



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	11.4 - 12.0 iApp version 1.4.0 requires 11.5.0 and later iApp version 1.3.0 requires 11.3.0 and later
VMware Horizon View	5.2, 5.3, 6.0 ¹ , 6.1 ¹ , 6.1.1 ^{1,2,4,5} , 6.2 ^{2,4,5}
iApp Template version	f5.vmware_view.v1.3.0 and f5.vmware_view.v1.4.0rc1 - rc3
Deployment Guide version	2.4 (see <i>Document Revision History on page 55</i>)
Last updated	04-01-2016

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. You must install 11.6 HF5 for Horizon View HTML5 client support in Horizon View 6.1.

² BIG-IP APM v12.0 requires **HF1** to support the Horizon View HTML5 client in Horizon View 6.1.1 or later.

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

⁴ You must be using BIG-IP 11.6 HF-6 (Hotfix-BIGIP-11.6.0.6.0.442-HF6) or later in the 11.x branch for Horizon View 6.1.1 and 6.2.

⁵ BIG-IP APM does not currently support the Linux Virtual Desktop feature introduced in v6.1.1.

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?	3
Prerequisites and configuration notes	3
Configuration examples and traffic flows	3
Modifying the View configuration	6
VMware Virtual Desktop Manager Global Settings	6
Configuring the BIG-IP iApp for View	11
Advanced options	12
Template options	12
BIG-IP Access Policy Manager	12
Advanced Firewall Manager (AFM)	17
SSL Encryption	19
PC over IP	20
Virtual Servers and Pools	21
Client Optimization	24
Server Optimization	25
Application Health	26
iRules	27
Statistics and Logging	28
Finished	29
Next steps	30
Troubleshooting	31
Appendix A: Configuring additional BIG-IP settings	35
Appendix B: Manual configuration tables	36
Configuring the BIG-IP LTM for load balancing and SSL offload of View Connection Servers for intranet access	36
Configuring the BIG-IP APM as a native PCoIP proxy for remote access	39
Configuring the BIG-IP LTM for load balancing View Security Servers	47
Manually configuring the BIG-IP Advanced Firewall Module to secure your View deployment	50
Document Revision History	55

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 11*.
 - » **Manual configuration**
If configuring the BIG-IP system manually, after modifying the VMware Virtual Desktop Manager Global Settings, see *Appendix B: Manual configuration tables on page 36*. Because of the complexity of the configuration, we recommend using the iApp template.
- ▶ For this deployment guide, the BIG-IP LTM system **must** be running version 11.4 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.
- ▶ For clarification on the version callouts in the Product Versions table on page 1, see the appropriate APM Client Compatibility Matrix guide for your version. For example, for v11.6:
https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-11-6-0.html
For v12.0: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-12-0-0.html
- ▶ 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.
- ▶ **New** If your SSL key is password protected, it will not appear as a selectable option in the iApp template. To use a password protected key, you must manually create a Client SSL profile outside the iApp template and then select it from the list. See Local Traffic > Profiles > SSL > Client to create an Client SSL profile. You can add the passphrase while creating the profile.

➡ **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.

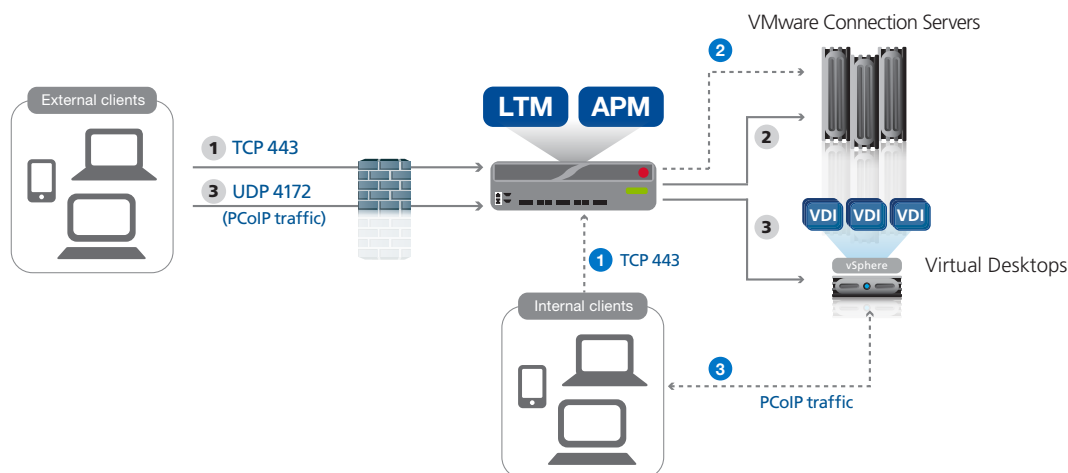
An additional option shows how to use the BIG-IP system to natively proxy PCoIP connections in a reliable and secure manner, thereby removing the need for VMware Security Servers. When using this option, you optionally can support HTML 5 browser based clients for users that are unable to install the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

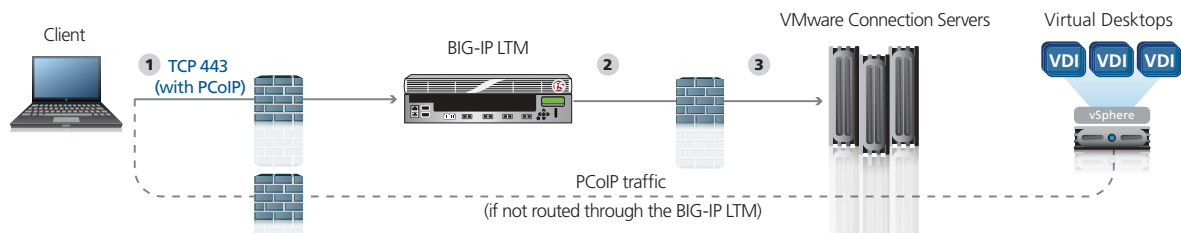
1. The client device (regardless of Mac, Windows, HTML 5, iPad, Zero Client) makes a connection to the virtual IP address on your BIG-IP system. The BIG-IP establishes a new connection to the Connection Servers and proceeds with authentication.
2. The BIG-IP system persists the TCP 443 XML connection 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.



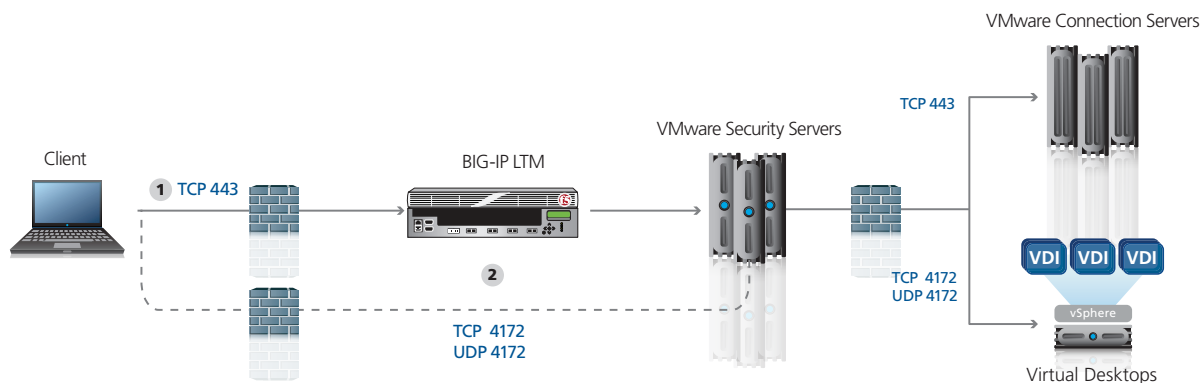
For deployments without Security Servers the traffic flow is:

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 traffic is 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 Security Servers and Connection Servers

This traffic flow diagram shows the BIG-IP LTM with a VMware 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 and should not be used if BIG-IP APM is available. 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.

