decryption of SSL is computationally intensive and consumes server CPU resources, if your environment does not require encryption between the BIG-IP system and the servers, select SSL Offload to terminate the SSL session from the client at the BIG-IP system and provide cleartext communication from the BIG-IP system to the servers.

If security requirements do not allow the BIG-IP system to offload SSL, select to re-encrypt to the servers. With this selection the system will use the SSL ID or Client/Server IP to enforce session persistence. Because these parameters are less granular, you may experience inconsistent distribution of client requests.

- **Terminate SSL for clients, plaintext to View servers (SSL offload)**
  Choose this method if you want the BIG-IP system to offload SSL processing from the View servers. You need a valid SSL certificate and key for this method.
- **Terminate SSL from clients, re-encrypt to servers**
  Choose this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers (SSL Bridging). You also need a valid SSL certificate and key for this method.

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

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

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

     a. *Which SSL certificate do you want to use?*
     Select the SSL certificate you imported for this View deployment.

     If you have not yet imported a trusted certificate, you must import one before it appears in the list. You can either complete the template using the default certificate and key, import the trusted certificate and key, use the Reconfigure option to re-enter the template, and then select them from the lists; or exit the template to import the certificate and key, and then start the configuration over from the beginning.

     ⚠ ***Warning***

     The default certificate and key on the BIG-IP system is not secure and should never be used in production environments. The trusted certificate must be valid for all fully qualified domain names used to access the application. For more information on importing certificates and keys, see the BIG-IP documentation.

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

     c. *Which intermediate certificate do you want to use?* Advanced
     If your implementation requires an intermediate or chain certificate, select the appropriate certificate from the list. You must have already imported the intermediate certificate before it appears in the list.

     Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

3. ***<u>Do you want to redirect inbound HTTP traffic to HTTPS?</u>*** Advanced
   Select whether you want the BIG-IP system to automatically redirect HTTP traffic to the HTTPS virtual server. This can lead to a better users experience if users forget to use HTTPS when attempting to connect to the View deployment.

   ▶ **Redirect HTTP to HTTPS**
   Select this option (the default) for the BIG-IP attaches a small redirect iRule to the virtual server. You must specify the appropriate port in the next question.

   a. *<u>From which port should traffic be redirected?</u>*
   Specify the port number for the traffic that you want to redirect to HTTPS. The most common is port 80 (the default).

   ▶ **Do not redirect HTTP to HTTPS**
   Select this option if you do not want to enable the automatic redirect.

4. ***<u>Which Server SSL profile do you want to use?</u>*** Advanced
   This question only appears if you selected SSL bridging.

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

   ▶ *Select the Server SSL profile you created from the list*
   If you have previously created a Server SSL profile for your View implementation, from the list, select the existing Server SSL profile you created. Note that if you are using a previously created Server SSL profile, and are using the native PCoIP proxy functionality, you must have the **Server Name** set to **SNI=pcoip-default-sni** in the Server SSL profile.

   ▶ **Use F5's recommended Server SSL profile**
   Select this option if you want the iApp to create a new Server SSL profile.

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

PC over IP

In this section, you configure PCoIP settings for the deployment.
This section **does not** appear if you are using BIG-IP version 11.4 or later and selected to use the BIG-IP APM as a PCoIP gateway.

1. ***<u>Should PCoIP connections go through the BIG-IP system?</u>***
   Select whether PCoIP connections are routed through the BIG-IP system.

   ▶ **No, PCoIP connections should not go through the BIG-IP system**
   Select this option if you do not want PCoIP connections routed through the BIG-IP system as a part of this configuration.

   If PCoIP connections will not go through the BIG-IP system, you must have a route on the system for traffic between the clients and the Virtual Desktops. If you do not have a route between the View Client and the Virtual Desktop, you can either exit this iApp template, configure a route on the BIG-IP system, and then start over; or select Yes now, and then reconfigure the iApp after you have created the route.

   If you select No, and do not have a route configured, the configuration produced by the iApp will not function properly. For more information on configuring routes on the BIG-IP system, see the online help for routes (Main tab > Network > Routes) or the BIG-IP system manuals.

   If you select No, continue with the following section; no further information is needed.

   ▶ **Yes, PCoIP connections should go through the BIG-IP system**
   Select this option if you want PCoIP connections routed through the BIG-IP system. If you answer Yes, you also have the option of VMware USB redirects going through the BIG-IP system.

   a. *<u>Will PCoIP connections be proxied by the View Security Servers?</u>*
   Select whether PCoIP connections will be forward proxied by the View Security Servers. Your answer here determines how the BIG-IP system handles the PCoIP traffic.

- **No, PCoIP connections are not proxied by the View Security Servers**
  Select this option if PCoIP connections are not forward proxied by the View Security Servers. In this case, the BIG-IP system creates TCP and UDP forwarding virtual servers on port 4172. These two virtual servers act as a route between the clients and the Virtual Desktops through the BIG-IP system.

  i). On which network do the Virtual Desktops reside?
  Specify the network on which the Virtual Desktops reside.

  ii). What is the network mask for the virtual desktops?
  Type the subnet mask associated with the network of the Virtual Desktops.

  iii). Which VLANs should accept PCoIP traffic?
  Select whether you want to allow PCoIP traffic destined for the forwarding virtual servers from all VLANs, or if you want to specify the VLANs that can accept or should deny traffic. By restricting PCoIP traffic to specific VLANs adds an additional layer of security.

  - **All VLANs should accept PCoIP traffic**
    Select this option if you do not want to restrict PCoIP traffic from specific VLANs.

  - **Accept PCoIP traffic only from specific VLANs**
    Select this option if you want this virtual server to only accept traffic from the VLANs you specify.

    1). Which VLANs should be allowed?
    *From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move them to the **Selected** box.*

  - **Deny PCoIP traffic from specific VLANs**
    Select this option if you want this virtual server to deny traffic from the VLANs you specify.

    1). Which VLANs should be denied?
    *From the **Options** box, click the name of the applicable VLAN(s) and then click the Add (**<<**) button to move them to the **Selected** box.*

- **Yes, PCoIP connections are proxied by the View Security Servers**
  Select this option if you PCoIP connections are forward proxied by the View Security Servers. The iApp does not create forwarding virtual servers, and instead directs all PCoIP traffic back to the View Servers. You ***must*** enable **PCoIP Secure Gateway Address** on the View servers for this option to function properly.

b. *Should VMware USB redirects go through the BIG-IP system? (View 5.0 only)*
Select whether you want to support USB redirects through the BIG-IP system. According to VMware, the USB redirection technology improves communication to the remote desktop and provides better mouse, screen, and keyboard performance.

➡ ***Note***

The USB Redirection technology implemented by VMware improves the communication to the remote Desktop. When using USB Redirection, the USB traffic is separated and passed over port 32111. This provides for better mouse, screen, and keyboard performance. If you select Yes, the system creates a forwarding virtual server for USB redirects. In View Manager 5.1 and later releases, the USB redirection over port 32111 is tunneled over SSL connection (port 443). This option should only be used if using View 5.0 and supporting USB redirects.

Virtual Servers and Pools

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

1. ***What virtual server IP address do you want to use for remote, untrusted clients?***
   Type the IP address you want to use for the BIG-IP LTM virtual server for external clients. If you are not using BIG-IP APM, this is the address external clients use to access View. If you are using BIG-IP APM, this is the IP address the APM uses for sending traffic to the BIG-IP LTM and then to the View Servers.

2. ***What virtual server IP address do you want to use for local clients?***
This is optional. Type the IP address you want to use for the BIG-IP LTM virtual server for internal, trusted clients. This IP address, combined with the port you specify below, becomes the BIG-IP virtual server address and port, which internal clients use to access the application. The system intercepts requests to this IP:Port and distributes them to the View Connection servers. Leave this field blank if you do not wish to create a virtual server for internal trusted clients.

3. ***What service port do you want to use for the virtual server(s)?***
Specify the service port you want to use for the virtual server(s). The port you specify here is used for both the remote, untrusted client virtual server, and the optional internal, trusted virtual server.

4. ***What FQDN will clients use to access the View environment?***
Type the Fully Qualified Domain Name (FQDN) that clients use to access VMware View. In our example, we use *view.view5.example.com*, which is the host name that resolves to the LTM virtual server address in the previous question.

5. ***Which persistence profile do you want to use?*** Advanced
Select whether you want the iApp to create a new persistence profile, or if you have previously created a persistence profile for your View implementation.

   ▶ *Select the persistence profile you created from the list*
   If you have created a persistence profile for your View implementation, from the list, select the existing profile you created.

   ▶ Do not use persistence
   If your implementation does not require persistence select this option.

   ▶ Use F5's recommended persistence profile
   Select this option if you want the iApp to create a new persistence profile. The iApp creates a Source Address persistence profile, which uses the source address to direct all subsequent requests from a given client to the same View server in the pool. We recommend this method, unless you have a specific reason to use another profile.

6. ***Which load balancing method do you want to use?*** Advanced
Select the load balancing method you want to use for this View Server pool. We recommend the default, **Least Connections (member)**. For more information on the available load balancing methods, see the BIG-IP documentation or the Pool online help.

7. ***Should the BIG-IP system queue TCP requests?*** Advanced
Select whether the BIG-IP system should queue TCP requests.
TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool, as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue according to defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on Ask F5.

   ⓘ ***Important***

   TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance.
   If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port for the Client Access Server nodes.

   ▶ No, do not enable TCP request queuing
   Select this option to leave TCP request queuing disabled. We recommend leaving TCP request queuing disabled unless you have a specific need to use it.

   ▶ Yes, enable TCP request queuing
   Select this option to enable TCP request queuing. You must answer the following questions.

      a. *What is the maximum number of queued TCP requests?*
      Type the maximum number of requests you want to queue. We do ***not*** recommend using 0, which means unlimited and is only constrained by available memory.

b. *How many milliseconds should requests stay in the queue?*
Type a number of milliseconds for the TCP request timeout value.

7. ***Use a Slow Ramp time for newly added servers?*** Advanced
Select whether you want to use a Slow Ramp time.
With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added View server over a time period you specify, rather than sending a full proportion of the traffic immediately. Slow Ramp is essential when using the Least Connections load balancing method (our recommended method for View), as the BIG-IP system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

- ▶ Use Slow Ramp
Select this option for the system to implement Slow Ramp time for this pool.

  a. *How many seconds should Slow Ramp time last?*
  Specify a duration in seconds, for Slow Ramp. The time period you select for Slow Ramp is highly dependent on the speed of your server hardware and the behavior of your web services. The default setting of 300 seconds (5 minutes) is very conservative in most cases.

