Deployment Guide

Document Version: 1.7
iApp Version: 2012_06_14

What's inside:

Deploying the BIG-IP System v11 with VMware View 5.0

Welcome to the F5 and VMware® View® Deployment Guide. This document contains guidance on configuring the BIG-IP system version 11, including BIG-IP Local Traffic Manager™ (LTM) and BIG-IP Access Policy Manager™ (APM) for VMware View 5.0, resulting in a secure, fast, and highly available deployment.

The VMware 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. iApp, introduced in BIG-IP v11, is an extremely easy and accurate way to configure the BIG-IP system for VMware View 5.

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 VMware View deployments. For large VMware 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.

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

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*

Products and versions tested

Product	Version
BIG-IP LTM	v11, 11.0.1, 11.1, 11.2
VMware View	5.0[1]

[1] This iApp was written for, and has been tested extensively with, VMware View version 5. However, this View 5 iApp also works with VMware View 4.6 with no modifications.

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:

- For VMware View 5, 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 the View 5 iApp. See *Downloading and importing the VMware View 5.0 iApp from DevCentral on page 9.*
  - **Manual configuration**
    If configuring the BIG-IP system manually, after modifying the VMware Virtual Desktop Manager Global Settings, see *Appendix: Manual configuration tables on page 20*.
- This iApp was written for, and has been tested extensively with VMware View version 5. However, this View 5 iApp also works with VMware View 4.6 with no modifications.
- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- If you have an existing iApp configuration for VMware View using an earlier version of the View 5.0 iApp template, you can retarget your existing template to use this new iApp. See *Modifying an existing template configuration to use a new iApp template on page 9.*
- Because the BIG-IP system is decrypting SSL, you must have an SSL certificate and key installed on the BIG-IP LTM system. For View 5.0, the BIG-IP system re-encrypts the traffic (SSL bridging) before sending it to the View servers. View 4.6 supports SSL offload.
- This document contains guidance on Application Visibility Reporting. AVR is licensed on all systems, but you must provision AVR before starting the iApp template. If you do use AVR, we recommend creating a custom Analytics profile before beginning the iApp.

- 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.
- After completing the configuration, if you enabled BIG-IP APM in the iApp and want to delete the entire iApp configuration, you must first disable APM and then delete the iApp. See *Deleting the iApp configuration on page 16.*
- If your organization wants to provide a mechanism for users to download the View Client software through the BIG-IP APM, after running the template, be sure to see *Modifying the Access Policy to customize the links to the View Client (optional) on page 17.*

Configuration examples and traffic flows

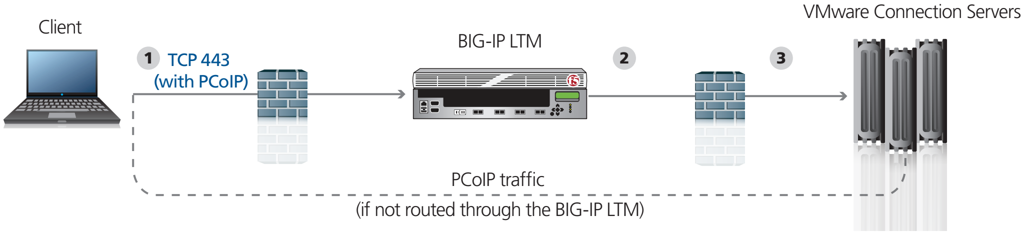
In this deployment guide, we present two modes of deploying the BIG-IP LTM with VMware View. Specifically, if View is deployed with View Security Server, the BIG-IP system can further protect, monitor, and load balance these servers, allowing PCoIP Security Gateway services to be moved out of the DMZ. If only View Connection Servers are used, the BIG-IP 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 either LTM scenario to provide pre-logon checks to the endpoint device and support a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. The BIG-IP APM can also enforce Active Directory group policies on corporate-owned and non-corporate-owned assets during the duration of the connection. Additionally, once authenticated, BIG-IP APM guarantees the encryption of all VMware View transport protocols, whether natively encrypted or not.

Traffic Flows

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

BIG-IP LTM with Connection Servers only
The following traffic flow diagram shows the BIG-IP LTM with a VMware View deployment using Connection Servers only.

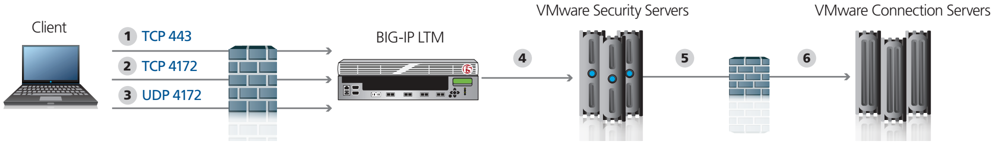

Client
1
TCP 443
(with PCoIP)
BIG-IP LTM
2
3
VMware Connection Servers
PCoIP traffic
(if not routed through the BIG-IP LTM)

For deployments without Security Servers or PCoIP protocol the traffic flow is as follows:

1. The client machine (regardless of Mac, Windows, iPad, or Zero Clients) makes a connection to the BIG-IP virtual IP address for the VMware Connection Servers. Depending on your configuration, PCoIP 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 (View 5), or offloads SSL (4.6 only) 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 Server and Connection Servers

This traffic flow diagram shows the BIG-IP LTM with a VMware View deployment using both Security Servers and Connection Servers.