Modifying the View configuration

In this section, we describe the tasks necessary 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 9*).

VMware Virtual Desktop Manager Global Settings

Before configuring the BIG-IP LTM, you must 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. Clear the check from **Use Blast Secure Gateway for HTML access to desktop**.
 - f. 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
```

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. 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
```

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, refer to the VMware documentation.

1. Download the **HTML Access Web Portal installer** from the downloads section of the VMware website.
Note: *This is only necessary if using a View version prior to 6.0. Version 6.0 and later has a check box during installation ("Install HTML Access") to include HTML 5.*
 - 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**.
Note: *This is only necessary if using a View version prior to 6.0. Version 6.0 and later has a check box during installation ("Install HTML Access") to include HTML 5.*
 - 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.

Modifying your Connection Servers to support two-pin prompt with Smart Card authentication

Use the following guidance to modify the Connection Servers to support the two-pin prompt solution with smart cards. For specific information, refer to the VMware documentation.

Important: All of these steps must be performed on each Connection server.

- Follow View documentation for Obtaining Certificate Authority Certificates and placing into truststore file: <https://pubs.vmware.com/horizon-62-view/index.jsp#com.vmware.horizon-view.administration.doc/GUID-2A035E01-599A-4A2E-8265-2DE014AB7244.html>
- Modify View Connection Server Configuration Properties: <https://pubs.vmware.com/horizon-62-view/index.jsp#com.vmware.horizon-view.administration.doc/GUID-86F44C4A-64EE-4AEA-94FD-8F6367865129.html>
- Configure SAML Authenticators in View Administrator: <https://pubs.vmware.com/horizon-62-view/index.jsp#com.vmware.horizon-view.administration.doc/GUID-CC32E0E2-373A-4875-9452-45C2DE55B7E1.html>
 - » In Authentication tab, set **Delegation of authentication to VMware Horizon** drop down to **Allowed**.
 - » Create a New Authenticator, using Metadata URL where <YOUR HORIZON SERVER NAME> is replaced with FQDN created for the BIG-IP (response to the question “What hostname is used to resolve to the IDP virtual server address?” in the iApp)
- Configure Smart Card Settings in View Administrator using the following settings: <https://pubs.vmware.com/horizon-62-view/index.jsp#com.vmware.horizon-view.administration.doc/GUID-B928C5CD-2884-420F-875F-69FB4B6999A8.html>
 - » In Authentication tab, set smart card authentication for user to **Required**.
- Reboot any Connection Servers you modified.

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> for the fully supported version.
NOTE: We recommend using iApp version **f5.vmware_view.v1.4.0rc3** which contains two fixes over 1.4.0rc1, available on DevCentral: <https://devcentral.f5.com/codeshare/vmware-horizon-view-iapp>.
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.v<latest version>** file.
We recommend using the new **f5.vmware_view.v1.4.0rc1** available in the RELEASE_CANDIDATE directory.
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 B: Manual configuration tables on page 36*.

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.v1.4.0** (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

This entire section only appears if you have licensed and provisioned BIG-IP APM

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 3* 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 plug-in, 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 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 for this View deployment.

- a. **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.

- b. **Should the BIG-IP APM support smart card authentication for Horizon View?**

Note: This question only appears in v1.4.0rc1 and later of the iApp template. If you are using a previous version, continue with step c asking about two-factor authentication.

Choose whether you want the BIG-IP system to support smart card authentication. You should select this option if your Horizon clients use smart cards to authenticate with the Horizon View implementation. If you select Yes, the iApp configures the BIG-IP APM to authenticate to the Horizon View Connection servers using smart cards. In this scenario, users must enter their PIN twice, once as they authenticate to APM (which will authenticate with VCS using SAML assertion token), and once as the Horizon View application or desktop is launched.

- **No, do not support smart card authentication**

Select this option if you do not need the system to support smart card authentication. Continue with step c.

- **Yes, support smart card authentication**

Select this option if you want the system to support smart card authentication. You must answer the following questions.

- a. **What virtual server IP address do you want to use for Horizon View server SAML requests?**

Type the IP address for SAML IDP services which will be used by View servers to validate authentication.

- b. **What hostname is used to resolve to the IDP virtual server address?**

Type the FQDN which is used to resolve to the IP address you entered for SAML IDP services.

- c. **What are the hostnames for your Horizon View Connection servers?**

Type the FQDN(s) of the View Connection servers you want to send SAML assertions. Click Add to include more hostnames.

- d. **Which Client SSL profile do you want to use for your SAML identity provider?**

If you have already created a Client SSL profile that includes the appropriate certificate and key, you can select it from the list. Otherwise, the iApp creates a new Client SSL profile.

- e. **Which SSL certificate do you want to use?**

Select the SSL certificate you imported for this deployment. Importing certificates and keys is not a part of this template, see Local Traffic >> SSL Certificate List. To select any new certificates and keys you import, you need to restart or reconfigure this template.

To establish encrypted communication, a client and server negotiate security parameters that are used for the session. As part of this handshake, a certificate is provided by the server to the client to identify itself. The client can then validate the certificate with an authority for authenticity before sending data. When the BIG-IP system is decrypting communication between the client and server, an SSL certificate and key pair for each fully-qualified DNS name related to this application instance must be configured on the system.

- f. **Which SSL private key do you want to use?**

Select the associated SSL key. This application service configuration is incomplete and will not be secure until you import and assign a trusted certificate and key that are valid for all fully qualified domain names used to access the application. See Local Traffic >> SSL Certificate List for importing certificates and keys. To select any new certificates and keys you import, you need to restart or reconfigure this template.

- g. **If external clients use a network translated address to access View, what is the public-facing IP address?**

You may not be translating your public address, however, if you are, enter the public NAT IP address View Clients resolve to for initial connections.

- c. Should the BIG-IP system support RSA SecurID for two-factor authentication? (f5.vmware_view.v1.3.0)
Should the BIG-IP system support RSA SecurID or RADIUS for two-factor authentication? (f5.vmware_view.v1.4.0rc1+)

Note: The question asking about RADIUS only appears in v1.4.0rc1 and later of the iApp template. If you are using a previous version, you only see the option for RSA SecurID two-factor authentication.

- **No, do not support RSA SecurID two-factor authentication** (f5.vmware_view.v1.3.0)
No, do not support RSA SecurID or RADIUS two-factor authentication (f5.vmware_view.v1.4.0rc1+)
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.
- **Yes, support RSA SecurID with AD two-factor authentication**
Select this option if you want to configure two-factor authentication using SecurID on the BIG-IP system.

i 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.

- a. 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.

- b. What label do you want to use for the SecurID in field?

There are three logon form fields when using two-factor authentication: User Name and Password, which are used to authenticate the user against Active Directory, and a third field which is used to pass the user's SecurID pin. Type the label you want the BIG-IP system to give this field. The default is **Passcode**.

- **Yes, support RADIUS with AD two-factor authentication (f5.vmware_view.v1.4.0rc1+ only)**

Select this option if you want to support RADIUS with AD two-factor authentication. You must answer the following questions.

- a. Create a new RADIUS AAA Server object or select an existing one?

Select 'Create a new RADIUS AAA Server object' if you want the system to create a new BIG-IP APM AAA server. If you have manually created a custom RADIUS AAA server object for this implementation, you can select it from the list.