- ▶ Do not use Slow Ramp
Select this option if you do not want to use Slow Ramp. If you select this option, we recommend you do not use the Least Connections load balancing method.

8. ***Do you want to enable Priority Group Activation?*** Advanced
Select whether you want to use Priority Group Activation.
Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP system then sends traffic to the group of servers with the next highest priority, and so on. See the BIG-IP documentation for more details.

- ▶ Do not use Priority Group Activation
Select this option if you do not want to enable Priority Group Activation.

- ▶ Use Priority Group Activation
Select this option if you want to enable Priority Group Activation.
You must add a priority to each View server in the Priority box described in #9.

  a. *What is the minimum number of active members for each priority group?*
  Specify the minimum number of servers that must be active to continue sending traffic to the priority group. If the number of active servers falls below this minimum number you set, traffic is sent to the group of servers with the next highest priority group number.

9. ***Which servers should be included in this pool?***
Specify the IP Address for each View server. If you are using nodes that already exist on the BIG-IP system, you can select them from the list. Otherwise, type the IP address in the box. Specify the service port in the **Port** box.

   You can optionally add a Connection Limit. If you enabled Priority Group Activation, you must also specify a Priority for each device. Click **Add** to include additional servers in the pool.

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

- ▶ BIG-IP virtual servers IP and View servers are on the same subnet
Select this option if the BIG-IP virtual servers and the View servers are on the same subnet. In this case SNAT is configured on the BIG-IP virtual server and you must specify the number of concurrent connections.

a. *What is the maximum number of concurrent users you expect?*
Select whether you expect more or fewer than 6000 concurrent users to each View server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 6000) or a SNAT pool (more than 6000).

- **Fewer than 6000**
  Select this option if you expect fewer than 6000 concurrent users per server. With this option, the system applies SNAT Auto Map, which doesn't require any additional IP addresses, as the system uses an existing self IP address for translation.

- **More than 6000**
  Select this option if you expect more than 6000 users at one time to each server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 6000 users you expect.

  i). *Which IP addresses do you want to use for the SNAT pool?*
  Specify one otherwise unused IP address for every 6000 concurrent users you expect, or fraction thereof. Click **Add** for additional rows.

  Important

  If you choose more than 6000 users, but do not specify enough SNAT pool address(es), after the maximum connection limit of 6000 concurrent users per server is reached, new requests fail.

- **BIG-IP virtual server IP and View servers are on different subnets**
  If the BIG-IP virtual servers and View servers are on different subnets, the following question appears asking how routing is configured.

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

- **View servers do not have a route to clients through the BIG-IP**
  If the View servers do not have a route to clients through the BIG-IP system, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent users in the next question.

  i). *What is the maximum number of concurrent users you expect?*
  Select whether you expect more or fewer than 6000 concurrent users to each View server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 6000) or a SNAT pool (more than 6000).

  - **Fewer than 6000**
    Select this option if you expect fewer than 6000 concurrent users per server. With this option, the system applies SNAT Auto Map, which doesn't require any additional IP addresses, as the system uses an existing self IP address for translation.

  - **More than 6000**
    Select this option if you expect more than 6000 users at one time to each server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 6000 users you expect.

    1). *Which IP addresses do you want to use for the SNAT pool?*
    Specify one otherwise unused IP address for every 6000 concurrent users you expect, or fraction thereof. Click **Add** for additional rows.

    Important

    If you choose more than 6000 users, but do not specify enough SNAT pool address(es), after the maximum connection limit of 6000 concurrent users per server is reached, new requests fail.

- **View servers have a route to clients through the BIG-IP**
  Select this option if the View servers use the BIG-IP system as their default gateway. In this scenario, no additional configuration is necessary to ensure correct server response handling.

11. ***Should the BIG-IP system insert the X-Forwarded-For header?*** Advanced
    Select whether you want the BIG-IP system to insert the X-Forwarded-For header in the HTTP header for logging purposes.
    - **Yes, insert the X-Forwarded-For header**
      Select this option if you want the system to include the X-Forwarded-For header.
      You may have to perform additional configuration on your View servers to log the value of this header. For more information on configuring logging on the View servers, refer to the VMware documentation.
    - **No, do not insert the X-Forwarded-For header**
      Select this option if you do not want the system to include X-Forwarded-For in the HTTP header.

Client Optimization

In this section, you configure the client optimization settings, such as caching and compression profiles. All but one of these options are available only if you selected Advanced.

1. ***Which Web Acceleration profile do you want to use for caching?*** Advanced
   This question only appears if you chose not to deploy BIG-IP APM, or if you chose to deploy APM and to forward proxy PCoIP traffic.

   The iApp can create a new Web Acceleration profile for caching, or if you have already created a Web Acceleration profile for the View servers, you can select it from the list. You can also choose not to use a Web Acceleration profile if your implementation does not require caching on the BIG-IP system.

   Caching can improve client request response times and improve server scalability by reducing load associated with processing subsequent requests.
   - **Use F5's recommended Web Acceleration profile**
     Select this option to have the system create the recommended Web Acceleration profile. The system uses the optimized-caching parent profile for View.
   - **Do not use a Web Acceleration profile**
     Select this option if you do not require the BIG-IP system to perform caching.
   - *Select the Web Acceleration profile you created from the list*
     If you created a custom Web Acceleration profile for the View servers, select it from the list. You should only use a custom Web Acceleration profile if you need to define specific URIs that should or should not be cached.

2. ***Which HTTP compression profile do you want to use?***
   This question only appears if you chose not to deploy BIG-IP APM, or if you chose to deploy APM and to forward proxy PCoIP traffic.

   The iApp can create a new HTTP Compression profile for compression, or if you have already created an HTTP Compression profile for the View servers, you can select it from the list. You can also choose not to use an HTTP Compression profile if your implementation does not require compression on the BIG-IP system.

   Compression improves performance and end user experience for Web applications that suffer from WAN latency and throughput bottlenecks. Compression reduces the amount of traffic sent to the client to complete a transaction.
   - **Use F5's recommended compression profile**
     Select this option to have the system create the recommended HTTP Compression profile. The system uses the wan-optimized-compression parent profile for VMware View.
   - **Do not compress HTTP responses**
     Select this option if you do not require the BIG-IP system to perform compression.

- *Select the HTTP Compression profile you created from the list*
  If you created a custom HTTP Compression profile for the View servers, select it from the list.

3. ***How do you want to optimize client-side connections?*** Advanced
   The iApp can create a new client-side TCP profile what is optimized for either LAN or WAN clients, or if you have already created a TCP profile for the View servers, you can select it from the list.

   The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   - **Use F5's recommended optimizations for WAN clients**
     Select this option if the majority of clients are connecting to the environment over the WAN. The system creates the recommended WAN-optimized TCP profile using the tcp-wan-optimized parent profile for View.

   - **Use F5's recommended optimizations for LAN clients**
     Select this option if the majority of clients are connecting to the environment across the LAN. The system creates the recommended WAN-optimized TCP profile using the tcp-lan-optimized parent profile for View.

   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for the View servers, select it from the list.

Server Optimization

In this section, you configure the server optimization settings, such as OneConnect and NTLM profiles. This entire section is available only if you selected Advanced.

1. ***Which OneConnect profile do you want to use?*** Advanced
   This question does not appear if you are using the secure PCoIP proxy scenario

   The iApp can create a new OneConnect profile for connection pooling, or if you have already created an OneConnect profile for the View servers, you can select it from the list. You can also choose not to use a OneConnect profile if your implementation does not require connection pooling on the BIG-IP system.

   OneConnect (connection pooling or multiplexing) improves server scalability by reducing load associated with concurrent connections and connection rate to View servers. When enabled, the BIG-IP system maintains one connection to each View server which is used to send requests from multiple clients.

   - **Use F5's recommended OneConnect profile**
     Select this option to have the system create the recommended OneConnect profile. The system uses the oneconnect parent profile with a Source Mask of 255.255.255.255 for VMware View.

   - **Do not use a OneConnect profile**
     Select this option if you do not require the BIG-IP system to perform connection pooling using a OneConnect profile.

   - *Select the OneConnect profile you created from the list*
     If you created a custom OneConnect profile for the View servers, select it from the list.

2. ***How do you want to optimize server-side connections?*** Advanced
   The iApp can create a new server-side TCP profile what is optimized for either the LAN or WAN, or if you have already created a TCP profile for the View servers, you can select it from the list.

   The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   - **Use F5's recommended optimizations for the LAN**
     Select this option if the servers behind the BIG-IP system are on the LAN. The system creates the recommended LAN-optimized TCP profile using the tcp-lan-optimized parent profile for View.

- ▶ **Use F5's recommended optimizations for the WAN**
  Select this option if the servers behind the BIG-IP system are on the WAN. The system creates the recommended WAN-optimized TCP profile using the tcp-wan-optimized parent profile for View.

- ▶ *Select the TCP profile you created from the list*
  If you created a custom server-side TCP profile for the View servers, select it from the list.

Application Health

In this section, you configure the health monitoring settings.

1. ***Create a new health monitor or use an existing one?***
   The iApp can create a new health monitor for the View servers, or if you have already created a health monitor, you can select it from the list.

   The iApp creates an HTTP or HTTPS monitor to verify the health of the View servers, depending on whether you selected SSL offload or SSL bridging in a previous question.

   - ▶ *Select the monitor you created from the list*
     If you manually created the health monitor, select it from the list.
     If you are deploying BIG-IP APM, continue with #2, otherwise, continue with the next section.

   - ▶ **Create an advanced health monitor**
     Select this option if you want the iApp to create a new advanced health monitor. The advanced monitor verifies all View services required to render published pools are properly running, and ensures at least one available entitled pool for the user (that you specify in the following questions) is available.

     a. *What user name should the monitor use?*
        Specify the user name of an account with access to the View servers. This account must be set to never expire, otherwise, a locked, deleted, or expired account will cause the BIG-IP system to mark the servers as unavailable and they will not be accessible until the account is reactivated. We recommend creating a new user account specifically for this monitor. This user must also have at least one available and entitled Virtual Desktop pool.

     b. *What is the password associated with that account?*
        Type the password for the user name you entered in the previous question.

     c. *What is the NetBIOS domain name for your environment?*
        Type the domain name for your environment in NetBIOS format, such as DOMAIN.