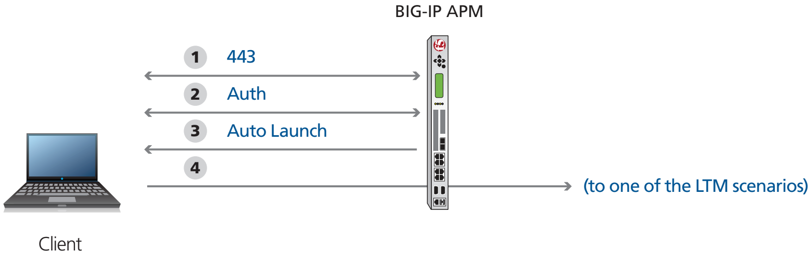


For deployments with Security Servers and PCoIP protocol the traffic flow is as follows:

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. The BIG-IP establishes a new connection to the Security Servers and proceeds with Authentication.
2. BIG-IP persists the TCP 4172 XML connection to the same Security Server.
3. Once desktop availability and entitlement are determined, PCoIP connections are persisted to the same Security Server.
4. The BIG-IP proxies the desktop PCoIP connection (UDP 4172) to Security Servers.
5. VMware Security Servers control load balancing and availability of the Connection Servers (6)

BIG-IP APM with VMware View

This traffic flow diagram shows the BIG-IP APM in front of the VMware View deployment. After the Auto Launch, traffic continues to one of the two LTM scenarios above.



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

1. The client machine launches the BIG-IP Edge Client makes a connection to the Virtual IP Address for either the VMware Connection Servers or Security Servers (depending on your configuration), residing on the BIG-IP. BIG-IP establishes a new connection to the VMware Active Directory Servers.
2. Authentication is performed directly from the BIG-IP APM. User credentials are securely cached on the BIG-IP.
3. The BIG-IP Edge client checks for the availability of the VMware View client and either downloads the client or launches it (on platforms that support BIG-IP Edge client).
4. Once the secured network tunnel is setup between the client and the BIG-IP APM, the client is automatically logged in using one of the LTM scenarios (either connecting to the Security or Connection Servers).

Preparation Worksheet

In order to use the iApp for VMware View, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages. You might find it useful to print this table and then enter the information.

➲ **Note:** *Although we show space for 5 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	SSL Decryption	Pool Members	Sync/Failover Groups*	TCP request queuing*	WAN or LAN clients
IP address you will use for the LTM virtual server: FQDN that will resolve to the virtual server address:	You must have imported a certificate and key into the BIG-IP LTM before running the template for SSL bridging or SSL offload (4.6 only). Certificate: Key:	View server IP addresses: 1: 2: 3: 4: 5: If using Connection servers only and routing PCoIP through the BIG-IP: Network on which the View Desktops reside: Subnet Mask:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to View are coming over a: LAN WAN

Access Policy Manager (APM) - Optional (you must have provisioned APM before running the template)

IP address	FQDN	Active Directory	Active Directory anonymous binding
IP address to use for Network Access:	Fully Qualified Domain Name used to Access VMware View:	Name or IP address of an Active Directory server in your domain that the BIG-IP system can contact:	Does your Active Directory Domain allow anonymous binding? If anonymous binding is not allowed, you need to supply the following: Active Directory user name with administrative privileges: Associated password: **Note:** Credentials are stored in plain text on the BIG-IP system.

Modifying the VMware Virtual Desktop Manager Global Settings

Before starting the BIG-IP LTM configuration, we modify the View configuration to allow the BIG-IP LTM to load balance View client connections.

The modifications depend on the requirements of your environment. Use the matrix on the previous page to find the best solution for your deployment, and then choose whether you will setup VMware View with Connection Servers only or Security and Connection Servers.

Modifying VMware View 5.0 if using Security Servers and Connection Servers

Use this procedure if using Security Servers and Connections Servers. In this scenario, the BIG-IP 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 5.0 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 in the main pane.
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. In our example we type: **https://192.0.2.123:443**

    d. Click **OK** to close the window

    e. Repeat these steps for each Connection Server.

Important

If the View Client is not using Network Access through the BIG-IP APM and has a routable path to the View Connection Servers directly, the PCoIP option must be selected/enabled.

4. For each View Security Server, perform the following:
    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

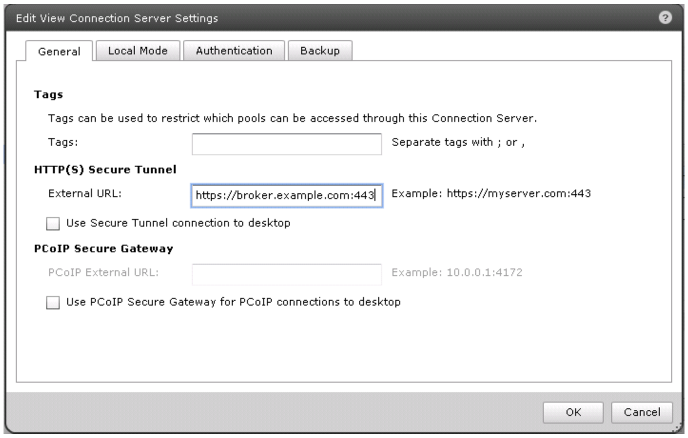
    f. Repeat these steps for each Security Server.

Modifying the VMware View 4.6 if using Connection Servers only

Use this procedure only if using View 4.6, and using the Connection Servers and not Security Servers. If you are using View 4.6, this allows the BIG-IP to terminate SSL transactions. In the following procedures, we disable the SSL requirement for client connections in the Virtual Desktop Manager administrator tool and modify the External URL to point to the virtual IP address on the BIG-IP LTM. This allows VMware to correctly direct connections to the BIG-IP LTM.

To modify the VMware configuration for View 4.6 without 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 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, in the HTTP(S) Secure Tunnel **External URL** box, type the DNS name or IP address you will associate with the BIG-IP LTM virtual IP address for the Connection servers, followed by a colon and the port. In our example we type: **https://broker.example.com:443**
   d. Click to clear the **Use Secure tunnel connection to desktop** box, if checked.
   e. Click **OK** to close the window
   f. Repeat these steps for each Connection Server.