- Select an existing RADIUS AAA Server from the list
If you already created a BIG-IP APM RADIUS AAA Server object for this implementation, select it from the list. Only AAA Servers with a Type of RADIUS appear in the list.
- **Create a new RADIUS AAA server object**
If you have not created a custom RADIUS AAA Server object for this deployment, leave this default option, and answer the following questions.
 - a. Which RADIUS servers are used for second factor user credential authentication?
Specify the IP address of each of your RADIUS servers used for this View environment. Click the Add button for additional rows.
 - b. Which port are you using for your RADIUS servers?
Specify the authentication port number of your AAA RADIUS servers. The default is 1812.
 - c. What password are you using for your shared secret?
Specify the shared secret password set on your AAA RADIUS servers.
 - d. What IP are you using for your NAS-IP-address?
Specify an IP address to use as RADIUS attribute 4, the NAS-IP-address, that you can configure without changing the source IP address in the IP header of the RADIUS packets. This is useful in situations where you are using a cluster of NAS to be recognized as a single RADIUS client. This is optional.
 - e. Create a new monitor for the RADIUS servers?
Choose whether you want to create a new RADIUS monitor, use a simple ICMP/ping monitor, or choose an existing monitor. The remaining questions in this section are all related to the RADIUS monitor.
 - Select an existing RADIUS monitor from the list
If you already created a RADIUS monitor for this implementation, select it from the list. Only monitors with a Type of RADIUS appear in the list.
 - **Do not monitor RADIUS**
Select this option if you do not want the BIG-IP system to monitor the RADIUS servers. We strongly recommend allowing the system to monitor these servers.

- **Yes, create a simple ICMP monitor**
Select this option if you want the BIG-IP system to monitor the RADIUS server using a simple ICMP (ping) health check.
- **Yes, create a new RADIUS monitor**
Select this option if you want the template to create a new health check to monitor the RADIUS servers.
 - a. *Which RADIUS user name should the monitor use?*
Specify a RADIUS user name. You should select an account that does not expire or has a mandatory password change. Note, your RADIUS servers will become unavailable if this account is locked out or deleted for any reason.
 - b. *What is associated password?*
Type the password associate with the user you just entered
 - c. *How many seconds between RADIUS health checks?*
Type the password associate with the user you just entered.

d. *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.

- a. *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.

e. *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.

f. *Do you want the BIG-IP system to support multiple Domains?* **Advanced**

Select whether your View implementation uses a single Active Directory domain or if your View environment requires support for authenticating to multiple Active Directory domains. If you are not using Advanced mode, continue with #a under *No, my View environment uses a single Active Directory domain* on the next page.

i Important *If you require support for multiple Active Directory domains, you must have manually created BIG-IP APM "AAA Server" objects for each domain you want to include. The iApp template does not create multiple AAA Server objects (but does create a single AAA server if necessary). See Access Policy > AAA Servers to create the AAA servers. For assistance, see the Help tab or product documentation.*

- **Yes, support multiple Active Directory Domains**
Select this option if you require support for multiple Active Directory Domains.
 - a. *Which AAA Server objects did you create for the Active Directory Domains?*
From the list, select the first AAA Server object you created for this View implementation. Click the **Add** button to add the other AAA Servers you created for this deployment.
 - b. *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 on the next page.
 - c. *Which APM logging profile do you want to use?*
This question only appears if you are using BIG-IP version 12.0 or later

BIG-IP version 12.0 allows you to attach a logging profile to your BIG-IP APM configuration. If you created an APM logging profile for this configuration, you can select it from the list. The default profile is named **default-log-setting**. For more information on APM logging, see the BIG-IP APM documentation for v12.0 and later.
 - **Do not specify a logging profile for the APM profile**
Select this option if you do not want to use an APM logging profile at this time. You can always re-enter the template at a later date to choose a logging profile. Continue with the next section.

- **Select an existing APM logging profile from the list**
If you already created a BIG-IP APM logging profile, or want to use the default profile (**default-log-setting**), select it from the list.

Continue with *SSL Encryption* on page 19.

- **No, my View environment uses a single Active Directory Domain**

Select this option if your View implementation uses a single Active Directory domain. You must answer the following questions.

- a. **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 on the next page.

- b. **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.

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?**

Type the fully qualified domain name (FQDN) used for the 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.

- a. **Which Active Directory user with administrative permissions do you want to use?**

Type an Active Directory user name with administrative permissions.

- b. **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.

- a. **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.
 - b. **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.
 - c. **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, a 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.
 - d. **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.
 - e. **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.
 - f. **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.
- e. **Which APM logging profile do you want to use?**
This question only appears if you are using BIG-IP version 12.0 or later
- BIG-IP version 12.0 allows you to attach a logging profile to your BIG-IP APM configuration. If you created an APM logging profile for this configuration, you can select it from the list. The default profile is named **default-log-setting**. For more information on APM logging, see the BIG-IP APM documentation for v12.0 and later.
- **Do not specify a logging profile for the APM profile**
Select this option if you do not want to use an APM logging profile at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.
 - **Select an existing APM logging profile from the list**
If you already created a BIG-IP APM logging profile, or want to use the default profile (**default-log-setting**), select it from the list.

Advanced Firewall Manager (AFM)

This entire section only appears if you have licenced and provisioned BIG-IP AFM

This section gathers information about BIG-IP Advanced Firewall Manager if you want to use it to protect your View deployment. For more information on configuring AFM, see <http://support.f5.com/kb/en-us/products/big-ip-afm.html>, and then select your version.

1. **Do you want to use BIG-IP AFM to protect your application?**

Choose whether you want to use BIG-IP AFM, F5's network firewall, to secure this View deployment. If you choose to use BIG-IP AFM, you can restrict access to the View virtual server(s) to a specific network or IP address. See the BIG-IP AFM documentation for specific details on configuring AFM.

- **No, do not use Application Firewall Manager**
Select this option if you do not want to enable BIG-IP AFM at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.
- **Select an existing AFM policy from the list**
If you already created a BIG-IP AFM policy for your View implementation, select it from the list. Continue with **c**.
- **Yes, use F5's recommended AFM configuration**
Select this option if you want to enable BIG-IP AFM using F5's recommended configuration.

a. Do you want to restrict access to your application by network or IP address?

Choose whether you want to restrict access to the View implementation via the BIG-IP virtual server.

- **No, do not restrict source addresses (allow all sources)**

By default, the iApp configures the AFM to accept traffic destined for the View virtual server from all sources. If you do not have a need to restrict access to the virtual server, leave this option selected and then continue with **b**.

- **Restrict source addresses**

Select this option if you want to restrict access to the View virtual server by IP address or network address.

- a. What IP or network addresses should be allowed to access your application?

Specify the IP address or network access that should be allowed access to the View virtual server. You can specify a single IP address, a list of IP addresses separated by spaces (not commas or other punctuation), a range of IP addresses separated by a dash (for example **192.0.2.10-192.0.2.100**), or a single network address, such as **192.0.2.200/24**.

b. How do you want to control access to your application from sources with a low reputation score?

The BIG-IP AFM uses an IP intelligence database to categorize IP addresses coming into the system. Choose what you want the system to do for sources that are attempting to access the View virtual server with a low reputation score. For more information, see the BIG-IP AFM documentation.

 **Important** You must have an active IP Intelligence license for this feature to function. See <https://f5.com/products/modules/ip-intelligence-services> for information.

- **Allow all sources regardless of reputation**

Select this option to allow all sources, without taking into consideration the reputation score.

- **Reject access from sources with a low reputation**

Select this option to reject access to the View virtual server from any source with a low reputation score.

- **Allow but log access from sources with a low reputation**

Select this option to allow access to the View virtual server from sources with a low reputation score, but add an entry for it in the logs.

c. Would you like to stage a policy for testing purposes?

Choose whether you want to stage a firewall policy for testing purposes. A staged policy allows you to evaluate the effect a policy has on traffic by analyzing the system logs, without actually modifying traffic based on the firewall rules. You must already have a policy on the system in order to select it.

- **Do not apply a staging policy**

Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.

- **Select an existing policy from the list**

If you have already created a firewall policy for this implementation, select it from the list. Only policies that already exist on the system appear in the list. To create a new policy, on the Main tab, click **Security > Network Firewall > Policies**. Specific instructions for creating a firewall policy is outside the scope of this iApp and deployment guide.

d. Which logging profile would you like to use?