   - ▶ **Create a simple health monitor**
     Select this option to enable the iApp to create a monitor that verifies basic web services are available on the View servers.

2. ***How many seconds should pass between health checks?***
   Specify how long the system should wait between each health check. This is used as the Interval setting for the monitor. We recommend the default of 30 seconds.

iRules

This section asks if you want to add custom iRules to the View deployment. This entire section is available only if you selected Advanced.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to this configuration?*** Advanced
   If you have iRules you want to attach to the virtual server the iApp creates for View, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

   If you do not want to add any iRules to the configuration, continue with the following section.

ⓘ ***Important***

While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

2. ***Do you want to add any custom iRules to the APM virtual server?*** Advanced

   If you are using BIG-IP APM, you have the option of attaching iRules to the virtual server the iApp creates for VMware View. If you have iRules to attach, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

   If you do not want to add any iRules to the configuration, continue with the following section.

   ⓘ ***Important***

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

Statistics and Logging

In this section, you configure the statistics and logging options. This entire section is available only if you selected Advanced.

1. ***Do you want to enable Analytics for application statistics?*** Advanced

   Select whether you want to enable Analytics for the View deployment.

   Analytics, also known as Application Visibility Reporting (AVR), allows you to view statistics specific to your VMware View implementation. AVR is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that this is only for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

   ⚠ ***Warning***

   Enabling Analytics may adversely affect overall system performance. If you choose to enable Analytics, we recommend gathering statistics for a set time period, such as one week, and then re-entering this template and disabling Analytics while you process the data.

   If you plan on using AVR for analytics, we recommend creating a custom Analytics profile. To create a new profile, from the Main tab, select **Profiles** and then click **Analytics**. Click **New** and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions. To select the new profile, you need to restart or reconfigure the iApp template.

   - **Do not enable Application Visibility Reporting for analytics**
     Select this option if you do not want to use Application Visibility Reporting for VMware View at this time.

   - **Use the default analytics profile**
     Select this option if you want to use the default analytics profile for your View implementation. If you want to use AVR, we strongly recommend creating a custom analytics profile for your View deployment.

   - *Select the analytics profile you created from the list*
     If you created a custom analytics profile for the View servers, select it from the list.

2. ***Which HTTP request logging profile do you want to use?*** Advanced

   The iApp allows you to use a custom Request Logging profile you created outside the template. You can also choose not to enable Request Logging.

   HTTP request logging on the BIG-IP system enables customizable log messages to be sent to a syslog server for each HTTP request processed by this application.

ⓘ ***Important***

The performance impact of using this Request Logging should be thoroughly tested in a staging environment prior to enabling on a production deployment.

The iApp does not provide the ability to create a Request Logging profile, you must have an existing profile. See Local Traffic>>Profiles: Other: Request Logging to create this profile.

- **Do not enable HTTP Request Logging**
  Select this option if you do not want to enable Request Logging at this time.

- *Select the Request Logging profile you created from the list*
  If you created a custom Request Logging profile for the View servers, select it from the list.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects. If using BIG-IP APM, you may need to click the **Apply Access Policy** link (in the upper left corner of the Configuration utility, to the right of the F5 logo) after running the iApp template.

Modifying the iApp configuration if necessary

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your VMware View Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Deleting the iApp configuration

You can simply delete the iApp configuration from the Application Services Properties page by clicking **Delete**. \

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the VMware View service you just created. To see the list of all the configuration objects created to support View, on the Menu bar, click **Components**. The complete list of all View related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

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

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

Troubleshooting

Q: *What do I use as the "External URL" in my View Connection Server settings?*

A: The External URL is the IP or DNS address that the View Client uses to connect back to the network. In this deployment guide, we give the example of the External URL https://broker.example.com:443. In this example we are suggesting that the IP addresses mapped to this Virtual Server is configured on the BIG-IP LTM. Connections from the View Client therefore map back to this IP address. If there is an upstream device, such as a firewall or router, in front of the BIG-IP LTM that is providing NAT to the BIG-IP, the External URL should be the IP or DNS address that maps to that NAT device. The NAT device would then deliver the traffic to the BIG-IP system.

Q: *Why am I seeing a "Couldn't reach port 4001 and port 389" error from the VMware client when connecting to virtual desktop?*

A: Typically, this error occurs when the Connection Server and Virtual Desktop Agent are different versions, or if the Virtual Desktop Agent has not been installed on the virtual desktop. The iApp template does not create a virtual server to manage the traffic between the agent and Connection Server. However, there could be an issue caused by the port being blocked by another network device; View Connection servers need to be able to communicate on port 4001 to the Virtual Desktop Agent.

After you have verified the correct version of the Virtual Desktop Agent has been installed on the virtual desktop, we recommend trying to verify port communication:

Ports required from Client to Agent without Security Server are:

- 3389 - RDP
- 50002 - PCoIP
- 4172 - PCoIP (View 4.6)
- 4001 -JMS

Port required from Client to Agent with Security Server is:

- 80 - HTTP and 443 to Security Server

To verify that the virtual desktop can communicate with the Connection Server over port 4001, run **netstat** on your virtual desktop using the following command:

```
netstat -an
```

If there is a connection between the local address and the Connection Server, the output looks similar to the following:

```
Proto Local Address Foreign Address State

TCP "IPOfVirtualMachine:random Port" "IP of the Connection Server:4001 ESTABLISHED
```

Note: Connectivity can be also tested by performing the netstat command on the Connection Server. After running netstat on the Connection server, the output should look similar to the following:

```
Proto Local Address Foreign Address State
TCP "IP of the Connection Server:4001 "IPOfVirtualMachine:random Port" ESTABLISHED
```

You can also just use **telnet** to do a quick test:

```
telnet <ip address> 4001
```

If you receive a connection error, check your firewalls enabled on the virtual desktop, Connection Server, or in the network infrastructure between the two points.

Q: *Why are users initially able to connect to a VDI pool, then if they log out of a desktop and choose another VDI pool, receive an error message stating "Cannot verify your connection..."?*

A: When the BIG-IP system is performing SSL bridging (if it is performing SSL offload, you will not experience this issue), if a user chooses a VDI pool, and then later logs out of that pool and attempts to choose another from the list of pools presented, they may receive the following error: "*Cannot verify your connection. The server provided a self-signed certificate instead of a verifiable certificate. Because the server has provided a verifiable certificate in the past, there is a strong likelihood that your connection is not secure. Contact your administrator for details.*"

Currently the iApp deploys a persistence profile that uses a timeout value of 180 seconds (3 minutes).

To solve this issue, modify the BIG-IP persistence profile **Timeout** value to match the View **Global Timeout** value. In View 5.2, the default Global Timeout value is 10 hours (or 36000 seconds).

There are two ways you can modify the BIG-IP configuration: create a new persistence profile and select it from within the iApp template, or modify the existing profile after disabling Strict Updates. We recommend creating a new profile and attaching it using the iApp template to avoid having to disable the Strict Updates feature.

To create a new persistence profile and add it to the iApp

a. On the Main tab, click **Local Traffic > Profiles**.

b. On the menu bar, click **Persistence**, and then click the **Create** button.

c. In the **Name** field, type a unique name.

d. From the **Persistence Type** list, select **Source Address**

e. In the **Timeout** row, click the **Custom** box, and then in the box, type a number of seconds that matches the View Global Timeout value. In our example, we type **36000**.

f. If you selected that PCoIP connections should go through the BIG-IP system and are using Security Servers, in the **Match Across Services** row, click the **Custom** box, and then check the box to enable Match Across Services.

g. Click **Finished**.

h. On the Main tab, click **iApp** > **Application Services**, and then from the list, click the name of your View Application Service.

i. On the menu bar, click **Reconfigure**.

j. In the *Virtual Servers and Pools* section, from the **Which persistence profile do you want to use?** question, select the persistence profile you just created.

k. Click the **Finished** button.

This completes the configuration for creating a new profile.

To modify the existing profile

a. On the Main tab, expand **iApp** and then click **Application Services**.

b. Click the name of your VMware View Application service from the list.

c. On the Menu bar, click **Properties**.

d. If necessary, from the **Application Service** list, select **Advanced**.

e. In the **Strict Updates** row, click the box to remove the check and disable Strict Updates.

f. Click the **Update** button.

g. On the Main tab, click **Local Traffic > Profiles**.

h. On the menu bar, click **Persistence**, and then click the persistence profile created by the iApp. This profile starts with the name you gave the iApp template, followed by **_src_addr**.

i. In the **Timeout** row, click the Custom box, and then in the box, type a number of seconds that matches the View Global Timeout value. In our example, we type **36000**.

j. Click **Update**.

k. We recommend re-enabling Strict Updates using steps a-f, but in step e, checking the **Strict Updates** box to re-enable Strict Updates.

Q: *Why do I see a black screen after successfully authenticating and selecting a pool?*

A: This is indicative of an issue with PCoIP traffic. Verify the BIG-IP system has a route to the user's Virtual Desktop, and UDP/TCP port 4172 are open. If you are using the BIG-IP system to natively proxy PCoIP, verify the BIG-IP system is running v11.4 or later with the most recent available hotfix and that your View environment is using version 5.2 or later. Verify your View client is one of the listed supported clients noted in the BIG-IP APM Client Compatibility Matrix manual for the version you are using, located at *https://support.f5.com/kb/en-us/products/big-ip_apm.html*.

If you are not using the BIG-IP system to proxy PCoIP traffic, verify the client has a route to the user's Virtual Desktop.

Q: *After configuring the BIG-IP APM as a PCoIP proxy, why are users with Horizon View 2.3 clients are having issues launching desktops?*

A: If you configured the BIG-IP APM to act as a PCoIP proxy and your users are having trouble launching desktops with Horizon View 2.3, you must add the following iRule to the HTTPS (port 443) virtual server.

If you used the iApp template to configure the BIG-IP system, you create the iRule manually and then attach it to the virtual server using the iApp. If you manually configured the system, attach the following iRule to the HTTPS (port 443) virtual server.

To create the iRule and add it to the virtual server

1. On the Main tab, expand **Local Traffic** and then click **iRules**.
2. Click **Create**.
3. In the **Name** box, type a unique name for this iRule.
4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers.

```
when HTTP_REQUEST {
    if { [HTTP::path] == "/broker/xml" && [HTTP::header Expect] == "100-continue" } {
        SSL::respond "HTTP/1.0 100 Continue\r\n\r\n"
    }
}
```

5. Click the **Finished** button.
6. Re-enter the iApp template (on the Main tab, click **iApp** > **Application Services** > [name of your View application service] and then from the Menu bar, click **Reconfigure**).
7. From the *Which configuration mode do you want to use?* question, select **Advanced - configure advanced options**.
7. In the iRules section, from the *Do you want to add any custom iRules to this configuration?* question, select the iRule you just created and then click the Add (<<) button to move it to the Selected box.
8. Click the **Update** button.