Tags

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

Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel

External URL: https://broker.example.com:443 Example: https://myserver.com:443

□ Use Secure Tunnel connection to desktop

PCoIP Secure Gateway

PCoIP External URL: Example: 10.0.0.1:4172

□ Use PCoIP Secure Gateway for PCoIP connections to desktop

Configuring DNS and NTP settings on the BIG-IP system

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

Configuring the DNS settings

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

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

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

To configure DNS settings

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

Configuring the NTP settings

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

To configure NTP settings

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

Downloading and importing the VMware View 5.0 iApp from DevCentral

The first task is to download the iApp for VMware View 5.0 from DevCentral and import it onto the BIG-IP system. Ensure you download the file with the latest date in the file name.

To download and import the iApp from DevCentral

1. Open a web browser and go to *http://devcentral.f5.com/wiki/iApp.VMware-View-5-iApp-Template.ashx*
2. Download the **vmware_view_5<latest date>.zip** file to a location accessible from your BIG-IP system.
   Important → *You must download the file, and not copy and paste the contents. F5 has discovered the copy paste operation does not work reliably.*
3. Extract (unzip) the **vmware_view_5<latest date>.tmpl** file.
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. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

If you are configuring the BIG-IP system manually, see *Appendix: Manual configuration tables on page 20.*

Modifying an existing template configuration to use a new iApp template

If you have an existing Application Service for VMware View from an older version of the iApp template, you can retarget the Application Service to use this new iApp template.

To retarget an existing Application Service to use a new iApp template

1. On the Main tab, expand **iApp**, and then click **Application Services**.
2. From the list, click the name of your existing View 5.0 Application Service.
3. On the Menu bar, click **Reconfigure**.
4. In the **Template** row at the top of the page, click the **Change** button, and then select the latest version of the View 5 iApp template from the list. Keep in mind the following:
   - Some questions appear in a different order and subsequently return to default values, make sure you read through the entire iApp and select appropriate values.
     Examples questions include:
     Will PCoIP connections be routed through the BIG-IP system?
     Will PCoIP connections be proxied by the View Servers?
     How should the BIG-IP system handle encrypted application traffic?
   - Some scenarios require additional information. Examples include:
     What is the IP Address of the DNS server used for remote client lookups? (New question when using APM)
     PCoIP Questions section and questions appear when you select to route PCoIP connections through the BIG-IP system is selected
5. When you have finished making modifications, click the **Finished** button. Use this deployment guide and the online help for more information on specific questions.

Configuring the BIG-IP iApp for VMware View 5.0

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

Note →

Before beginning the iApp template, we strongly recommend you set the ***Idle Timeout 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**.

Getting Started with the iApp for VMware View

To begin the VMware 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_5_<latest date>**.
   Note that some versions of the iApp may contain a date at the end of the name. If applicable, choose the iApp with the latest date. The VMware View 5.0 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. **Configure Sync/Failover?**
   If you want to configure the Application for Sync or failover groups, select **Yes** from the list.
   a. **Device Group**
      If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.
   b. **Traffic Group**
      If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group.

Analytics

ⓘ **Tip**
If using AVR, create a new Analytics profile before beginning the iApp for more specific reporting

This section of the template asks questions about Analytics. The Application Visibility Reporting (AVR) is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear in the iApp. The AVR module allows you to view statistics specific to your VMware View implementation. Note that this section is for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile before beginning the template. 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.

1. **Enable Analytics**
   Choose whether you want to enable AVR for Analytics.

2. **Analytics Profile**
   You must decide whether to use the default Analytics profile, or create a new one. As mentioned previously, we recommend creating a new profile to get the most flexibility and functionality out of AVR. If you choose to create a new profile after starting the template, you must exit the template, create the profile, and then restart the template.

   To use the default Analytics profile, choose Use **Default Profile** from the list.

   To choose a custom profile, leave the list set to **Select a Custom Profile**, and then from the Analytics profile list, select the custom profile you created.

General Questions

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

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

   Select whether PCoIP connections are routed through the BIG-IP system.

   a. **No**
      If you answer that PCoIP connections are not routed through the BIG-IP system, you must have a route between the clients and the Virtual Desktop. If you do not have a route between the clients and the virtual desktops, you must either select Yes, or create a route before the configuration produced by the iApp will work properly.
      If you select No, continue with the following section; no further information is needed.

   b. **Yes**
      If you answer Yes, an additional question appears:

      Will PCoIP connections be proxied by the View Servers?

      - ***Yes***
        If you select Yes, the iApp does not create forwarding virtual servers. The BIG-IP system directs all PCoIP traffic back to the View Servers. You ***must*** enable the **Use Secure Tunnel for PCoIP** option on the View servers for this option to function properly.

      - ***No***
        If you select No, the iApp 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. You must provide additional information in *PCoIP Questions on page 12.*

2. **Deploying APM?**
   Select whether you want to deploy APM at this time. You must have APM licensed and provisioned on your BIG-IP system for this section to appear.

   The BIG-IP APM can provide pre-logon checks to the endpoint device and support a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. See *Configuration examples and traffic flows on page 3* or *http://www.f5.com/products/big-ip/access-policy-manager.html* for more information on BIG-IP APM.

PCoIP Questions

This section only appears if you selected that PCoIP connections are routed through the BIG-IP system and that PCoIP connections are not proxied by the View servers. If you do not see this section, continue with Web Traffic Questions.

The BIG-IP system uses the answers provided in this section to create a route between the client and the Virtual Desktops on port 4172 only.