Choose whether you or not you want to use a logging profile for this AFM implementation. You can configure the BIG-IP system to log detailed information about BIG-IP system Network Firewall events and store those logs on the BIG-IP system or a remote logging server (supports syslog and Splunk). If you want to use a logging profile, we recommend creating one outside this template. The list only contains profiles with Network Firewall enabled.

- **Do not apply a logging profile**

Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.

- **Select an existing logging profile from the list**

If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging Profiles**. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the **BIG-IP Network Firewall: Policies and Implementations** guide for more information.

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.

Intermediate 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. **Do you want to redirect inbound HTTP traffic to HTTPS?** **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. **From which port should traffic be redirected?**

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. **Which Server SSL profile do you want to use?** **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 selected to use the BIG-IP APM as a PCoIP gateway.

1. **Should PCoIP connections go through the BIG-IP system?**

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 *Virtual Servers and Pools on page 21*; 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. **Will PCoIP connections be proxied by the View Security Servers?**

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.

- a. On which network do the Virtual Desktops reside?
Specify the network on which the Virtual Desktops reside.
- b. What is the network mask for the virtual desktops?
Type the subnet mask associated with the network of the Virtual Desktops.
- c. 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.
 - a. 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.
 - a. 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.

2. Will VMware View HTML 5 client connections go through the BIG-IP system?

Select whether your View HTML 5 client connections will go through the BIG-IP system or not. For more information on HTML 5 support in View, see the VMware documentation.

- **No, support only View Client connections**
Choose No if you only need to support View Client connections and do not need to support the View HTML 5 client.
- **Yes, support HTML 5 View clientless browser connections**
Choose this option to enable support for both HTML 5 clientless browser connections and View Client connections to the Virtual Desktops. You must verify the Connection servers are configured to direct HTML 5 connections to the BIG-IP virtual server address.

Virtual Servers and Pools

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

i 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 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.

8. 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.

9. ***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.

10. ***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.

11. ***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.

a. ***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.

- 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.

- a. *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.

i 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.

12. **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 LAN-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 onconnect 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 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.
- **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.

d. Do Connection servers have a pre-login message enabled?

Choose whether your View Connections servers require a pre-login message. A pre-login message requires the user agree to the message to continue.

- **No, Connection servers do not have a pre-login message**

Select this option if your Connection servers do not have a pre-login message enabled.

- **Yes, Connection servers have a pre-login message**

Select this option if your Connection servers are configured to display a pre-login message. Selecting Yes configures the BIG-IP health monitor to send the correct response to the pre-login message sent by the Connection server.

e. Which logging level do you want to use for this monitor?

Select the log level for the associated monitor being used in this solution. Log entries are found in the LTM system log file: **/var/log/ltn**.

- **Monitor logs disabled**

Select this option if you do not want monitor logs enabled at all

- **Monitor logging enabled**

Select this option if you want the monitor logs enabled at the default level (as opposed to verbose logging).

- **Verbose monitor logging enabled**

Select this option if you want to enable verbose logging for the health monitor.

f. What published application(s) or pool(s) should the BIG-IP system expect in the monitor response?

Type the published application name or pool the BIG-IP system should look for in the response to the health monitor. The published application name or desktop pool is case sensitive and must exactly match the resource display name you have configured on your Connection servers; spaces are ok in this field. Click the **Add** button to include additional pools or applications.

g. Do all published applications or desktop pools listed need to be available?

If you specified multiple applications or pools in the previous question, you have the option of requiring only one of the applications or pools to be returned by the server, or requiring all of the applications and pools you specified be available.

- **Only one of the applications or desktop pools listed need to be returned by the server**

Select this option if you want the health monitor to require only one of the applications or pools you specified is returned by the servers in order for the server to be marked as available.

- **All listed applications or desktop pools need to be returned by the server**

Select this option if you want the health monitor to require all of the applications or pools you specified are returned by the servers in order for the server to be marked as available. If even one of the applications or pools is not returned, the server will be considered unavailable by the BIG-IP system until all applications or pools are once again available.

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.

 **Warning** 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. We recommended you verify the impact of an iRule prior to deployment in a production environment.

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.

 **Warning** 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. We recommended you verify the impact of an iRule prior to deployment in a production environment.


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 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 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.

```
1  when HTTP_REQUEST {
2      if { [HTTP::path] == "/broker/xml" && [HTTP::header Expect] == "100-continue" } {
3          SSL::respond "HTTP/1.0 100 Continue\r\n\r\n"
4      }
5  }
```

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 be because of an APM provisioning issue. This issue has been fixed as of version 1.2.1rc1 of the iApp template. If you are experiencing this issue, upgrade your application service to v1.2.1rc1 or later of the iApp template.

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 *d. 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 workaroud 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.

Q: *Why do I see "http 500 error" directly after trying to connect to BIG-IP system?*

A: This could be a result of BIG-IP removing weak *Diffie Hellman* encryption (DHE) options from its cipher suite starting in BIG-IP release 12.0. If running BIG-IP TMOS 12+, add the following cipher string to your Server SSL profile:

DEFAULT:!DHE:@STRENGTH. Doing so will remove the option to use DHE and order the remaining available cipher preferences according to strength.

Q: *Why are applications or Virtual Desktop resources not responding after selecting a resource?*

A: PCoIP (port 4172) TCP network traffic will flow through any matching virtual server that exists on the BIG-IP system (for example, an **any:any** forwarding virtual server), which may lead to Virtual Desktops failing to launch. You should ensure that your BIG-IP system does not contain virtual servers that will match TCP port 4172 network traffic to VMware Virtual Desktops.

Appendix A: Configuring additional BIG-IP settings


This section contains information on configuring the BIG-IP system for objects or settings that are required, but not part of the template.


Configuring DNS and NTP settings

If you are configuring the iApp to use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the iApp.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

 **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 self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. 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 a DNS server that can resolve the Active Directory server.
 - b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

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

To configure NTP settings

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

To verify the NTP setting configuration, you can use the **ntpq** utility. From the 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.

Appendix B: 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

Health Monitors (<i>Local Traffic > Monitors</i>)		
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 String¹	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.		
Pools (<i>Local Traffic > Pools</i>)		
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 (<i>Local Traffic > Profiles</i>)		
HTTP (<i>Profiles-->Services</i>)	Name Parent Profile Redirect Rewrite ³	Type a unique name http Matching²
HTTP Compression (<i>Profiles-->Services</i>)	Name Parent Profile	Type a unique name wan-optimized-compression
Web Acceleration (<i>Profiles-->Services</i>)	Name Parent Profile	Type a unique name optimized-caching
TCP WAN (<i>Profiles-->Protocol</i>)	Name Parent Profile	Type a unique name tcp-wan-optimized
TCP LAN (<i>Profiles-->Protocol</i>)	Name Parent Profile	Type a unique name tcp-lan-optimized
Persistence (<i>Profiles-->Persistence</i>)	Name Persistence Type	Type a unique name Source Address Affinity
OneConnect (<i>Profiles-->Other</i>)	Name Parent Profile	Type a unique name oneconnect
Client SSL (<i>Profiles-->SSL</i>)	Name Parent Profile Certificate and Key	Type a unique name clientssl Select your Certificate and key
Server SSL³ (<i>Profiles-->SSL</i>)	Name Parent Profile Ciphers Server Name ⁴	Type a unique name serverssl <i>v12.0 and later only:</i> DEFAULT:!DHE:@STRENGTH pcoip-default-sni⁴

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

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.

Virtual Servers (Local Traffic > Virtual Servers)

Redirect virtual server²

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	serverssl³
Secure Address Translation	Auto Map (optional; see <i>SNAT Pools on page 38</i>)
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
Secure Address Translation	Auto Map (optional; see <i>SNAT Pools on page 38</i>)

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
Secure Address Translation	Auto Map (optional; see <i>SNAT Pools on page 38</i>)

Forwarding virtual server - HTML 5 (Optional)

Name	Type a unique name.
Destination	Type: Network Address: Type the appropriate address Mask: Type the associated subnet Mask.
Service Port	8443
Protocol	TCP
Secure Address Translation	Auto Map (optional; see <i>SNAT Pools on page 38</i>)

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.