Q: *Why am I getting script errors when trying to submit the iApp template?*

A: If you are receiving an error when trying to submit the template, it may because of an APM provisioning issue. F5 has released version 1.2.1rc1 of the iApp template on DevCentral that contains the following fixes:

- Corrected an error when APM was not provisioned which prevented an LTM-provisioned-only deployment.
- Corrected an error when APM was not provisioned and using advanced monitor.

Go to *https://devcentral.f5.com/wiki/iApp.Early-Release-VMware-View-and-Horizon-View-iApp-v1-1-1rc1.ashx* to download the new iApp.

Q: *Why are available pool members being marked down after deploying the advanced health monitors?*

A: The advanced monitor created by the iApp template is unable to respond to disclaimer messages generated from Connection servers, which causes the monitor to mark servers down.

The next release of the iApp template will correct this behavior. Until that time, if you have disclaimer messages generated from Connection servers, you must either use the simple monitor option in the template (re-enter the template, and then from the "Create a new health monitor or use an existing one?" question, select "Create a Simple Monitor.") or use the BIG-IP APM to generate the disclaimer message and remove the disclaimer message from the Connection servers. See *ii). Should the BIG-IP system show a message to View users during logon? on page 15.*

Q: *Why are users getting multiple authentication prompts using the View Client?*
Why are the View desktop resources failing to render when connecting using a browser-based View connection?

A: These issues occur if you have a pre-authentication message configured on your VMware Connection servers. Because BIG-IP APM displays a login prompt for the client, you must disable the **Display a pre-login message** setting on the VMware Horizon View server (see *https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-third-party-integration-implementations-11-6-0/7.html* for more required settings for VMware Horizon View).

To workaround this issue using the iApp template, re-enter the iApp template (on the Main tab, click **iApp** > **Application Services** > [name of your View application service] and then from the Menu bar, click **Reconfigure**).
In the APM section, from the *Should the BIG-IP system show a message to View users during logon?* question, select **Yes, add a message during logon**. From the *What message should be displayed to users?* question, type the message you want to display.

Appendix: Manual configuration tables

We strongly recommend using the iApp template to configure the BIG-IP system for VMware View. Users familiar with the BIG-IP system can use the following tables to configure the BIG-IP system manually. These tables contain a list of BIG-IP configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration.

Be sure to see the optional user name based persistence methods in the previous section.

Configuring the BIG-IP LTM for load balancing and SSL offload of View Connection Servers for intranet access

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor *(Main tab-->Local Traffic -->Monitors)*	**Simple Health monitor**		
	Name	Type a unique name	
	Type	**HTTPS** (Use **HTTP** if offloading SSL)	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Send String	**GET /broker/xml/ HTTP/1.1\r\nHost: <FQDN for your View environment>\r\nConnection: Close\r\n\r\n**	
	Receive String[1]	**clientlaunch-default**	
	Advanced Health monitor (optional)		
	Because of the complexity of the advanced health monitor, you must create the monitor using the iApp template, even if you are otherwise configuring the BIG-IP system manually. In order to create the monitor using the iApp, you must answer the "What FQDN will clients use to access the View environment?" question accurately, select **Create an advanced health monitor** from the health monitor question, and then accurately answer all of the questions in the Application Health section. All other information in the iApp template does not need to be accurate.		
Pool *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Load Balancing Method	Choose your preferred load balancing method	
	Address	Type the IP Address of the Connection Server nodes	
	Service Port	**443** (Use **80** if offloading SSL) Repeat Address and Service Port for all nodes	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***HTTP*** *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
		Redirect Rewrite[3]	**Matching**[2]
	HTTP Compression *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	Web Acceleration *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**optimized-caching**
	TCP WAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Persistence *(Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
	OneConnect *(Profiles-->Other)*	Name	Type a unique name
		Parent Profile	**oneconnect**
	Client SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select your Certificate and key
	Server SSL[3] *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
		Server Name[4]	**pcoip-default-sni** [4]

[1] This appears in the default View installation. Modify as applicable for your configuration.

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers *(Main tab-->Local Traffic -->Virtual Servers)*	***Redirect virtual server***[2]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	iRule	Enable the built-in **_sys_https_redirect** iRule.
	Main virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created
	OneConnect Profile	Select the OneConnect profile you created
	HTTP Profile	Select the HTTP profile you created
	HTTP Compression Profile	Select the HTTP Compression profile you created
	WAN Optimization Profile	Select the WAN Optimization profile you created
	SSL Profile (Client)	Select the Client SSL profile you created
	SSL Profile (Server)[3]	**serverssl**[3]
	SNAT Pool	**Auto Map** (optional; see *SNAT Pools on page 37*)
	Default Pool	Select the pool you created above
	Persistence Profile	Select the persistence profile you created
	Forwarding virtual server - TCP (For PCoIP traffic routed through the BIG-IP LTM)	
	Name	Type a unique name.
	Destination	**Type**: Network **Address**: Type the appropriate address **Mask**: Type the associated subnet Mask.
	Service Port	**4172**
	Protocol	**TCP**
	SNAT Pool	**Auto Map** (optional; see *SNAT Pools on page 37*)
	Forwarding virtual server - UDP (For PCoIP traffic routed through the BIG-IP LTM)	
	Name	Type a unique name.
	Destination	**Type**: Network **Address**: Type the appropriate address **Mask**: Type the associated subnet Mask.
	Service Port	**4172**
	Protocol	**UDP**
	SNAT Pool	**Auto Map** (optional; see *SNAT Pools on page 37*)
	Forwarding virtual server - USB redirect (Optional: For USB redirect traffic routed through the BIG-IP LTM)	
	Name	Type a unique name.
	Destination	**Type**: Network **Address**: Type the appropriate address **Mask**: Type the associated subnet Mask.
	Service Port	**32111**
	Protocol	**TCP**
	SNAT Pool	**Auto Map** (optional; see *SNAT Pools on page 37*)

[2] Only necessary if you want to redirect inbound HTTP traffic to HTTPS

[3] You do not need the Server SSL profile if offloading SSL and not using PCoIP proxy. This profile is required for both SSL offload and SSL bridging when using the PCoIP proxy.

[4] Only necessary if using the BIG-IP system as a full PCoIP proxy.

SNAT Pools

If your Connection Servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, enable SNAT Auto Map to translate the client's source address to an address. The Connection Servers use this new source address as the destination address for client traffic originating through the BIG-IP.

If your View deployment is large, specifically more than 6000 simultaneous users, a SNAT Pool must be configured, with a SNAT address for each 6000 simultaneous users you expect. See the BIG-IP documentation on configuring SNAT Pools.

This completes the Connection Server LTM configuration.

Configuring the BIG-IP APM as a native PCoIP proxy for remote access

This section contains LTM and APM configuration guidance if you are using View Horizon 5.2 or later Connection Servers and BIG-IP version 11.4 or later. If you are using Security Servers or earlier versions of View, do not use this section, and continue with the APM using Edge Clients section.

Configuration for PCoIP proxy with View Horizon 5.2 Connection Servers requires 2 virtual servers. The following tables contain a list of BIG-IP system configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product documentation.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors *(Main tab-->Local Traffic -->Monitors)*	***HTTP monitor***	
	Name	Type a unique name
	Type	**HTTP**
	Alias Service Port[1]	**80**
	Send String	**GET /broker/xml/ HTTP/1.1\r\nHost: <FQDN for your View environment>\r\nConnection: Close\r\n\r\n**
	Receive String	**clientlaunch-default**[2]
	HTTPS monitor	
	Name	Type a unique name
	Type	**HTTPS**
	Alias Service Port[1]	**443**
	Send String	**GET /broker/xml/ HTTP/1.1\r\nHost: <FQDN for your View environment>\r\nConnection: Close\r\n\r\n**
	Receive String	**clientlaunch-default**[2]
	Advanced Health monitor (optional)	
	Because of the complexity of the advanced health monitor, you must create the monitor using the iApp template, even if you are otherwise configuring the BIG-IP system manually. In order to create the monitor using the iApp, you must answer the "What FQDN will clients use to access the View environment?" question accurately, select **Create an advanced health monitor** from the health monitor question, and then accurately answer all of the questions in the Application Health section. All other information in the iApp template does not need to be accurate.	
	Active Directory LDAP monitor	
	Configuration	Select **Advanced** from the Configuration list (if necessary).
	Name	Type a unique name, such as AD_LDAP_monitor.
	Type	**LDAP**
	Interval	**10** (recommended)
	Timeout	**31** (recommended)
	User Name	Type a user name with administrative permissions. This should be in Canonical Name format. For example, CN=user1,CN=Users,DC=view,DC=local,DC=com
	Password	Type the associated password
	Base	Specify your LDAP base tree. For example, CN=View Users,DC=my,DC=domain,DC=com
	Filter	Specify the filter. We type **cn=user1**, using the example above: user1 in OU group "View Users" and domain "my.domain.com"
	Security	Select a Security option (either None, SSL, or TLS)
	Chase Referrals	**Yes**
	Alias Address	***All Addresses**
	Alias Address Port	**389** (for None or TLS) or **686** (for SSL)
Pool *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name
	Health Monitors	Select the HTTP or HTTPS monitor you created, depending on the protocol you are using.
	Load Balancing Method	**Least Connections (Member)**
	Address	Type the IP Address of the Connection Server nodes
	Service Port	**443** or **80** (defaults) Depending on the protocol you are using. Repeat Address and Service Port for all nodes.