1. **Network of the Virtual Desktops**
   Type the network on which the Virtual Desktops reside. For example, 192.0.2.0.
2. **Associated Network Mask**
   Type the subnet mask associated with the network of the Virtual Desktops.
3. **Specify VLANs**
   You can specify specific VLANs on which this virtual server should listen, or choose all VLANs. If you select to enable or disable on specific VLANs, move the appropriate VLAN from the **Options** box to the **Selected** box.

Web Traffic

This section of the template asks questions about the way you want to handle encryption in your environment. The questions in this section are different depending on your answers in the General Question section.

1. **How should the BIG-IP system handle encrypted application traffic?**
   Choose one of the following options:

   a. *There will be no encrypted traffic (**View 4.6 only**)*
   If you select this option, your clients will connect on port 80.
   You must disable **Require SSL for client connections and View Administrator** in the Global Settings of View Server.

   b. *SSL Offload (**View 4.6 only**)*
   If you select this option, your clients will connect on port 443, but the View servers will not be listening on port 443.
   If you select this option, you are asked for the certificate and key you want to use. Select the appropriate certificate and key from the list.

   c. *SSL Bridging* (***You must select this option for View 5.0***)
   If you select this option, your clients will connect on port 443, and the servers will also listen on port 443, providing full encryption for the traffic. You must manage and maintain certificates on both the servers and the BIG-IP system.

   If you select this option, the template asks for the certificate and key you want to use. Select the appropriate certificate and key from the list.

Virtual Server

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

1. **IP address for the virtual server**
   This is the IP address for the BIG-IP LTM virtual server. If you are not using BIG-IP APM, this is the address clients use to access VMware View. If you are using BIG-IP APM, this is the IP address the APM uses for sending traffic to the BIG-IP LTM and then to the View Servers.
2. **FQDN**
   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.
3. **Route back to application or secure network address translation**
   If the View 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, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #4) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new address as the destination address when responding to traffic originating through the BIG-IP.
   If you indicate the View servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the View servers.
   We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

   If you are configuring your BIG-IP LTM in a "one-armed" configuration with your View servers -- where the BIG-IP virtual server(s) and the View servers have IP addresses on the same subnet – you must choose No.
4. **More than 64,000 simultaneous connections**
   If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #5.

   If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.
5. **NTLM**
   Some organizations may have single sign-on solutions deployed in front of VMware View which may be using NTLM authentication. While this is not typical, if your organization is using NTLM authentication in front of your View deployment, you must answer Yes to this question.

   If you are not using NTLM with View, leave the list set to No.
6. **WAN or LAN**
   Specify whether most clients are connecting over a WAN or LAN. Your answer determines the type of optimized TCP profile the LTM system uses.

Server Pool

In this section, you add the View servers and configure the pool.

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

2. **Address/Port**
   Type the IP address and Secure Port (443 is the default) for each View Server that is a part of this implementation. Click **Add** to include additional servers to the pool.

3. **TCP Request Queuing**
   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 in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on Ask F5.

   Important

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

   If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.

   a. Type a queue length in the box. We do not recommend 0 for unlimited.

   b. Type a number of milliseconds for the timeout value.

4. **Health Monitor Interval**
   Specifies how often the system checks the health of the servers. We recommend the default of 30 seconds.

5. **HTTP Request**
   You can configure the template to retrieve a specific page by typing the path here. We recommend the default.

6. **Monitor response string**
   Required: This is where you enter the expected response from the HTTP request. In our example above, our response string is **VMware.*View Portal**. If you have a custom page, type a text string from that page here.

   Important

   *If you modify the default HTTP request (GET /) or the response (VMware.*View Portal), you must enter valid strings or the View servers will be marked as unavailable. Response changes based on the version of View server being used; wildcard .*is used in this iApp to catch these variations.*

Access Policy Manager

If you specified you are deploying the BIG-IP Access Policy Manager (APM), in this section you configure the APM options. If you did not specify APM, this section does not appear.

1. **IP address**
   Type the IP address clients will use for access into the network. This will be the address of the BIG-IP APM virtual server.

2. **SSL Certificate**
   Select the Certificate that will be used to authenticate access to the Network Access (VPN) virtual server.

3. **Key**
   Select the associated key.

4. **Path to View Client**
   Type the full path to the View Client. The default path is
   C:\Program Files\VMware\VMware View\Client\bin\wswc.exe
   If you have a different path to the View Client, make sure to use the same format as the default.

Important → *Auto-Launch only works in Microsoft Windows environments.*

5. **IP Address Range Start**
   The BIG-IP APM needs unallocated IP addresses to assign to each client connecting through the APM for the lease pool.
   In this example, we are using a range of IP addresses for the APM to use for View clients. Type the start of the IP address range. In our example, we type 10.133.84.20.
6. **IP Address Range Finish**
   Type the end of the IP address range. In our example, we type 10.133.84.23.
7. **IP Address of the DNS Server**
   Specify the IP address of the DNS server used for remote client lookups. This is necessary as a part of the Network Access resource created by APM for access.
8. **Add a secondary DNS Server**
   You can optionally add a secondary DNS server used for remote client lookups. If you select Yes, type the IP address of this second DNS server.
9. **Anti-virus software check**
   If you want the BIG-IP APM to perform a check to ensure that a valid Virus Scanner is installed on the host before they are allowed to connect, select **Yes** from the list.
10. **Location of View Client for download**
    If you want to provide a mechanism for users to download the View Client, select **https://** or **http://** from the list, and then type the IP address or FQDN of a web server that is hosting your VMware View Client software. After completing the iApp, see *Modifying the Access Policy to customize the links to the View Client (optional) on page 17.*

    If you do not want to provide a way for users to download the View Client through the APM, we suggest creating a web page that would contain further instructions on how users can acquire the View Client. ***This field is currently required, so you must type an IP address or FQDN here***. If you do not want to send users to a web page, after completing the iApp, see *Removing the option for providing the View Client on page 18.*

APM Authentication

In this section of the template, you answer the Active Directory Auth questions.