Importing the script file for the optional advanced health monitor

Before you can create the advanced monitor described in the following table, you must import the monitor script file onto the BIG-IP system.

 **Note:** *If you are using a redundant BIG-IP system, you need to make sure any modifications to the script EAVs are manually copied between BIG-IP LTMs, and given the required permissions when configuration is synchronized.*

To download and install the script

1. Download the script: http://www.f5.com/pdf/deployment-guides/adv_view_eav_example.zip
2. Extract the appropriate file(s) to a location accessible by the BIG-IP system.
3. From the Main tab of the BIG-IP Configuration utility, expand **System**, and then click **File Management**.
4. On the Menu bar, click **External Monitor Program File List**.
5. Click the **Import** button.
6. In the **File Name** row, click **Browse**, and then locate the appropriate file.
7. In the **Name** box, type a name for the file related to the script you are using.
8. Click the **Import** button.

Now when you create the advanced monitors, you can select the name of the file you imported from the **External Program** list.

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.

Health Monitors (<i>Local Traffic > Monitors</i>)																	
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-default²																
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-default²																
Advanced Health monitor (optional)																	
Name	Type a unique name																
Type	External																
Interval	30 (recommended)																
External Program	See <i>Importing the script file for the optional advanced health monitor on page 38</i>																
Variables	<table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>ALL</td> <td><0 or 1> Where 0 means only one published application or desktop pool needs to be returned by the server, and 1 means all applications or pools must be returned</td> </tr> <tr> <td>APP1, APP2, APP3, etc</td> <td><published application name> The published application(s) or pool(s) the system should expect in the monitor response. App1 is required, use additional APP# variables for more applications/desktop pools.</td> </tr> <tr> <td>DEBUG</td> <td><0, 1 or 2> Where 0 is no logging, 1 is normal logging, and 2 is verbose logging</td> </tr> <tr> <td>DISCLAIMER</td> <td><0 or 1> Where 0 means no pre-login message/disclaimer message, and 1 means the View Connection servers are set to display a disclaimer message</td> </tr> <tr> <td>NETBIOS</td> <td><domain> The NetBIOS domain name for your View implementation</td> </tr> <tr> <td>PASSWORD</td> <td><password> The password for the username you want to use in the health check. This is stored in plaintext on the BIG-IP system.</td> </tr> <tr> <td>USERNAME</td> <td><username> The password for the username you want to use in the health check</td> </tr> </tbody> </table>	Name	Value	ALL	<0 or 1> Where 0 means only one published application or desktop pool needs to be returned by the server, and 1 means all applications or pools must be returned	APP1, APP2, APP3, etc	<published application name> The published application(s) or pool(s) the system should expect in the monitor response. App1 is required, use additional APP# variables for more applications/desktop pools.	DEBUG	<0, 1 or 2> Where 0 is no logging, 1 is normal logging, and 2 is verbose logging	DISCLAIMER	<0 or 1> Where 0 means no pre-login message/disclaimer message, and 1 means the View Connection servers are set to display a disclaimer message	NETBIOS	<domain> The NetBIOS domain name for your View implementation	PASSWORD	<password> The password for the username you want to use in the health check. This is stored in plaintext on the BIG-IP system.	USERNAME	<username> The password for the username you want to use in the health check
Name	Value																
ALL	<0 or 1> Where 0 means only one published application or desktop pool needs to be returned by the server, and 1 means all applications or pools must be returned																
APP1, APP2, APP3, etc	<published application name> The published application(s) or pool(s) the system should expect in the monitor response. App1 is required, use additional APP# variables for more applications/desktop pools.																
DEBUG	<0, 1 or 2> Where 0 is no logging, 1 is normal logging, and 2 is verbose logging																
DISCLAIMER	<0 or 1> Where 0 means no pre-login message/disclaimer message, and 1 means the View Connection servers are set to display a disclaimer message																
NETBIOS	<domain> The NetBIOS domain name for your View implementation																
PASSWORD	<password> The password for the username you want to use in the health check. This is stored in plaintext on the BIG-IP system.																
USERNAME	<username> The password for the username you want to use in the health check																
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 636 (for SSL)																

Pools (<i>Local Traffic > Pools</i>)	
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.
Profiles (<i>Local Traffic > Profiles</i>)	
TCP WAN (<i>Profiles-->Protocol</i>)	Name Parent Profile Type a unique name tcp-wan-optimized
TCP LAN (<i>Profiles-->Protocol</i>)	Name Parent Profile Type a unique name tcp-lan-optimized
Client SSL (<i>Profiles-->SSL</i>)	Name Parent Profile Certificate and key Type a unique name clientssl Select the Certificate and key you imported
Server SSL (<i>Profiles-->SSL</i>)	Name Parent Profile Ciphers Certificate and key Server Name Type a unique name serverssl <i>v12.0 and later only:</i> DEFAULT:!DHE:@STRENGTH Default or imported certificate and key pcoip-default-sni
VDI (<i>BIG-IP v11.6 and later only</i>) (<i>Profiles-->Services</i>)	Name Parent Profile Type a unique name VDI
AAA Servers (<i>Access Policy-->AAA Servers</i>)	
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.
Optional: RADIUS AAA Server for two factor authentication	
Name	Type a unique name.
Type	RADIUS
Mode	Authentication
Server Connection	Use Pool
Server Pool Name	Type a unique name.
Server Addresses	Type the IP addresses of your RADIUS server
Server Pool Monitor	Optional but recommended: Select a health monitor for your RADIUS servers.
Authentication Service Port	If necessary, type the service port used by your RADIUS servers
Secret (and Confirm Secret)	Type and confirm your RADIUS secret
NAS IP Address (and/or IPv6)	If applicable, type the NAS IP Address and/or the NAS IPv6 Address

Optional: Active Directory Trusted Domains AAA Server for multiple AD domains (only) - BIG-IP APM v11.5 and later

Name	Type a unique name.
AAA Servers	Click AAA Servers in the left pane. From the Available list, select all of the applicable AAA servers.
Root	Select the root domain that should be used for the initial authentication request.

Remote Desktop (*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

Remote Desktop (*Access Policy > Secure Connectivity*)

Name	Type a unique name
Parent Profile	Connectivity

Access Profile (*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 <i>Editing the Access Policy for the PCoIP proxy on page 42</i> for details.
-------------	--

Virtual Servers (*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
Secure Address Translation	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	serverssl³
Secure Address Translation	Auto Map (optional; see <i>SNAT Pools on page 38</i>)
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
Secure Address Translation	Auto Map (if you expect more than 6000 concurrent users per server, create a SNAT Pool)
Default Pool	None
VDI & Java Support	Check Enable

Manually configuring the BIG-IP APM to support smart card authentication

Because of the complexity of the APM configuration for supporting smart card authentication for View, at this time we are not providing manual configuration guidance, and direct users who want to support smart card authentication to use the iApp template.

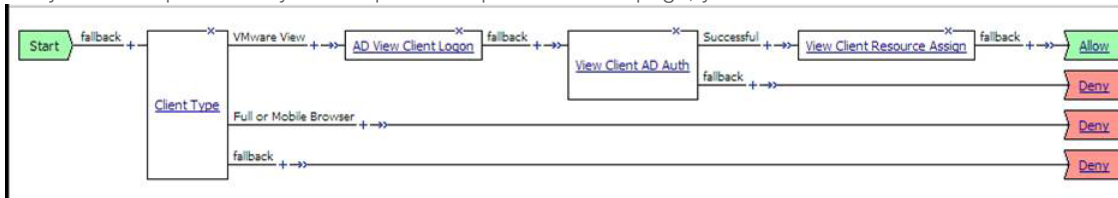
Editing the Access Policy for the PCoIP proxy

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 then click **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. The next step depends on whether you are using a single AD domain or multiple AD domains (v11.5+ only)
 - If you are using a single AD implementation:* From the **Server** list, select the Active Directory AAA server you created using the guidance in the table.
 - If you are using multiple AD domains (v11.5+):* From the **Cross Domain Support** list, select **Enabled**. From the **Trusted Domains** list, select the Active Directory Trusted Domains AAA Server you created using the guidance in the table. Note the **Server** list must be set to **None** in order to select the Trusted Domain.
 - 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 you created.
 - 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 on the next page, your VPE should look similar to the following.