BIG-IP LTM Object	Non-default settings/Notes		
Profiles *(Main tab-->Local Traffic -->Profiles)*	***TCP WAN*** *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Client SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and key	Select the Certificate and key you imported
	Server SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
		Certificate and key	Default or imported certificate and key
		Server Name	**pcoip-default-sni**
	VDI *(BIG-IP v11.6 and later only)* *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**VDI**
AAA Servers *(Main tab-->Access Policy -->AAA Servers)*	***Active Directory AAA Server***		
	Name	Type a unique name	
	Type	**Active Directory**	
	Server Connection	**Use Pool**	
	Domain Controller Pool Name	Default is based on the name you entered above. You can optionally change it.	
	Domain Controllers	**IP Address:** Type the Ip address of a Domain Controller **Hostname:** Type the host name for the Domain Controller Click **Add** and repeat for each domain controller.	
	Server Pool Monitor	Select the AD LDAP monitor you created	
	Admin Name	If required for authentication, type the admin name	
	Admin Password	If required, type the associated password	
	Optional: SecurID AAA Server for two factor authentication		
	Name	Type a unique name.	
	Type	**SecurID**	
	Agent Host IP Address	Click **Select from Self IP LIst**. Select the self IP address that you have configured on your RSA Authentication server as an Authentication Agent.	
	SecurID Configuration File	Click **Choose File** and then browse to your SecurID Configuration file. This is the file you generated and downloaded from your RSA Authentication server.	
Remote Desktop *(Main tab-->Access Policy -->Application Access--> Remote Desktops)*	***Name***	Type a unique name.	
	Type	**VMware View**	
	Destination	Click **Pool**. Select the Connection Server pool you created.	
	Server Side SSL	Enable Server Side SSL if the servers are using encryption.	
	Auto Logon	**Enable**	
Connectivity Profile *(Main tab-->Access Policy -->Secure Connectivity)*	***Name***	Type a unique name	
	Parent Profile	**Connectivity**	
Access Profile *(Main tab-->Access Policy -->Access Profiles)*	***Name***	Type a unique name	
	Languages	Move the appropriate language(s) to the **Accepted** box.	
Access Policy	***Edit***	Edit the Access Profile you created using the Visual Policy Editor. See *Editing the Access Policy for the PCoIP proxy on page 40* for details.	

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Server *(Main tab-->Local Traffic -->Virtual Servers)*	***External Client virtual Server***	
	Name	Type a unique name.
	IP Address	Type the IP address for the virtual server
	Service Port	**443**
	Protocol Profile (client)	Select the WAN optimized TCP profile you created
	Protocol Profile (server)	Select the LAN optimized TCP profile you created
	Web Acceleration Profile	Select the Web Acceleration profile you created
	SSL Profile (Client)	Select the Client SSL profile you created
	SSL Profile (Server)	Select the Server SSL profile you created
	SNAT Pool	**Auto Map** (if you expect more than 6000 concurrent users per server, create a SNAT Pool)
	Access Profile	Select the Access profile you created and edited
	Connectivity Profile	Select the Connectivity profile you created
	VDI & Java Support	Check **Enable** (This is not necessary if using BIG-IP version 11.6 or later).
	VDI Profile	11.6 and later only: Select either the default VDI profile, or the VDI profile you created.
	Internal Client virtual Server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created
	HTTP Profile	Select the HTTP profile you created
	SSL Profile (Client)	Select the Client SSL profile you created
	SSL Profile (Server)[3]	**serverssl**[3]
	SNAT Pool	**Auto Map** (optional; see *SNAT Pools on page 37*)
	Default Pool	Select the Connection server pool you created
	Internal Client Redirect virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	iRule	Enable the built-in **_sys_https_redirect** iRule.
	PCoIP virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**4172**
	Protocol	**UDP**
	SNAT Pool [2]	**Auto Map** (if you expect more than 6000 concurrent users per server, create a SNAT Pool)
	Default Pool	None
	VDI & Java Support	Check **Enable**.

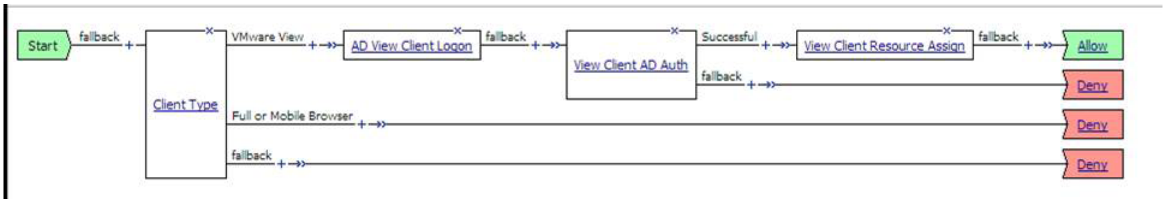
Editing the Access Policy for the PCoIP proxy

In the following procedure, we show you how to configure the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the + symbol between Start and Deny. A box opens with options for different actions.
    a. Click the Endpoint Security (Server-Side) tab, click Client Type option button, and click on add item
    b. In the Name field, you can optionally type a new name.
    c. Click the Branch Rules tab and remove all the branches except Vmware View and Full or Mobile Browser.
    d. Click Save
4. On the VMWare View branch, click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
    a. Click the Logon tab (if necessary) click **VMware View Logon Page** option button, and then click **Add item**.
    b. In the **Name** field, you can optionally type a new name.
    c. From the **VMware View Logon Screen** list, select **Windows Password**.
    d. In the **VMware View Windows Domains** box, type each domain separated by a space.
    e. Click **Save**.
5. Click the **+** symbol between **VMware View Logon Page** and **Deny**.
    a. Click the Authentication tab, click the **AD Auth** option button, and then click **Add item**.
    b. In the **Name** field, you can optionally type a new name.
    c. From the **Server** list, select the Active Directory AAA server you created using the guidance in the table.
    d. Click **Save**.
6. Click the **+** symbol on the *Successful* path between **AD Auth** and **Deny**. A box opens with options for different actions.
    a. Click the Assignment tab, click **Advanced Resource Assign**, and then click **Add item**.
    b. Click **Add new entry**.
    c. Click **Add/Delete**.
    d. Click the Remote Desktop tab, and then check the box for the Remote Desktop profile created using the guidance in the table.
    e. Click the Webtop tab, and then select the Webtop object you created using the guidance in the table.
    f. Click **Update**.
    g. Click **Save**.
7. On the fallback path between **Advanced Resource Assign**, click the **Deny** box link, click **Allow**, and then click **Save**.

    If you do not perform any of the optional steps, your VPE should look similar to the following.



The following steps are all optional.

8. (Optional: HTML 5 client support) Click the + symbol on the *Full or Mobile Browser* branch between **Client Type** and **Deny**
    a. Click the Logon tab, select the **Logon Page** option button, and then click **Add Item**.

   b. In the **Name** field, type a new name such as Browser Logon.
   c. Click **Save**.
   d. Click the + symbol on the fallback path between **Logon page** and **Deny**.
      i. Click the Assignment Tab and select **Variable Assign** option button, and then click **Add Item**.
      ii. In the **Name** field, type a new name such as **Domain Variable Assign**.
      iii. Click **Add new entry**, and then click **Change**.
      iv. On the left side, make sure **Custom Variable** and **Unsecure** are selected. In the box, type **session.logon.last.domain**.
      v. On the right side, make sure **Custom Expression** is selected. In the box, use the following syntax **expr {"<domain>"}**, where <domain> is replaced by the NETBIOS domain used for this View environment.
      vi. Click **Finished** and then click **Save**.
   e. Click the + symbol on the fallback path between **Variable Assign** and **Deny**.
      i. Click the Authentication tab, click the **AD Auth** option button, and then click **Add item**.
      ii. In the **Name** field, you can optionally type a new name such as Browser AD Auth.
      iii. From the **Server** list, select the Active Directory AAA server you created using the guidance in the table.
      iv. Click **Save**.
   f. Click the + symbol on the Successful path between AD Auth and Deny. A box opens with options for different actions.
      i. Click the Assignment tab, click **Advanced Resource Assign**, and then click **Add item**.
      ii. Click **Add new entry**.
      iii. Click **Add/Delete**.
      iv. Click the Remote Desktop tab, and then check the box for the Remote Desktop profile created using the table.
      v. Click the Webtop tab, and then select the Webtop object you created using the guidance in the table.
      vi. Click **Update**.
      vii. Click **Save**.
   g. On the fallback path between **Advanced Resource Assign** and **Deny,** click the **Deny** box link, click **Allow**, and then click **Save**.

9. (Optional: Disclaimer message) Click the **+** symbol between **Client Type** and **VMware View Logon Page**.
   a. On the Logon tab and select **VMware View Logon Page** option button, and then click **Add item**.
   b. In the **Name** box, type a new name such as *View Client Disclaimer*.
   c. From the **VMware View Logon Screen** list, select **Disclaimer**.
   d. In the **Disclaimer message** box, type the message you want presented to View users during logon.
   e. Click **Save**.
   f. (Optional: Disclaimer message with HTML 5 client support): On the **Full or Mobile Browser** branch, click the **+** symbol between **Client type** and **Browser Logon Page**.
   g. On the General Purpose Tab select **Message Box** option button, and click **Add item**.
   h. In the **Name** box, type a new name such as **View Browser Disclaimer**.
   i. In the **Message** box, type the message you want presented to View users during logon.
   j. Click **Save.**

10. (Optional: RSA SecurID two-factor authentication logon page) Click the **+** symbol between **View Client Disclaimer** (or **Client Type** if you did not create the disclaimer message) and **VMware View Logon Page**.

a. On the Logon tab, click **VMware View Logon Page** option button, and then click **Add item**.

b. In the **Name** field, type a new name such as *SecurID View Client Logon*.

c. From the **VMware View Logon Screen** list, select **RSA SecurID**.

d. In the **Disclaimer message** box, you can type a message you want presented to View users during SecurID logon.

e. Click **Save**.

f. (Optional: RSA SecureID two-factor authentication with HTML 5 support logon page) Click the **Browser Logon** page to open and modify the logon page.

g. Modify the **Post Variable** and **Session Variable** name for item 2 to **password1**.

h. Modify Type item 3 from **None** to **password**.

i. Modify the **Post Variable** and **Session Variable** name for item 3 to **password**.

j. In **Logon Page Input Field #3**, type a name such as **Passcode**.

k. Click **Save.**

11. (Optional: RSA SecurID authentication) Click the **+** symbol between **SecurID View Client Logon** and **VMware View Logon Page**.

a. Click the Authentication tab, click the **RSA SecurID** option button, and then click **Add item**.

b. In the **Name** field, type a new name, such as *RSA SecurID Auth*.

c. From the **AAA Server** list, select the RSA AAA profile you created using the guidance in the table.

d. Click **Save**.

e. (Optional: RSA SecurID authentication with HTML 5 client support) Click the + symbol on the fallback path between **Browser logon** page and **Domain Variable Assign**.

f. Click the Authentication tab, click the **RSA SecurID** option button, and then click **Add item**.

g. In the **Name** field, type a new name such as *RSA SecurID Browser Auth*.

h. From the **AAA Server** list, select the RSA AAA profile you created using the guidance in the table.

i. Click **Save**.

j. Click the + symbol between RSA SecurID Browser Auth and Domain variable assign

k. Click the Assignment tab, click the **Variable Assign** option button, and then click **Add item**.

l. In the **Name** field, type a new name such as *Password Variable Assign*.

m. Click **Add new entry**, and then click **Change**.

n. On the left side, make sure **Custom Variable** and **Unsecure** are selected. In the box, type **session.logon.last.password**.

o. On the right side, make sure **Custom Expression** is selected. In the box, use the following syntax:
expr {[mcget {session.logon.last.password1}]}

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

12. (Optional: If using a translation device between the View Clients and the BIG-IP system) Click the + symbol between **AD Auth** and **Advanced Resource Assign**.

a. Click the Assignment Tab and select Variable Assign option button, and then click **Add item**.

b. In the **Name** field, type a new name such as *NAT Variable Assign*.

c. Click **Add new entry**, and then click **Change**.

d. On the left side, make sure **Custom Variable** and **Unsecure** are selected. In the box, type **view.proxy_addr**.

e. On the right side, make sure **Custom Expression** is selected. In the box, use the following syntax **expr {"<ip address>"}**, where <ip address> is replaced by the public network translated IP address.