1. **Active Directory address**
   Type the IP Address of the Active Directory server for user credential authentication. The Active Directory must be accessible by the BIG-IP in order to successfully authenticate users.

   The value of this field can also be a Virtual Server address containing multiple Active Directory servers if high availability is required.
2. **Active Directory FQDN**
   Type the host name of the Active Directory server used for user authentication. This is the host name that resolves to the IP address in the previous question.
3. **NETBIOS domain name**
   Type the NETBIOS domain name for your Active Directory environment.

4. **Active Directory Anonymous Binding**
   If your Active Directory deployment supports anonymous binding, leave the list set to Anonymous binding is allowed.

   If anonymous binding is not allowed, select Credentials are required for binding. Two new rows appear asking for a user name and password.
   Note that after submitting the template, the user name and password are stored in plain text on the BIG-IP.

   » *Active Directory user name*
   Type a user name with administrative permissions.

   » *Password*
   Type the associated password.

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

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

If you did not configure the iApp to use APM by answering No to question #2 in *General Questions on page 11*, you can simply delete the iApp configuration from the Application Services Properties page by clicking **Delete**.

If you answered Yes to enable APM on question #2 in *General Questions on page 11*, to completely delete the iApp configuration you must first re-enter the template and disable APM.

To delete the iApp configuration if you enabled APM

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. In the General Questions section, select **No** from the question asking about enabling APM.
5. Click **Finished**. You return to the Application Services Properties page.
6. Click the **Delete** button to delete the iApp configuration.

Note →

Modifying the Access Policy to customize the links to the View Client (optional)

If you are providing a location where the View Client software is hosted (as described in #10 on *page 15*), you can use the procedures in this section to customize the links presented to the end users.

If you do not want to provide the View Client, see *Removing the option for providing the View Client on page 18.*

Modifying the Decision Box produced by the iApp

By default, if the APM does not detect the View Client, the users are presented two options, a green option called "Option 1" which points to the external web server where you host the View Client for download, and a red option called "Option 2", which logs the user off. In this section, we modify the text to make the options more clear for the end user.

To modify the decision box

1. On the Main tab, expand **Access Policy**, and then click **Customization**.
2. Ensure the **Language** list on the far right is set to the proper language.
3. In the Left navigation pane, click the **Localization** tab.
4. Click the **+** symbol to expand **Access Profiles**.
5. Click the **+** symbol to expand the Access Profile created by the iApp. This has the name you gave the Application service, followed by **_apm_access**.
6. Click the **+** symbol to expand **Access Policy**.
7. Click the **+** symbol to expand **Decision Pages**.
8. Click the **+** symbol to expand **Decision Box**.
9. Click **General**.
10. In the **Value** box for **Option 1**, delete the words "Option 1", type the appropriate text, and then press **Enter**. In our example, we type **Download the View Client** and then press **Enter**.
    Important: You must press Enter after typing the value.
11. In the **Value** box for **Option 2**, delete the words "Option 2", type the appropriate text, and then press **Enter**. In our example, we type **Log off** and then press Enter. You must press Enter.
12. On the Menu bar, click **Save**.
13. In the upper left corner of the screen, near the F5 logo, click **Apply Access Policy**.

Modifying the Webtop Link produced by the iApp

In this procedure, we modify the Webtop Link to the View Client software download. By default, the iApp uses the path to the file as the download link. Using this procedure, you can make the link more intuitive by changing the link to read "Download the View Client" or another option of your choosing.

To modify the Webtop Link

1. On the Main tab, expand **Access Policy**, and then click **Customization**.
2. Ensure the **Language** list on the far right is set to the proper language.
3. In the Left navigation pane, click the **Localization** tab.
4. Click the **+** symbol to expand **Webtop Links**.
5. Click the Webtop Link created by the iApp. This has the name you gave the Application service, followed by **_apmDownloadLink**.
6. Click **Caption** (or anywhere in the Caption row).
7. In the **Value** box, type the text you want users to click to access the location of the View Client software, and then press **Enter**. In our example, we type **Download the View Client**.
   Important: You must press Enter after typing the value.
8. On the Menu bar, click **Save**.
9. In the upper left corner of the screen, near the F5 logo, click **Apply Access Policy**.

This completes the customizations.

Removing the option for providing the View Client

If you do not want to provide a way to download the View Client through the BIG-IP APM, and do not want to provide a link to a web page with further instructions (as described in #10 on *page 15*), you can modify the configuration produced by the iApp to remove the option for download altogether. This requires removing the option from the Decision box, and then modifying the Webtop Link display value.

Important → *The following procedure requires that you disable Strict Updates on the iApp. If after making the following changes, you re-enter the iApp to reconfigure the settings, these changes will be overwritten and you will need to perform the following procedure again.*

To remove the download option from the Decision box produced by the iApp

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. From the **Application Service** list, select **Advanced**.
4. In the **Strict Updates** row, clear the checkbox to disable Strict Updates.
5. Click **Update**.
6. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
7. Locate the Access Profile created by the iApp (prefaced by the Name you gave the iApp, followed by **_apm_access**), and then, in the **Access Policy** column, click **Edit**.
   The VPE opens in a new window.
8. Click the **Decision Box** link. The Decision Box Properties page opens.
9. From the **Field 1 image** list, select **None**. You are now finished with the modifications.
10. Click **Save**.

This completes the modifications.

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.

Appendix: Manual configuration tables

We strongly recommend using the iApp template to configure the BIG-IP system for VMware View. Users familiar with the BIG-IP can use 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.