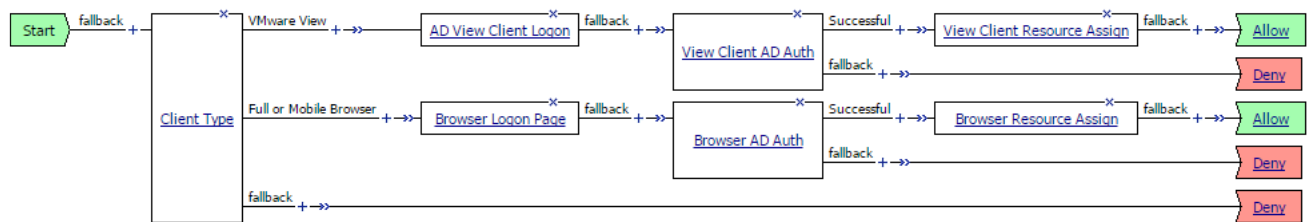


The following steps are all optional

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. If you are using multiple Active Directory domains only: In #4, from the **Type** list, choose **select**. In the **Port Variable Name** and **Session Variable Name** fields, type domain. In the **Values** field, type each AD domain followed by a space. In the Customization area, in the **Logon Page Input Field #4** field, type **Domain**.
 - d. Click **Save**.
 - e. Click the + symbol on the fallback path between **Logon page** and **Deny**.
 - Note:** Do NOT create this object if using multiple Active Directory domains.
 - 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**.
 - f. 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. The next step depends on whether you are using a single AD domain or multiple AD domains (v11.5+ only)
 - If you are using a single AD implementation:* From the **Server** list, select the Active Directory AAA server you created using the guidance in the table.
 - If you are using multiple AD domains (v11.5+):* From the **Cross Domain Support** list, select **Enabled**. From the **Trusted Domains** list, select the Active Directory Trusted Domains AAA Server you created using the guidance in the table. Note the **Server** list must be set to **None** in order to select the Trusted Domain.
 - iv. Click **Save**.
 - g. 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**.
- h. On the fallback path between **Advanced Resource Assign** and **Deny**, click the **Deny** box link, click **Allow**, and then click **Save**.

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



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: RADIUS 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 *RADIUS View Client Logon*.
 - c. From the **VMware View Logon Screen** list, select **RADIUS**.
 - d. In the **Disclaimer message** box, you can type a message you want presented to View users during RADIUS logon.
 - e. Click **Save**.
 - f. (Optional: RADIUS 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 **RADIUS Password**.
 - k. Click **Save**.

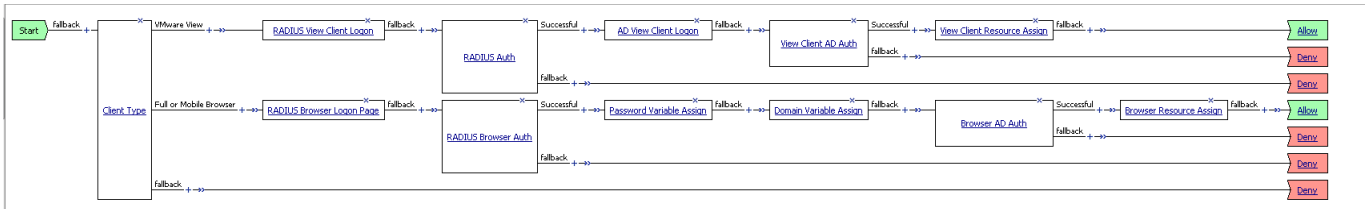
11. (Optional: RSA SecurID two-factor authentication logon page) Click the + symbol between **View Client Disclaimer** (or **Client Type** if you did not create the disclaimer message) and **VMware View Logon Page**.
 - a. On the Logon tab, click **VMware View Logon Page** option button, and then click **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**.

12. (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**.

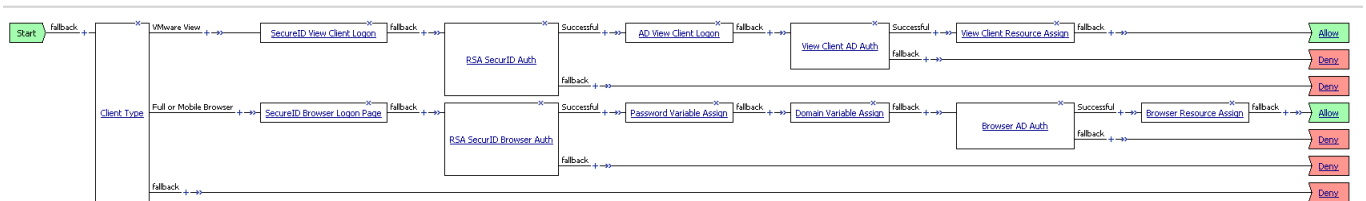
13. (Optional: If using a translation device between the View Clients and the BIG-IP system) Click the + symbol between **AD Auth** and **Advanced Resource Assign**.
 - a. Click the Assignment Tab and select Variable Assign option button, and then click **Add item**.
 - b. In the **Name** field, type 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**.

The following is an example VPE with RADIUS two-factor authentication and HTML5 support:



The following is an example VPE with SecurID two-factor authentication and HTML5 support:



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.

Health Monitors (<i>Local Traffic > Monitors</i>)		
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-default²	
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
Pools (<i>Local Traffic > Pools</i>)		
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 Requirement¹	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 (<i>Local Traffic > Profiles</i>)		
HTTP (<i>Profiles-->Services</i>)	Name	Type a unique name
	Parent Profile	http
TCP WAN (<i>Profiles-->Protocol</i>)	Name	Type a unique name
	Parent Profile	tcp-wan-optimized
TCP LAN (<i>Profiles-->Protocol</i>)	Name	Type a unique name
	Parent Profile	tcp-lan-optimized

Profiles continued (Local Traffic > Profiles)		
UDP (Profiles-->Protocol)	Name Parent Profile	Type a unique name UDP
Persistence (Profiles-->Persistence)	Name Persistence Type Match Across Services Mirror Persistence	Type a unique name Source Address Affinity Check this box If using a redundant pair of BIG-IP devices, check this box
Client SSL (Profiles-->SSL)	Name Parent Profile Certificate Key	Type a unique name clientssl Select the Certificate you imported Select the Key you imported
Server SSL (Profiles-->SSL)	Name Parent Profile Certificate and key	Type a unique name serverssl Default or imported certificate and key
Virtual Servers (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	
Secure Address Translation²	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	
Secure Address Translation²	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	
Protocol Profile (client)¹	Select the UDP profile you created above	
Secure Address Translation²	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	

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.

Virtual Servers continued (*Local Traffic > Virtual Servers*)

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
Secure Address Translation²	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.

Manually configuring the BIG-IP Advanced Firewall Module to secure your View deployment

This section describes how to manually configure BIG-IP AFM, F5's Network Firewall module, to secure your View deployment. BIG-IP AFM is particularly useful if you want to only allow access from specific clients or networks. Because this configuration can be complex, we recommend using the iApp template in version 11.6 and later to configure BIG-IP AFM.