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

g. (Optional: If using a translation device between the View Clients and the BIG-IP system with HTML 5 client support) Click the + symbol between **Browser AD Auth** and **Browser Resource Assign**.

h. Click the Assignment Tab and select the **Variable Assign** option button, and then click **Add item**.

i. In the **Name** field, type a new name such as *Browser NAT Variable Assign.*

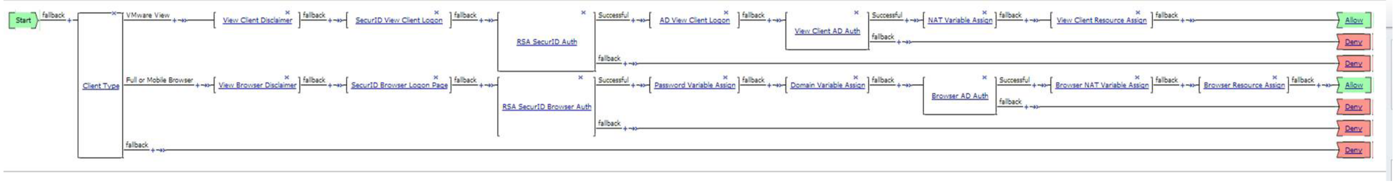
j. Click **Add new entry**, and then click **Change**.

k. On the left side, make sure **Custom Variable** and **Unsecure** are selected. In the box, type **view.proxy_addr**.

l. On the right side, make sure **Custom Expression** is selected. In the box, use the following syntax: **expr {"<ip address>"}**, where <ip address> is replaced by the public network translated IP address.

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

If you use all the available options, your VPE should look similar to this:



Configuring the BIG-IP LTM for load balancing View Security Servers

This section contains LTM configuration guidance if you are using the Security Servers. If you are not using Security Servers, do not use this section, and continue with the APM section.

Configuration for Security Server requires three virtual servers. The following tables contain a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product documentation.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors *(Main tab-->Local Traffic -->Monitors)*	***TCP***	Name	Type a unique name
		Type	**TCP**
		Alias Service Port[1]	**4172**
	HTTPS	Name	Type a unique name
		Type	**HTTPS**
		Alias Service Port[1]	**443**
		Send String	**GET /broker/xml/ HTTP/1.1\r\nHost: <FQDN for your View environment>\r\nConnection: Close\r\n\r\n**
		Receive String	**clientlaunch-default[2]**
	UDP	Name	Type a unique name
		Type	**UDP**
		Alias Service Port[1]	**4172**
	USB Redirect	Name	Type a unique name
		Type	**TCP**
		Alias Service Port[1]	**32111**
Pool *(Main tab-->Local Traffic -->Pools)*	***HTTPS Pool***		
	Name	Type a unique name	
	Health Monitors	Select the HTTP monitor you created	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the Security Server nodes	
	Service Port	**443** (repeat Address and Service Port for all nodes)	
	UDP Pool		
	Name	Type a unique name	
	Health Monitors	Select the TCP and UDP monitors you created	
	Availability Requirement[1]	**All**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the Security Server nodes	
	Service Port	**4172** (repeat Address and Service Port for all nodes)	
	USB Redirect Pool		
	Name	Type a unique name	
	Health Monitors	Select the HTTP monitor you created	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the Security Server nodes	
	Service Port	**32111** (repeat Address and Service Port for all nodes)	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***HTTP*** *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
	TCP WAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**

BIG-IP LTM Object	Non-default settings/Notes		
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP LAN*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	UDP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**UDP**
	Persistence (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Match Across Services	Check this box
		Mirror Persistence	If using a redundant pair of BIG-IP devices, check this box
	Client SSL (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate	Select the Certificate you imported
		Key	Select the Key you imported
	Server SSL (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
		Certificate and key	Default or imported certificate and key
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**TCP**		
	Name	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**4172**	
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above	
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Source Address Persistence profile you created above	
	HTTPS		
	Name	Type a unique name.	
	Address	Type the same IP Address for the virtual server	
	Service Port	**443**	
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above	
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	SSL Profile (client)	Select the Client SSL profile you created above	
	SSL Profile (server)	Select the Server SSL profile you created above	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])	
	Default Pool	Select the HTTPS pool you created above	
	Persistence Profile	Select the Source Address Persistence profile you created above	
	UDP		
	Name	Type a unique name.	
	Address	Type same the IP Address for the virtual server	
	Service Port	**4172**	
	Protocol	**UDP**	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] If your Security Servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, enable SNAT Auto Map to translate the client's source address to an address. The Security Servers will use this new source address as the destination address for client traffic originating through the BIG-IP. If your View deployment is exceptionally large, specifically more than 6000 simultaneous users, a SNAT Pool must be configured. See the BIG-IP documentation on configuring SNAT Pools.

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Protocol Profile (client)***[1]	Select the UDP profile you created above
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])
	Default Pool	Select the UDP pool you created above
	Persistence Profile	Select the Source Address Persistence profile you created above
	USB Redirect	
	Name	Type a unique name.
	Address	Type same the IP Address for the virtual server
	Service Port	**32111**
	Protocol	**TCP**
	Protocol Profile (client)[1]	Select the TCP profile you created above
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])
	Default Pool	Select the USB Redirect pool you created above
	Persistence Profile	Select the Source Address Persistence profile you created above

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] If your Security Servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, enable SNAT Auto Map to translate the client's source address to an address. The Security Servers will use this new source address as the destination address for client traffic originating through the BIG-IP.
If your View deployment is exceptionally large, specifically more than 6000 simultaneous users, a SNAT Pool must be configured. See the BIG-IP documentation on configuring SNAT Pools.

Configuring the BIG-IP APM as a forwarding PCoIP proxy using the BIG-IP Edge Client

In this section, we configure the BIG-IP Access Policy Manager (APM) for the VMware View Security or Connection Servers. APM may be used with either of the configuration modes described in the LTM portion of this guide. This table contains any non-default setting you should configure as a part of this deployment. Settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help.

BIG-IP Object	Non-default settings/Notes	
DNS and NTP	See *Configuring BIG-IP LTM DNS and NTP settings on page 12* for instructions.	
AAA Servers health monitor *(Main tab-->Local Traffic -->Monitors)*	***Name***	Type a unique name
	Type	**LDAP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the user name of a valid Active Directory user account.
	Password	Type the associated password
	Base	Type the LDAP tree for system account. For example: user@my.domain.com is in organizational unit view users: ou=view users,dc=my,dc=domain,dc=com
	Filter	Type the filter for the system account. For example cn=user
	Alias Service Port	**389**
AAA Servers *(Main tab-->Access Policy -->AAA Servers)*	***Name***	Type a unique name
	Type	**Active Directory**
	Server Connection	**Use Pool**
	Domain Controller Pool Name	Default is based on the name you entered above. You can optionally change it.
	Domain Controllers	**IP Address:** Type the Ip address of a Domain Controller **Hostname:** Type the host name for the Domain Controller Click **Add** and repeat for each domain controller.
	Server Pool Monitor	Select the monitor you created
	Admin Name	If required for authentication, type the admin name
	Admin Password	If required, type the associated password
Network Access *(Main tab-->Access Policy -->Network Access)*	***Name***	Type a unique name
	Caption	Type a caption. By default, the system uses the name you typed. Click **Finished**, but stay on this page to configure DNS/Hosts.
- **Network Access DNS/ Hosts** *(Access Policy--> Network Access-->*DNS/Hosts)	***Primary Name Server***	Type the IP address of your Active Directory server.
	DNS Default Domain Suffix	Type the default Domain suffix. We type **localhost**.
Lease Pools *(Main tab-->Access Policy -->Network Access--> Lease Pools)*	***Name***	Type a unique name
	Member List: Type	Click **IP Address** or **IP Address Range** as applicable
	Member List: IP address	Type the applicable IP address. If you selected IP Address Range, type a start and end IP address.
Connectivity Profile *(Main tab-->Access Policy -->Secure Connectivity)*	***Name***	Type a unique name
	Parent Profile	**Connectivity**
Web Application *(Main tab-->Access Policy -->Web Applications)*	***Name***	Type a unique name. We use **DownloadViewClient**
	Patching	Type: **Minimal Patching**. Click **Scheme Patching** box. Click **Create**. Stay on Web Application page to add Resource item.
- Resource Items *(Web Application page-->Resource Items section-->Add)*	***Destination***	Click **IP Address** option button. Type the IP address of the LTM virtual server you created for the Connection Servers.
	Port	Type **443**
	Scheme	Select **HTTPS**
	Paths	Type **/***
	Compression	Select **GZIP** ***All other settings at the defaults***

BIG-IP Object	Non-default settings/Notes		
Webtop *(Main tab--> Access Policy-->Webtops)*	***Name***	Type a unique name.	
	Type	**Full**	
Webtop Link *(Main tab-->Access Policy-->Webtop Links)*	***Name***	Type a unique name.	
	Application URI	Type the IP address or FQDN of the LTM virtual server you created for the Connection Servers or Security Servers.	
Health Monitor *(Main tab-->Local Traffic -->Monitors)*	***Name***	Type a unique name.	
	Type	If using Security Servers, select **HTTPS** If using Connection Servers and no SSL offload, select **HTTPS** If using Connection Servers and offloading SSL, select **HTTP**.	
	Interval	Type an Interval. We recommend **30**.	
	Timeout	Type a Timeout. We recommend **91**.	
	Send String	**GET /broker/xml/ HTTP/1.1\r\nHost: <FQDN for your View environment>\r\nConnection: Close\r\n\r\n**	
	Receive String	**clientlaunch-default**[1]	
Pools *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name	
	Health Monitor	Select the health monitor you created above	
	Load Balancing Method	Choose **Least Connections (Member)**	
	Address	Type the IP address of BIG-IP LTM virtual server you created	
	Service Port	If using Security Servers, select **HTTPS** If using Connection Servers and no SSL offload, select **HTTPS** If using Connection Servers and offloading SSL, select **HTTP**	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***Rewrite*** *(Profiles-->Services)*	Name	Type a unique name
		Client Caching Type	Must be set to **CSS and Java Script**
	HTTP *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
	HTTP Compression *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	Web Acceleration *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**optimized-caching**
	TCP WAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	Client SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and key	Select your Certificate and Key
	Server SSL[2] *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
Access Profile *(Main tab-->Access Policy -->Access Profiles)*	***Name***	Type a unique name	
	Languages	Move the appropriate language(s) to the **Accepted** box.	
Access Policy	***Edit***	Edit the Access Profile you created using the Visual Policy Editor. See *Editing the Access Policy on page 21* for details.	