Note:
For specific instructions on configuring individual objects, see the online help or product manuals.

Connection Servers (not necessary if using Security Servers)

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTPS** (Use **HTTP** only if using View 4.6 and offloading SSL)	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Send String	**GET /**	
	Receive String	**VMware.*View Portal**	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Load Balancing Method	Choose your preferred load balancing method	
	Address	Type the IP Address of the Connection Server nodes	
	Service Port	**443** (Use **80** only if using View 4.6 and offloading SSL) Repeat Address and Service Port for all nodes	
iRule	See *Creating the Universal Inspection Engine persistence iRule on page 21*		
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Redirect Rewrite[3]	**Matching[2]**
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	Web Acceleration (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**optimized-caching**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Persistence (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Universal**
		iRule	Select the iRule you created above
	OneConnect (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
	Client SSL (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select your Certificate and key
	Server SSL[3] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**

This table continues on the following page

[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 using View 4.6 and offloading SSL.

Configuration table, continued

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)k	***Redirect virtual server***[2]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	iRule	Enable the built-in **_sys_https_redirect** iRule.
	Main virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	OneConnect Profile	Select the OneConnect profile you created above
	HTTP Profile	Select the HTTP profile you created above
	HTTP Compression Profile	Select the HTTP profile you created above
	WAN Optimization Profile	Select the HTTP profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SSL Profile (Server)[3]	**serverssl**[3]
	SNAT Pool	**Automap** (optional; see *SNAT Pools on page 22*)
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Universal Persistence profile you created above
	Forwarding virtual server - TCP (For PCoIP traffic routed through the BIG-IP LTM)	
	Name	Type a unique name.
	Destination	**Type**: Network **Address**: Type the appropriate address **Mask**: Type the associated subnet Mask.
	Service Port	**4172**
	Protocol	**TCP**
	SNAT Pool	**Automap** (optional; see *SNAT Pools on page 22*)
	Forwarding virtual server - UDP (For PCoIP traffic routed through the BIG-IP LTM)	
	Name	Type a unique name.
	Destination	**Type**: Network **Address**: Type the appropriate address **Mask**: Type the associated subnet Mask.
	Service Port	**4172**
	Protocol	**UDP**
	SNAT Pool	**Automap** (optional; see *SNAT Pools on page 22*)

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

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

[3] You do not need the Server SSL profile if using View 4.6 and offloading SSL.

Creating the Universal Inspection Engine persistence iRule

Using the following iRule, the BIG-IP LTM is able to direct traffic with greater precision resulting in a more uniform load distribution on the Connection Servers. Using the Universal Inspection Engine (UIE), the iRule looks for session information so that the BIG-IP LTM can persist the connections to the proper nodes. The View Clients first use the session information in a cookie, and then use it as an URI argument when the tunnel is opened. The first response from the server contains a

JSESSIONID cookie. The iRule enters that session ID into the connection table and upon further client requests looks for the information in a cookie or in the URI.

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

To create the persistence iRule

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

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

5. Click the **Finished** button.

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 Automap 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 exceptionally large, specifically more than 64,000 simultaneous connections, a SNAT Pool must be configured, with a SNAT address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

This completes the Connection Server LTM configuration.

Configuration for View 5.0 with Security Server

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

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

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors *(Main tab-->Local Traffic -->Monitors)*	***TCP***	Name	Type a unique name
		Type	**TCP**
		Alias Service Port[1]	**4172**
	HTTPS	Name	Type a unique name
		Type	**HTTPS**
		Alias Service Port[1]	**443**
		Send String	**GET /**
		Receive String	**VMware.*View Portal**[2]
	UDP	Name	Type a unique name
		Type	**UDP**
		Alias Service Port[1]	**4172**
Pool *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name	
	Health Monitors	Select each of the monitors you created above	
	Availability Requirement[1]	**All**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the Security Server nodes	
	Service Port	**0** (repeat Address and Service Port for all nodes)	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***HTTP*** *(Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
	TCP WAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	UDP *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**UDP**
	Persistence *(Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Match Across Virtual Servers	Click a check in the box
	Client SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate	Select the Certificate you imported
		Key	Select the Key you imported
	Server SSL *(Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
		Certificate and key	Default or imported certificate & key

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

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

This table continues on the following page

Configuration table, continued

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**TCP**	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**4172**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	SNAT Pool [2]	**Automap** (optional; see footnote [2])
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Source Address Persistence profile you created above
	HTTPS	
	Name	Type a unique name.
	Address	Type the same IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	SSL Profile (client)	Select the Client SSL profile you created above
	SSL Profile (server)	Select the Server SSL profile you created above
	SNAT Pool [2]	**Automap** (optional; see footnote [2])
	Default Pool	Select the 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
	SNAT Pool [2]	**Automap** (optional; see footnote [2])
	Default Pool	Select the 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 Automap 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 64,000 simultaneous connections, a SNAT Pool must be configured. See the BIG-IP documentation on configuring SNAT Pools.

This completes the Security Server configuration for BIG-IP LTM.