Network Firewall settings

When configuring the BIG-IP Advanced Firewall Manager, you may want to configure your BIG-IP system to drop all traffic that you have not specifically allowed with firewall rules. This is known as **firewall mode**. By default, your BIG-IP system is set to default-accept, or **ADC mode**. Instructions for configuring your BIG-IP system, and the implications to consider, can be found on AskF5. For example, for BIG-IP v11.5: <http://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-11-5-0/1.html>

If you have licensed IP Intelligence on the BIG-IP system, you can prohibit connections from sources with low reputation scores.

The following instructions cover a basic firewall configuration that is effective for the most common scenario of wanting to allow connections from a single trusted network. If you have complex requirements, such as the need to schedule different policies for different times of the day, or you want to create complicated rule or address lists, consult the BIG-IP AFM documentation. The basic steps for Policy and Rule creation apply to all scenarios.

To configure the BIG-IP AFM to allow connections from a single trusted network

1. Create the Network Firewall Policies:
 - a. From the Configuration utility, click **Security > Network Firewall > Policies**, and then click **Create**.
 - b. In the **Name** field, type a unique name for the policy, such as **View-Policy**.
 - c. Click **Finished**.
2. Create a rule to allow authorized hosts or networks to connect:
 - a. Click **Security > Network Firewall > Policies**.
 - b. Click the name of the policy you just created.
 - c. In the Rule section (below the General Properties section), click the **Add** button.
 - d. Leave the **Type** list set to Rule.
 - e. From the **Order** list, select **First**. The Order list only appears in version 11.5 and later. In 11.4.x, you must reorder the rules from the Policy General Properties page.
 - f. In the **Name** field, type a unique name, for instance **View-traffic-Allowed**.
 - g. Ensure the **State** list is set to **Enabled**.
 - h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.
 - i. In the **Source** section, from the **Address/Region** list, select **Specify**.
You are now able to list the trusted source addresses for your connection.
In the following example, we will configure a single subnet as trusted.
 - Select **Address**.
 - In the box, type the network address you want to allow, including netmask if more than a single host. Specify a network using CIDR notation, such as **10.0.0.0/24**.
 - Do not configure a source port.
 - Optional: If you want to limit inbound connections to a specific VLAN or Tunnel, from the **VLAN / Tunnel** list, select **Specify**, and then move the VLANs or tunnels that are allowed access to the Selected box.
 - Click **Add**.
 - Repeat these steps for additional hosts or networks. Use **Address List** or **Address Range** when appropriate.
 - j. In the **Destination** section, leave the **Address/Region** and **Port** set to **Any**. Because you will be applying your policy to a virtual server that listens only on a single desired address and port, do not specify that information here.

- k. If necessary, from the **Action** list, select **Accept**.
- l. *Optional:* If you have configured a logging profile and want to log connections, from the **Logging** list, select **Enabled**. Typically, allowed connections do not need to be logged.
- m. Click **Repeat**.
- n. Return to step "c" and repeat this entire procedure for UDP (in step "h" select **UDP** from the **Protocol** list and leave **17**).
- o. Click **Finished**. You should now see two rules in your policy.

3. Creating a firewall rule to block all other traffic

The next task is to create a firewall rule to block all other traffic that you have not allowed. Although this is not a required step if your BIG-IP system is set to default deny (**Firewall mode**), it is required in default-accept (**ADC mode**), and is a good practice to always configure such a rule.

- a. Click **Security > Network Firewall > Policies**.
- b. Click the name of the policy you created in step 1.
- c. In the Rule section (below the General Properties section), click the **Add** button.
- d. Leave the **Type** list set to **Rule**.
- e. Leave the **Order** list, select **Last**.
- f. In the **Name** field, type a unique name, for example **View-traffic-Prohibited**.
- g. Ensure the **State** list is set to **Enabled**.
- h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.
- i. In the **Source** section, leave all the lists set to **Any**.
- j. From the **Action** list, select either **Drop** (to silently discard incoming connections) or **Reject** (to send a Destination Unreachable message to the sender).
- k. If you configured a logging profile as described in *Optional: Configuring the BIG-IP system to log network firewall events on page 52*, from the **Logging** list, select **Enabled**.
- l. Click **Repeat**.
- m. Return to step "c" and repeat this entire procedure for UDP (in step "h" select **UDP** from the **Protocol** list and leave **17**).
- n. Click **Finished**. You return to the Policy Properties page.
- o. On the Policy Properties page, in the Rules section, ensure the rules with the Action of Accept come before the Drop or Reject rules you just created. If they do not, use the **Reorder** button and drag the rules into the correct order.

4. Apply Your Firewall Policy to your Virtual Server

- a. Click **Security > Network Firewall > Active Rules**.
- b. In the Rule section (below the General Properties section), click the **Add** button.
- c. From the **Context** list, select **Virtual Server**, and then select the appropriate View virtual server(s).
 - If you are deploying BIG-IP APM, this is the TCP virtual server on port 443 (and port 80 if you configured the redirect virtual server), and the UDP virtual server on port 4172.
 - If you are not deploying APM, this is the TCP virtual servers on port 443 (and port 80 if you configured the redirect virtual server), 4172 (if you configured PCoIP support), and 8443 (if you configured HTML5 support), and the UDP virtual server on 4172 (if you configured PCoIP support).
- d. From the **Type** list, select **Policy**, and then select the firewall policy you created.
- e. From the **Policy Type** list, select **Enforced**.
- f. Click **Finished**.

Optional: Assigning an IP Intelligence Policy to your View virtual server(s)

If you want to restrict access to your View virtual server based on the reputation of the remote sender, you can enable and assign an IP Intelligence policy. This requires an IP intelligence license; contact your F5 Sales representative for more information.

It is outside the scope of this document to provide instructions on configuring an IP Intelligence Policy. Full documentation on enabling and configuring the IP Intelligence feature can be found on AskF5. For example, the manual for BIG-IP AFM v11.5 is: <https://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-11-5-0/5.html>

After you have enabled and configured an IP Intelligence policy, use the following procedure to assign the policy to your View virtual server:

To assign the IP intelligence policy to the View virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your View port 443 virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **IP Intelligence**, select **Enabled**, then select the IP intelligence policy to apply to traffic on the virtual server.
5. Click **Update**. The list screen and the updated item are displayed. The IP Intelligence policy is applied to traffic on the virtual server.
6. Repeat this procedure for each View virtual server you configured:
 - If you are deploying BIG-IP APM, this is the TCP virtual server on port 443 (and port 80 if you configured the redirect virtual server), and the UDP virtual server on port 4172.
 - If you are not deploying APM, this is the TCP virtual servers on port 443 (and port 80 if you configured the redirect virtual server), 4172 (if you configured PCoIP support), and 8443 (if you configured HTML5 support), and the UDP virtual server on 4172 (if you configured PCoIP support).

Optional: Configuring the BIG-IP system to log network firewall events

If you are using BIG-IP AFM, you have the option of logging network firewall events to one or more remote syslog servers (recommended) or to log events locally. You can either use an iApp template to create the logging profile, or create the logging profile manually.

For specific information on logging on the BIG-IP system, see the appropriate guide for your version. For example, for 11.5.0:

- Remote High-Speed Logging:
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-5-0/22.html
- Local logging:
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-concepts-11-5-0/11.html

Creating the logging profile using the iApp template


Use this section to create the logging profile using the logging profile iApp template. If you have not already downloaded the iApp template, see <https://devcentral.f5.com/wiki/iApp.F5-Remote-Logging-iApp.ashx>.

To configure the logging profile iApp

1. Log on to the BIG-IP system.
2. On the Main tab, click **iApp > Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **logging-iapp_**.
5. From the **Template** list, select **f5.remote_logging.v<latest-version>**. The template opens
6. Use the following table for guidance on configuring the iApp template. Questions not mentioned in the table can be configured as applicable for your implementation.