[1] This appears in the default View installation. Modify as applicable for your configuration.

[2] 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. 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.

BIG-IP Object	Non-default settings/Notes	
Virtual Server *(Main tab-->Local Traffic -->Virtual Servers)*	***Name***	Type a unique name.
	IP Address	Type the IP address that clients will use for access.
	Service Port	443
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	HTTP Compression Profile	Select the HTTP Compression profile you created above
	Web Acceleration Profile	Select the Web Acceleration profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SSL Profile (Server)	If applicable, select the Server SSL profile you created above
	SNAT Pool	**Auto Map** (if you expect more than 6000 concurrent users, create a SNAT Pool)
	Access Profile	Select the Access profile you created and edited above
	Connectivity Profile	Select the Connectivity profile you created above
	Rewrite Profile	Select the Rewrite profile you created above
	Access Profile	Select the Access profile you created and edited above
	Default Pool	Select the pool you created above

[1] This appears in the default View installation. Modify as applicable for your configuration

Editing the Access Policy

In the following procedure, we show you how to configure the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

*In the following example, we are configuring the Access Policy for the optional anti-virus check. If you do not want to perform the anti-virus check, skip those steps. However because the procedure references the antivirus VPE objects when specifying the paths, see **VPE Example on page 57** for a visual representation of the VPE in our example and how the paths would flow without the anti-virus checks.*

To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Client OS** option button, and then the **Add Item** button.
   a. In the **Name** field, you can optionally type a new name.
   b. Click the **Branch Rules** tab.
   c. For each of the following Branch rules, click the delete (**x**) button on the right: **Linux**, **iOS**, **Android**, and **Windows mobile**. In this guide, we detect Windows and Mac systems in order to provide AutoLaunch and Single Sign On. Currently VMware only supports these features on the Windows Platform. If you would like to provide specific actions for other client operating systems in your environment, you may choose to leave these paths in place and customize the VPE accordingly.
   d. Click the **Change** button located at the bottom of the Windows branch.
   e. For each of the following click the delete (x) button on the right: **Windows 2000**, **Windows Server 2003**, **Windows Server 2008**, and **Windows NT**. These specific Windows operating systems are not supported by View Client and should be removed.
   f. Click the **Finished**.
   g. Click the **Save** button.

5. *Optional:* If you want the APM to perform a check for antivirus software for Windows clients, on the Windows path between Client OS and Deny, click the **Antivirus Check** option button, and then click **Add Item**.
   Configure the check as applicable for your configuration. In our example, we leave the default. Click **Save**.

   In the rest of the examples in this procedure, we assume this antivirus check is in place.

6. *Optional:* If you want the APM to perform a check for antivirus software for Mac clients, on the MacOS path between Client OS and Deny, click the **Antivirus Check** option button, and then click **Add Item**.

   From the **State** list, select **Unspecified**. Configure the check as applicable for your configuration, we leave the defaults. Click **Save**.

   In the rest of the examples in this procedure, we assume this antivirus check is in place.

7. *Optional:* Click the (**+**) button located on the fallback branch located between **Client OS** and **Deny**. Click the Antivirus Check option button and then click **Add Item**.
   a. Click the Branch Rules tab.
   b. Click the **Change** link.
   c. Under OR, click the **Add Expression** button.
   d. From the **Agent Sel** list, select **Client OS**.
   e. From the **Condition** list, select **Client OS** (if necessary).
   f. From the **Client OS is** list, select **Android**.
   g. Return to step c and repeat steps c-f. In step f, select iOS in place of Android.
   h. Click **Finished**.
   i. From the State list, select **Unspecified**, and then click **Save**.
      Note: Android and iOS currently do not support antivirus client side checks.
      In the rest of the examples in this procedure, we assume this antivirus check is in place.

8. On the *Windows* - Successful path, between **Antivirus check** and **Deny** click the **+** symbol.

9. Click the **Logon Page** option button, and then the **Add Item** button.
   a. Configure the Logon Page as applicable for your configuration. In our example, we leave the default.
   b. Click **Save**.

10. On the *Windows Fallback* path between **Logon Page** and **Deny**, click the **+** symbol.

11. Click the **Variable Assign** option button, and then click the **Add Item** button. Complete the following:
    a. In the **Name** box, you can optionally type a new name. We type **Password Session Variable Assign**.
    b. Click the **Add new entry** button.
    c. Click the **change** link.
    d. From the lists on the left, leave **Custom Variable** and **Unsecure** selected.
    e. In the left box, type **session.custom.pass**.
    f. From the list on the right, select **Session Variable**.
    g. In the box, type **session.logon.last.password**.
    h. Click **Finished** and then click **Save**.

12. On the *Windows Fallback* path between **Password Session Variable Assign** (or the name you gave the Variable Assign object you just created) and **Deny**, click the **+** symbol.

13. Click the **AD Auth** option button, and then the **Add Item** button.
    a. From the **Server** list, select the AAA server you configured in the configuration table.

   b. All other settings are optional.
   c. Click **Save**. You now see a Successful and Fallback path from AD Auth.

14. On the *Successful* path between **AD Auth** and **Deny**, click the **+** symbol.
15. 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.
    b. Click the **Add new entry** button.
    c. In the **FileName** box, type the path to the View Client as appropriate for your View deployment. In our example, we type the default path:

```
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.*

    d. From the **Version Comparison** list, select **=**.
    e. Leave the rest of the settings at their default levels.
    f. Click the **Save** button. You know see a Successful and Fallback path from Windows File Check.

16. On the *Successful* path between **Windows File Check** and **Deny**, click the **+** button.
17. Click the **Full Resource Assign** option button, and then the **Add Item** button. Complete the following:
    a. Click the **Add New Entry** button.
    b. Click the **Add/Delete** link.
    c. Click the Network Access Resources tab.
    d. Click the option button for the Network Access Resource object you created in the configuration table.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop you created in the configuration table.
    g. Click **Update**.
    h. Click **Save**.

18. On the *Fallback* path between **Full Resource Assign** and **Deny**, click the **+** button.
19. Click the **Variable Assign** option button, and then click the **Add Item** button. The Resource Assignment page opens.
    a. In the **Name** box, you can optionally type a new name.
    b. Click the **Add new entry** button.
    c. Click the **change** link.
    d. From the list on the left, select **Configuration Variable** and then select **Secure** from the adjacent list.
    e. From the **Type** list, select **Network Access** if necessary.
    f. From the **Name** list, select the name of the Network Access object you created in the configuration table if necessary.
    g. From the **Property** list, near the bottom, select **application_launch**.
    h. 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).

    The following expression 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 proper section of code from the following text file:

http://www.f5.com/solutions/resources/deployment-guides/files/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 %{session.custom.pass} -domainName view5 -serverURL https://
broker.example.com:443</parameter><os_type>WINDOWS</os_type></item></application_launch>"}
```

If your View Client is installed in a custom location, be sure to set the correct path to the executable. Our domainName is view5; 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.

i. Click the **Finished** button.

j. On the Variable Assign page, click the **Save** button.

20. On the *Fallback* path after **Variable Assign** click the **Deny** box link.
21. Click the **Allow** option button, and then click **Save**.
22. Back on the Fallback path between **Windows File Check** and **Deny**, click the **+** button.
23. Click the **Decision Box** option button and then click **Add Item**. Complete the following:

    a. Configure the Properties as applicable. We leave the defaults.

    b. Click the **Branch Rules** tab.

    c. In the **Name** box, type **Download the View Client**.

    d. Click **Save**.

24. On the *Download View Client* path between **Decision Box** and **Deny**, click the **+** button.
25. Click the **Webtop and Links Assign** option button and then click **Add Item**. Complete the following:

    a. Click the **Add/Delete** link next to **Webtop Links**.

    b. Check the box for the Webtop Link you created in the configuration table.

    c. Click the **Add/Delete** link next to **Webtop**.

    d. Check the box for the Webtop you created in the configuration table.

    e. Click **Save**.

26. On the Fallback path after **Webtop and Links Assign** click the **Deny** box link.
27. Click the **Allow** option button, and then click **Save**.
28. Back near the Start, on the *Fallback* path between **Antivirus Check** and **Deny**, click the **+** symbol.
29. Click the **Message Box** option button, and then click **Add Item**.

    a. In the **Message** box, type the message that is presented to the user in the event their antivirus check fails.

    b. In the **Link** box, type the link text users will click. The user session restarts once they click this link.

    c. Click **Save**.

30. Back near the Start, on the *MacOS - Successful* path between **Antivirus Check** and **Deny**, click the **+** symbol.
31. Click the **Logon Page** option button, and then the **Add Item** button.

    a. Configure the Logon Page as applicable for your configuration. In our example, we leave the default.

    b. Click **Save**.