Configuring the BIG-IP APM for VMware View 5.0

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

BIG-IP Object	Non-default settings/Notes	
DNS and NTP	See *Configuring DNS and NTP settings on the BIG-IP system on page 8* for instructions.	
AAA Servers (*Main tab-->Access Policy -->AAA Servers*)	***Name***	Type a unique name
	Type	**Active Directory**
	Domain Controller	Type the IP address of the Domain controller
	Domain Name	Type the Windows Fully Qualified Domain Name (FQDN)
	Admin Name/Password	If required, type the Admin name and Password
Network Access (*Main tab-->Access Policy -->Network Access*)	***Name***	Type a unique name
	Caption	Type a caption. By default, the system uses the name you typed. Click **Finished**, but stay on this page to configure DNS/Hosts.
- **Network Access DNS/Hosts** (*Access Policy-->Network Access-->*DNS/Hosts)	***Primary Name Server***	Type the IP address of your Active Directory server.
	DNS Default Domain Suffix	Type the default Domain suffix. We type **localhost**.
Lease Pools (*Main tab-->Access Policy -->Network Access--> Lease Pools*)	***Name***	Type a unique name
	Member List: Type	Click **IP Address** or **IP Address Range** as applicable
	Member List: IP address	Type the applicable IP address. If you selected IP Address Range, type a start and end IP address.
Connectivity Profile (*Main tab-->Access Policy -->Secure Connectivity)*	***Name***	Type a unique name
	Parent Profile	**Connectivity**
Web Application (*Main tab-->Access Policy -->Web Applications*)	***Name***	Type a unique name. We use **DownloadViewClient**
	Patching	Type: **MInimal Patching**. Click **Scheme Patching** box. Click **Create**. Stay on Web Application page to add Resource item.
- **Resource Items** (*Web Application page-->Resource Items section-->Add)*	***Destination***	Click **IP Address** option button. Type the IP address of the LTM virtual server you created for the Connection Servers.
	Port	Type **443**
	Scheme	Select **HTTPS**
	Paths	Type **/***
	Compression	Select **GZIP** ***All other settings at the defaults***
Webtop (*Main tab--> Access Policy-->Webtops*)	***Name***	Type a unique name.
	Type	**Full**
Webtop Link (*Main tab-->Access Policy-->Webtop Links*)	***Name***	Type a unique name.
	Application URI	Type the IP address or FQDN of the LTM virtual server you created for the Connection Servers or Security Servers.
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name.
	Type	If using Security Servers, select **HTTPS** If using Connection Servers and no SSL offload, select **HTTPS** If using Connection Servers and offloading SSL, select **HTTP**.
	Interval	Type an Interval. We recommend **30**.
	Timeout	Type a Timeout. We recommend **91**.
	Send String	**GET /**
	Receive String	**VMware.*View Portal**[1]

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

This table continues on the following page

BIG-IP Object	Non-default settings/Notes		
Pools (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the health monitor you created above	
	Load Balancing Method	Choose **Least Connections (Member)**	
	Address	Type the IP address of BIG-IP LTM virtual server you created	
	Service Port	If using Security Servers, select **HTTPS** If using Connection Servers and no SSL offload, select **HTTPS** If using Connection Servers and offloading SSL, select **HTTP**	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Rewrite*** (*Profiles-->Services)*	Name	Type a unique name
		Client Caching Type	Must be set to **CSS and Java Script**
	HTTP (*Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**http**
	HTTP Compression (*Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
	Web Acceleration (*Profiles-->Services)*	Name	Type a unique name
		Parent Profile	**optimized-caching**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	Client SSL (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and key	Select your Certificate and Key
	Server SSL (see note on left) (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
Access Profile (*Main tab-->Access Policy -->Access Profiles*)	***Name***	Type a unique name	
	Languages	Move the appropriate language(s) to the **Accepted** box.	
Access Policy	***Edit***	Edit the Access Profile you created using the Visual Policy Editor. See *Editing the Access Policy on page 21* for details.	
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	IP Address	Type the IP address that clients will use for access.	
	Service Port	**443**	
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above	
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	HTTP Compression Profile	Select the HTTP Compression profile you created above	
	Web Acceleration Profile	Select the Web Acceleration profile you created above	
	SSL Profile (Client)	Select the Client SSL profile you created above	
	SSL Profile (Server)	If applicable, select the Server SSL profile you created above	
	SNAT Pool	**Auto Map** (if you expect more than 64,000 concurrent connections, create a SNAT Pool)	
	Access Profile	Select the Access profile you created and edited above	
	Connectivity Profile	Select the Connectivity profile you created above	
	Rewrite Profile	Select the Rewrite profile you created above	
	Access Profile	Select the Access profile you created and edited above	
	Default Pool	Select the pool you created above	
	Default Persistence profile	**source_addr**	

➲ **Note:**

If your download source is an SSL protected server, a Server SSL profile is required. Your download source was defined in both the Web Application and Webtop you created. For example, if you are pointing to the Connection Broker LTM virtual server as recommended in this guide, you will need this Server SSL profile.

If you are pointing directly at a Connection Broker listening on port 80, this Server SSL profile is not required.

Editing the Access Policy

In the following procedure, we show you how to configure edit 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.
4. *Optional:* If you want the APM to perform a check for antivirus software, click the **Antivirus Check** option button, and then click **Add Item**.

   Configure the check as applicable for your configuration. In our example, we leave the default. Click **Save**.
5. On the Successful path between **Antivirus Check** (if applicable, or **Start** if you did not configure an antivirus check) and **Deny**, click the **+** symbol.
6. Click the **Client OS** option button, and then the **Add Item** button.
   a. In the **Name** field, you can optionally type a new name.
   b. Click the **Branch Rules** tab.
   c. For each of the following Branch rules, click the delete (**x**) button on the right: **Linux**, **MacOS**, **iOS**, **Android**, and **Windows mobile**.
   In this guide, we detect Windows systems in order to provide AutoLaunch and Single Sign On. Currently VMware only supports these features on the Windows Platform. If you would like to provide specific actions for client OS's in your environment, you may choose to leave these paths in place and customize the VPE accordingly.
   d. Click the **Save** button.
7. On the *Windows* path between **Client OS** and **Deny**, click the **+** symbol.
8. Click the **Logon Page** option button, and then the **Add Item** button.
   a. Configure the Logon Page as applicable for your configuration. In our example, we leave the default.
   b. Click **Save**.
9. On the *Windows Fallback* path between **Logon Page** and **Deny**, click the **+** symbol.
10. Click the **AD Auth** option button, and then the **Add Item** button.
    a. From the **Server** list, select the AAA server you configured in the table above.
    b. All other settings are optional.
    c. Click **Save**. You now see a Successful and Fallback path from AD Auth.
11. On the *Successful* path between AD Auth and Deny, click the **+** symbol.
12. Click the **Windows File Check** option button, and then click the **Add Item** button. The Windows File Checker page opens. Complete the following:
    a. In the **Name** box, you can optionally type a new name.