Question	Your selection
Do you want to create a new pool of remote logging servers, or use an existing one?	Unless you have already created a pool on the BIG-IP system for your remote logging servers, select Create a new pool .
Which servers should be included in this pool?	Specify the IP addresses of your logging servers. Click Add to include more servers.
What port do the pool members use?	Specify the port used by your logging servers, typically 514 .
Do the pool members expect UDP or TCP connections?	TCP
Do you want to create a new monitor for this pool, or use an existing one?	Unless you have already created a health monitor for your pool of logging servers, select Use a simple ICMP (ping) monitor .
Do your log pool members require a specific log format?	If your logging servers require a specific format, select the appropriate format from the list.

- Click **Finished**.
- On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
- Click the name of your View virtual server.
- From the **Security** menu, choose **Policies**.
- Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
- Click **Update**. The list screen and the updated item are displayed.

 **Note:** The iApp template creates a log publisher and attaches it to the logging profile. If the publisher does not appear in the BIG-IP Configuration utility (GUI), you can verify the configuration by running the following command from the Traffic Management shell (tmsh): **list security log profile <your profile name>**.

Creating logging profile manually

If you do not want to use the iApp template to create a logging profile, use this section for guidance on configuring the logging profile manually. You must have access to the tmsh command line to use this method.

To manually configure a logging profile

- Use the following guidance for configuring a health monitor and load balancing pool for the logging servers.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (Local Traffic -->Monitors)	Name	Type a unique name
	Type	ICMP
	Interval	30 (recommended)
	Timeout	91 (recommended)
Pool (Local Traffic -->Pools)	Name	Type a unique name
	Health Monitor	Select the appropriate monitor you created
	Slow Ramp Time	300
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)
	Address	Type the IP Address of a server.
	Service Port	Type the appropriate port, such as UDP port 514 , the port on which logging typically occurs. Click Add , and then repeat Address and Port for all nodes

- Log into the BIG-IP system using the command line. Enter the tmsh shell, by typing **tmsh** from the prompt.
- Create a Remote High Speed Log (HSL) destination:
(tmsh)# create / sys log-config destination remote-high-speed-log [name] pool-name [specified pool] protocol [udp or tcp]
- If you have a specific log format requirement, create a format-specific log destination, and forward that to the previously-created HSL destination:
(tmsh)# create / sys log-config destination [splunk|arcsight|remote-high-speed-log] [name] forward-to [HSL name]

5. Create a log publisher:

```
(tmoss)# create / sys log-config publisher [name] destinations add { [logdestination name] }
```

6. Create the logging profile to tie everything together.

If you chose to log allowed connections, include the green text (as in step 2 substep 1 in *To configure the BIG-IP AFM to allow connections from a single trusted network on page 50*).

If you set the rule to drop incoming connections, include the text in blue.

If you chose to log IP intelligence events, include the text in red to add the parameter that sets the log publisher.

```
(tmoss)# create / security log profile [name] network add { [name] { filter { log-acl-match-accept enabled  
log-acl-match-drop enabled log-acl-match-reject enabled } format { field-list { date time action drop reason  
protocol src ip src port dest ip dest port } type field-list } publisher [logpublisher name] } } ip-  
intelligence { log-publisher [logpublisher name] }
```

Assigning the logging profile to the virtual server

The final task is to assign the logging profile to the virtual server.

To assign the logging profile to the View virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your View virtual server on port 443.
3. From the **Security** menu, choose **Policies**.
4. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
5. Click **Update**. The list screen and the updated item are displayed.
6. Repeat this procedure for each View virtual server you configured:
 - If you are deploying BIG-IP APM, this is the TCP virtual server on port 443 (and port 80 if you configured the redirect virtual server), and the UDP virtual server on port 4172.
 - If you are not deploying APM, this is the TCP virtual servers on port 443 (and port 80 if you configured the redirect virtual server), 4172 (if you configured PCoIP support), and 8443 (if you configured HTML5 support), and the UDP virtual server on 4172 (if you configured PCoIP support).

This completes the manual configuration.

Document Revision History

Version	Description	Date
1.0	<p>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):</p> <ul style="list-style-type: none"> - 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. <p>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.</p>	12-16-2014
1.1	<p>Added a new troubleshooting entry on <i>page 33</i> 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.</p>	01-28-2015
1.2	<p>Added a new entry on <i>page 33</i> concerning pool members being unavailable after deploying advanced health monitors.</p>	02-11-2015
1.3	<p>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:</p> <ul style="list-style-type: none"> - 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	<p>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.</p>	04-30-2015
1.5	<ul style="list-style-type: none"> - 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	<p>Added a new troubleshooting entry on <i>page 33</i> concerning possible issues when using APM with pre-authentication messages configured on the View Connection servers.</p>	06-22-2015
1.7	<p>Updated this guide for the fully supported iApp f5.vmware_view.v1.3.0 available on downloads.f5.com. This release contained the following:</p> <ul style="list-style-type: none"> - Added support for using multiple Active Directory domains. Note this requires 11.5 when using HTML 5 Clients or allowing browser based authentication. - Added the ability to use BIG-IP Advanced Firewall Manager (AFM). - Added a new advanced health monitor - Increased the minimum BIG-IP version to v11.4, and added support for BIG-IP v12.0 - Increased the minimum supported VMware Horizon View software version to 5.2. - Added a troubleshooting entry for users seeing a HTTP 500 error. - Added an option to support HTML 5 client connections when using LTM only. - Added the ability to create and attach an APM-specific logging profile (v12.0 and later only). - Removed the Edge client solution to help reduce confusion and eliminate unsupported View features. - Removed the virtual server to support View 5.0 USB redirection connections. 	09-11-2015
1.8	<p>Updated the note in the Product/Version table on page 1 to state BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.1.</p>	10-09-2015
1.9	<ul style="list-style-type: none"> - Modified the troubleshooting entry on <i>page 34</i> to update the Cipher string which was missing a colon (:). - Added manual configuration instructions for BIG-IP AFM - Clarified the note in <i>Modifying your Connection Servers to support HTML 5 clients</i> on <i>page 9</i> that the download instructions in steps 1 and 2 were not necessary if using View 6.0 or later, not the entire section. 	10-28-2015
2.0	<p>Updated the note in the Product/Version table on page 1 to include Horizon View 6.2. Included callouts which clarify HTML5 client support, or lack thereof.</p>	11-13-2015

Version	Description	Date
2.0	<p>Updated this guide for the fully supported iApp f5.vmare_view.v1.4.0rc1 available on downloads.f5.com. This release contained the following:</p> <ul style="list-style-type: none"> - Added support for Horizon View 6.2 - Added smart card support (2 pin prompt solution). Note there is currently no manual configuration for smart cards - Added two-factor authentication using RADIUS with Active Directory <p>Issues resolved</p> <ul style="list-style-type: none"> - Filtered out SSL keys which contain passwords. The iApp is unable to parse or retain password field in key and therefore was causing an error. Noted that to use password-protected keys, you must create a Client SSL profile outside the iApp template. - Corrected the LDAP monitor port when using LDAPS 	01-26-2016
2.1	Added the section <i>Modifying your Connection Servers to support two-pin prompt with Smart Card authentication on page 10</i>	01-28-2016
2.2	Updated the footnotes in the table <i>Products and versions tested on page 1</i>	02-04-2016
2.3	Added a new troubleshooting entry on <i>page 34</i> applications or Virtual Desktops not responding after selecting a resource.	02-18-2016
2.4	<ul style="list-style-type: none"> - Updated this guide to add f5.vmare_view.v1.4.0rc2 and rc3 on DevCentral (https://devcentral.f5.com/codeshare/vmware-horizon-view-iapp). Both these RCs only contain fixes: <ul style="list-style-type: none"> RC2: Fixed an issue in the APM RADIUS configuration where the iApp would fail when attempting to create an APM RADIUS AAA Server profile object on APM versions 11.5 and 11.6. RC3: Resolved issue when advanced monitor password field contained curly braces. - Noted the minimum version required for iApp v1.4.0 is 11.50, and for v1.3.0 is 11.4.0. 	04-01-2016

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