32. On the MacOS *Fallback* path between **Logon Page** and **Deny**, click the **+** symbol.
33. Click the **AD Auth** option button, and then the **Add Item** button.
    a. From the **Server** list, select the AAA Server you configured in the configuration table.
    b. All other settings are optional.
    c. Click **Save**. You now see a Successful and Fallback path from AD Auth.
34. On the *Successful* path between **AD Auth** and **Deny**, click the **+** symbol.
35. Click the **Mac File Check** option button, and then click the **Add Item** button. The Mac File Checker page opens. Complete the following:
    a. In the **Name** box, you can optionally type a new name.
    b. Click the **Add new entry** button.
    c. In the **FileName** box, type the path to the View Client as appropriate for your View deployment. In our example, we type the default path:
    /Applications/VMware View Client.app
    d. Leave the rest of the settings at their default levels.
    e. Click the **Save** button. You know see a Successful and Fallback path from Mac File Check.
36. On the *Successful* path between **Mac File Check** and **Deny**, click the **+** button.
37. Click the **Full Resource Assign** option button, and then the **Add Item** button. Complete the following:
    a. Click the **Add New Entry** button.
    b. Click the **Add/Delete** link.
    c. Click the **Network Access Resources** tab.
    d. Click the option button for the Network Access Resource object you created in the configuration table.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop you created in the configuration table.
    g. Click **Update**.
    h. Click **Save**.
38. On the Fallback path between **Full Resource Assign** and **Deny**, click the **+** button.
39. 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.
    b. Click the **Add new entry** button.
    c. Click the **change** link.
    d. From the list on the left, select **Configuration Variable** and then select **Secure** from the adjacent list.
    e. From the **Type** list, select **Network Access** if necessary.
    f. From the **Name** list, select the name of the Network Access object you created in the configuration table if necessary.
    g. From the **Property** list, near the bottom, select **application_launch**.
    h. 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).

    The following expression 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 proper section of code from the following text file: *www.f5.com/solutions/resources/deployment-guides/files/view-vpe-expression.txt*.
And then carefully replace the values in red below with values from your implementation.

```
expr {"<application_launch><item><path>/usr/bin/open</path><parameter>vmware-view://[mcget {session.
logon.last.username}]@broker.example.com:443/?domainName=BD</parameter><os_type>MAC</os_type></
item></application_launch>"}
```

Our domainName is BD; insert the correct name of your domain. The @ 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.

i. Click the **Finished** button.

j. On the Variable Assign page, click the **Save** button.

40. On the Fallback path after **Variable Assign** click the **Deny** box link.
41. Click the **Allow** option button, and then click **Save**.
42. Back on the Fallback path between **Mac File Check** and **Deny**, click the **+** button.
43. Click the **Decision Box** option button and then click **Add Item**. Complete the following:
    a. Configure the Properties as applicable. We leave the defaults.
    b. Click the **Branch Rules** tab.
    c. In the **Name** box, type **Download the View Client**.
    d. Click **Save**.
44. On the *Download View Client* path between **Decision Box** and **Deny**, click the **+** button.
45. Click the **Webtop and Links Assign** option button and then click **Add Item**. Complete the following:
    a. Click the **Add/Delete** link next to **Webtop Links**.
    b. Check the box for the Webtop Link you created in the configuration table.
    c. Click the **Add/Delete** link next to **Webtop**.
    d. Check the box for the Webtop you created in the configuration table.
    e. Click **Save**.
46. On the Fallback path after **Webtop and Links Assign** click the **Deny** box link.
47. Click the **Allow** option button, and then click **Save**.
48. Back near the Start, on the MacOS fallback path between **Antivirus Check** and **Deny**, click the **+** symbol.
49. Click the **Message Box** option button, and then click **Add Item**.
    a. In the **Message** box, type the message that is presented to the user in the event their antivirus check fails.
    b. In the **Link** box, type the link text users will click. The user session restarts once they click this link.
    c. Click **Save**.
50. Back near the start, on the *successful* path between the bottom **Antivirus Check** box and **Deny**, click the **+** button.
51. Click **Logon Page** option button, and then the **Add Item** button.
    a. Configure the Logon Page as applicable for your configuration. In our example, we leave the default.
    b. Click **Save**.

52. On the *Fallback* path between **Logon Page** and **Deny**, click the **+** symbol.
53. Click **AD Auth** option button, and then the **Add Item** button.
    a. From the **Server** list, select the AAA server you configured in the configuration table.
    b. All other settings are optional.
    c. Click **Save**. You now see Successful and Fallback paths from AD Auth.
54. On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
55. Click **Full Resource Assign** option button, and then the **Add Item** button. Complete the following:
    a. Click the **Add New Entry** button.
    b. Click the **Add/Delete** link.
    c. Click the Network Access Resources tab.
    d. Click the option button for the Network Access Resource object you created in the configuration table.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop you created in the configuration table.
    g. Click **Update**.
    h. Click **Save**.
56. On the Fallback path after **Full Resource Assign** and **Deny**, click the **+** button.
57. 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.
    b. Click the **Add new entry** button.
    c. Click the **change** link.
    d. From the list on the left, select **Configuration Variable** and then select **Secure** from the adjacent list.
    e. From the **Type** list, select **Network Access** if necessary.
    f. From the **Name** list, select the name of the Network Access object you created in the configuration table if necessary.
    g. From the **Property** list, near the bottom, select **application_launch**.
    h. 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).
    The following expression 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 proper section of code from the following text file: *www.f5.com/solutions/resources/deployment-guides/files/view-vpe-expression.txt*.
    And then carefully replace the values in red below with values from your implementation.

```
expr {"<application_launch><item><path>/usr/bin/firefox</path><parameter>vmware-view://[mcget
{session.logon.last.username}]@broker.example.com:443/?domainName=BD</parameter><os_type>UNIX</os_
type></item></application_launch>"}
```

    Our domainName is BD; insert the correct name of your domain. The @ 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 View Client documentation for more information.
    i. Click the **Finished** button.

   j. On the Variable Assign page, click the **Save** button.

58. On the *fallback* path after **Variable Assign**, click the **Deny** box link.

59. Click the **Allow** option button, and then click **Save**.

60. Back near the Start, on the *Fallback* path between the lower **Antivirus Check** box and **Deny**, click the **+** symbol.

61. Click the **Message Box** option button, and then click **Add Item**.

   a. In the **Message** box, type the message that is presented to the user in the event their antivirus check fails.

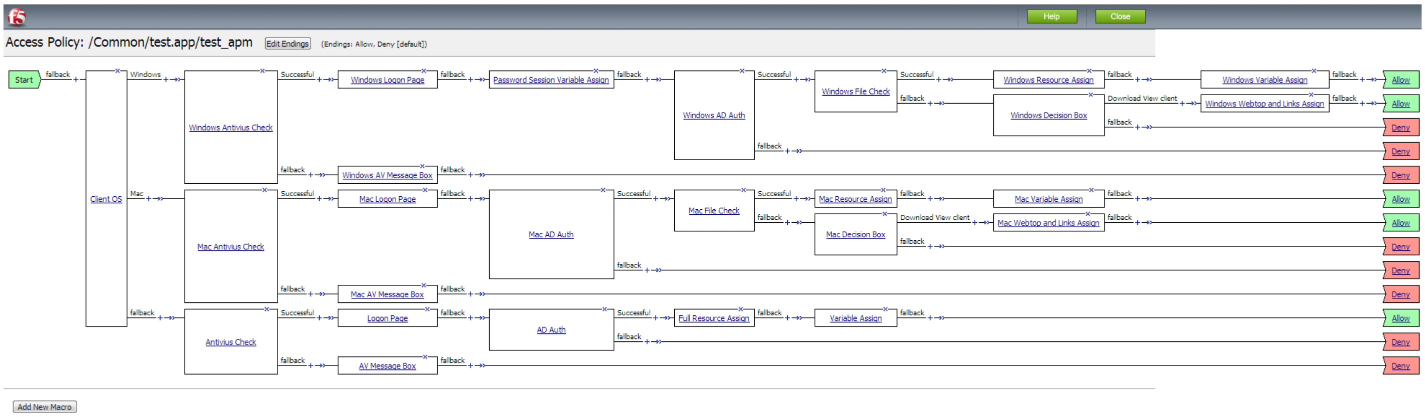
   b. In the **Link** box, type the link text users will click. The user session restarts once they click this link.

   c. Click **Save**.

62. 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.

When complete, if you configured the optional antivirus checks, your VPE will look like the following example (in this example, we did not change any of the object names, so additional objects of the same type have a (1) and (2) next to them).

VPE Example



Access Policy: /Common/test.app/test_apm

(Endings: Allow, Deny [default])

This completes the manual configuration.

Document Revision History

Version	Description	Date
1.0	New deployment guide for the fully supported iApp f5.vmware_view.v1.2.0 available on downloads.f5.com. This iApp contains the following features and fixes (these items were contained in release candidates iApps): - Added BIG-IP v11.6 Support - Added option to create trusted View Client Virtual server connection - Added advanced monitoring option, which verifies all View Connection services are functioning rather than simple monitor which only verifies web services. - Corrected an issue in the LDAP monitor so it now correctly uses canonical user name format. Modified the Product and version footnote on page 1 to mention an engineering hotfix is available from F5 technical support for BIG-IP v11.6 which enables the View Remote App publishing feature.	12-16-2014
1.1	Added a new troubleshooting entry on *page 33* concerning script errors when trying to submit the template. As a part of the resolution, noted the release of v1.2.1rc1 of the iApp template on DevCentral.	01-28-2015
1.2	Added a new troubleshooting entry on *page 34* concerning pool members being unavailable after deploying advanced health monitors.	02-11-2015
1.3	Updated this guide for the fully supported iApp f5.vmware_view.v1.2.1 available on downloads.f5.com. There were no new features in this release, only the following fixes: - The iApp now correctly uses Source IP persistence when an internal virtual server is used - The iApp now allows using advanced monitors when BIG-IP APM is not used, by asking an additional question about the NetBIOS name. Previously, the iApp would display a script error. - The iApp no longer displays a script error when in LTM only mode. Previously, the iApp would display an error when BIG-IP APM was not provisioned. - Modified the note in the Product version table on page 1 to state that support for the View Remote App publishing feature is available in BIG-IP v11.6 HF-4 and later.	04-09-2015
1.4	Added support for VMware Horizon View 6.1, with the exception that BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.	04-30-2015
1.5	- Added a footnote to the Product and Version table page 1 to mention that BIG-IP APM does not support proxying the VMware View RDP protocol. - For BIG-IP APM, removed official support for VMware View 5.0 and 5.1.	05-20-2015
1.6	Added a new troubleshooting entry on *page 34* concerning possible issues when using APM with pre-authentication messages configured on the View Connection servers.	06-22-2015

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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