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

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

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

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

d. From the **Version Comparison** list, select **=**.

e. Leave the rest of the settings at their default levels.

f. Click the **Save** button. You know see a Successful and Fallback path from Windows File Check.

13. On the *Successful* path between **Windows File Check** and **Deny**, click the **+** button.
14. Click the **Full Resource Assign** option button, and then the **Add Item** button. Complete the following:

a. Click the **Add New Entry** button.

b. Click the **Add/Delete** link.

c. Click the Network Access Resources tab.

d. Click the option button for the Network Access Resource object you created in the table above.

e. Click the Webtop tab.

f. Click the option button for the Webtop you created in the table above.

g. Click **Update**.

h. Click **Save**.

15. On the *Fallback* path between **Full Resource Assign** and **Deny**, click the **+** button.
16. Click the **Variable Assign** option button, and then click the **Add Item** button. The Resource Assignment page opens. Complete the following:

a. In the **Name** box, you can optionally type a new name.

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

c. Click the **change** button.

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

e. From the **Property** list, select **application_launch**.

f. In the **Custom Expression** box on the right, use the following syntax for the expression, replacing the red text with information from your implementation (see note following).

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

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

Note

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

g. Click the **Finished** button.

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

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

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

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

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

    d. Click **Save**.

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

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

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

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

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

    e. Click **Save**.

23. On the Fallback path after **Webtop and Links Assign** click the **Deny** box link.
24. Click the **Allow** option button, and then click **Save**.
25. Back near the Start, on the *Fallback* path between **Client OS** and **Deny**, click the **+** symbol.
26. Click **Logon Page** option button, and then the **Add Item** button.

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

    b. Click **Save**.

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

28. Click **AD Auth** option button, and then the **Add Item** button.
    a. From the **Server** list, select the AAA server you configured in the table above.
    b. All other settings are optional.
    c. Click **Save**. You now see a Successful and Fallback path from AD Auth.
29. On the Successful path between AD Auth(1) and Deny, click the **+** symbol.
30. Click **Full Resource Assign** option button, and then the **Add Item** button. Complete the following:
    a. Click the **Add New Entry** button.
    b. Click the **Add/Delete** link.
    c. Click the Network Access Resources tab.
    d. Click the option button for the Network Access Resource object you created in the table above.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop you created in the table above.
    g. Click **Update**.
    h. Click **Save**.
31. On the Fallback path after **Full Resource Assign** click the **Deny** box link.
32. Click the **Allow** option button, and then click **Save**.
33. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.

This completes the manual configuration.

Document Revision History

Version	Description	Date
1.0	New document	N/A
1.1	- Clarified guidance on entering the FQDN that clients use to access View in step 2 on page 10. - Added the section: *Modifying the Access Policy to customize the links to the View Client (optional) on page 17.*	N/A
1.2	- Added a field for the Active Directory domain name - Added a field for the addition of a custom download location for the View client - Made the Health monitor response string required (with a default value of "View") - Changed the section *Providing the View Client software download for Windows PCs (Optional)* to be *Modifying the Access Policy to customize the links to the View Client (optional),* and updated instructions. - Added section on removing the option to provide the View Client.	N/A
1.3	- Updated the guide to reflect a new version of the downloadable iApp (vmware_view_5.2011-11-15), available on DevCentral. - Modified steps 3c, 4c, and 4d (the External URL box in the View and Security Server Configuration) in the *Modifying VMware View 5.0 if using Security Servers and Connection Servers on page 6* to remove the DNS name option. This field must contain an IP address. - Added a note to the same section stating that if the View Client is not using Network Access through the APM and has a routable path to the View Connection Servers directly, PCoIP must be enabled. - Added examples to the FQDN and Active Directory domain name questions (2 and 3) in *Virtual Server on page 12.* - Added a new field (in the new iApp as well as this guide) for the Active Directory FQDN in the *APM Authentication on page 15.*	N/A
1.4	- Added the question regarding PCoIP in *General Questions on page 11.* - Added the Web Traffic section which asks questions on how the BIG-IP system handles encrypted traffic. Removed the encryption questions from the individual sections. - Removed the Node field when using Security Servers, or Connection Servers only with SSL Offload or SSL Bridging, or if using PCoIP. The iApp automatically sets the correct port. - Added questions about setting the ACL order in *Access Policy Manager on page 14*	N/A
1.5	- Updated the iApp version referenced in the guide to reflect the latest version of the downloadable iApp (vmware_view_5.2012_04_05), available on DevCentral.	05/10/2012
1.6	- Updated multiple locations in the guide to clarify the fact that SSL Offload is only an option if using VMware View 4.6. VMware does not support SSL offload in View versions 5.0 and later.	05/18/2012
1.7	- Updated the deployment guide for version 06_13_2012 of the iApp template. - Added the ability to forward PCoIP traffic through the BIG-IP LTM. - Added additional SSL encryption options, calling out the fact that SSL offload and no SSL are options for View 4.6 only. Because of changes in VMware View, you must select SSL Bridging for View 5.0 and later.	06/14/2012

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