BIG-IP® Access Policy Manager®:
Third-Party Integration Implementations

Version 12.0

Table of Contents

Legal Notices

Legal notices

Publication Date

This document was published on September 1, 2015.

Publication Number

MAN-0505-03

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Citrix Requirements for Integration with APM

About Access Policy Manager and Citrix integration types

When integrated with Citrix, Access Policy Manager® (APM™) performs authentication (and, optionally uses SmartAccess filters) to control access to Citrix published applications. APM supports these types of integration with Citrix:

Integration with Web Interface sites

In this deployment, APM load-balances and authenticates access to Web Interface sites, providing SmartAccess conditions based on endpoint inspection of clients. Web Interface sites communicate with XML Brokers, render the user interface, and display the applications to the client.

Integration with XML Brokers

In this deployment, APM does not need a Web Interface site. APM load-balances and authenticates access to XML Brokers, providing SmartAccess conditions based on endpoint inspection of clients. APM communicates with XML Brokers, renders the user interface, and displays the applications to the client.

About Citrix required settings

To integrate Access Policy Manager® with Citrix, you must meet specific configuration requirements for Citrix as described here.

Trust XML Requests

To support communication with APM®, make sure that the Trust XML requests option is enabled in the XenApp AppCenter management console.

Web Interface site authentication settings

If you want to integrate APM with a Citrix Web Interface site, make sure that the Web Interface site is configured with these settings:

- Authentication point set to **At Access Gateway**.
- Authentication method set to **Explicit**.
- Authentication service URL points to a virtual server on the BIG-IP® system; the URL must be one of these:
  - `http://`*`address of the virtual server`*`/CitrixAuth`
  - `https://`*`address of the virtual server`*`/CitrixAuth` (if traffic is encrypted between APM and the Citrix Web Interface site).

    The address can be the IP address or the FQDN. If you use HTTPS, make sure to use the FQDN that you use in the SSL certificate on the BIG-IP system.

Application access control (SmartAccess)

If you want to control application access with SmartAccess filters through Access Policy Manager, make sure that the settings in the XenApp AppCenter management console for each of the applications you want to control, match these:

Citrix setting	Value
Allow connections made through Access Gateway	enabled
Access Gateway Farm	`APM`
Access Gateway Filter	The value must match the literal string that Access Policy Manager sets during access policy operation (through the Citrix SmartAccess action item)

Note: *The navigation path for application access control is* `AppCenter > Citrix Resources > XenApp > farm_name > Applications > application_name > Application Properties > Advanced Access Control`*.*

User access policies (SmartAccess)

You can control access to certain features, such as Client Drive or Printer Mapping, so that they are permitted only when a certain SmartAccess string is sent to XenApp server. If you want to control access to such features with SmartAccess filters through Access Policy Manager, you need to create a Citrix User Policy with Access Control Filter in the XenApp AppCenter management console for each feature that you want to control. Make sure that the Access Control Filter settings of the Citrix User Policy match these:

Citrix setting	Value
Connection Type	With Access Gateway
Access Gateway Farm	`APM`
Access Gateway Filter	The value must match the literal string that Access Policy Manager sets during access policy execution (through the Citrix SmartAccess action item)

Note: *The navigation path for user access policies is* `AppCenter > Citrix Resources > XenApp > farm_name > Policies > Users > Citrix User Policies > new_policy_name`*. Choose the feature from Categories and, if creating a new filter, select New Filter Element from Access Control.*

About Citrix Receiver requirements for Mac, iOS, and Android clients

To support Citrix Receivers for Mac, iOS, and Android, you must meet specific configuration requirements for the Citrix Receiver client.

Address field for standard Citrix service site (`/Citrix/PNAgent/`)

`https://<APM-external-virtual-server-FQDN>`

Address field for custom Citrix service site

`https://<APM-external-virtual-server-FQDN/custom_site/config.xml`, where `custom_site` is the name of the custom service site

Access Gateway
Select the Access Gateway check box and select Enterprise Edition.

Authentication
Choose either: Domain-only or RSA+Domain authentication

About Citrix Receiver requirements for Windows and Linux clients

To support Citrix Receiver for Windows and Linux clients, you must meet specific configuration requirements for the Citrix Receiver client, as described here.

Address field for standard Citrix service site (`/Citrix/PNAgent/`)
`https://`*`<APM-external-virtual-server-FQDN>`*

Address field for custom Citrix service site
`https://`*`<APM-external-virtual-server-FQDN`*`/`*`custom_site`*`/config.xml`, where *`custom_site`* is the name of the custom service site.

About Citrix requirements for Kerberos and SmartCard SSO

Access Policy Manager® (APM®) supports single sign-on (SSO) for XenApp and XenDesktop clients that connect through an APM dynamic webtop. SSO for XenApp is supported with the Kerberos SSO method. SSO for XenDesktop is supported with either the Kerberos SSO or the SmartCard method.

To use the SSO options that APM supports, you must meet specific configuration requirements for Citrix as described here:

- Kerberos: Configure Kerberos Delegation in Active Directory as described in Citrix knowledge article *CTX124603*.
- SmartCard: Enable SID Enumeration on XenApp and XenDesktop as described in these Citrix knowledge articles: *CTX117489* and *CTX129968*.

About Citrix product terminology

XenApp server
Refers to the XML Broker in the farm where Citrix SmartAccess filters are configured and from which applications and features are delivered.

XenApp AppCenter
Refers to the management console for a XenApp farm.

Note: *The names of the Citrix products and components that provide similar services might be different in your configuration. Refer to AskF5™ (`support.f5.com`) to identify the supported version of Citrix in the compatibility matrix for the Access Policy Manager® version that you have. Then refer to version-specific Citrix product documentation for Citrix product names and features.*

About Wyse Xenith Zero client character set settings

On Citrix XenApp or Storefront servers, administrators can provide application names using various languages, some of which use non-ASCII character sets. When using a supported Wyse Zenith Zero client with F5® BIG-IP® APM® Secure Proxy, if an application name was specified using a non-ASCII character set, it can display as ????. If this occurs, it indicates a mismatch between that character set and the character set configured for the keyboard in the peripheral settings on the client.

To view an application name in its correct format, the character set configured for the keyboard on the client must match the language in which the name is specified on the server.

For example, for an application name that is specified in Arabic on the server, peripheral settings for the keyboard on the client must specify character set cp1256. Similarly, for an application name in Cyrillic on the server, the character set specified on the client must be cp1251. Refer to product documentation for the Wyse Xenith Zero client for definitive information.

About Citrix StoreFront proxy support

On Citrix XenApp or Storefront servers, BIG-IP® APM® supports Citrix StoreFront proxy with native protocol using either StoreFront option: Secure Ticket Authority (STA) tickets, or ICA patching. Each of these two options requires administrators to ensure certain pre-requisites on both APM and StoreFront.

For STA ticket, the administrator must ensure that APM acts as a gateway, and the admin uses APM to enable remote access to the StoreFront store clients that the administrator connects to. Both APM and StoreFront require the STA server address.

For ICA patching, the administrator must ensure that APM does not act as a gateway in StoreFront because configuring APM as a gateway can break the client authentication. In addition, ICA patching mode clients can access all StoreFront stores.

Integrating APM with a Citrix Web Interface Site

Overview: Integrating APM with Citrix Web Interface sites

In this implementation, Access Policy Manager® performs authentication while integrating with a Citrix Web Interface site. The Web Interface site communicates with the XenApp server, renders the user interface, and displays the applications to the client.

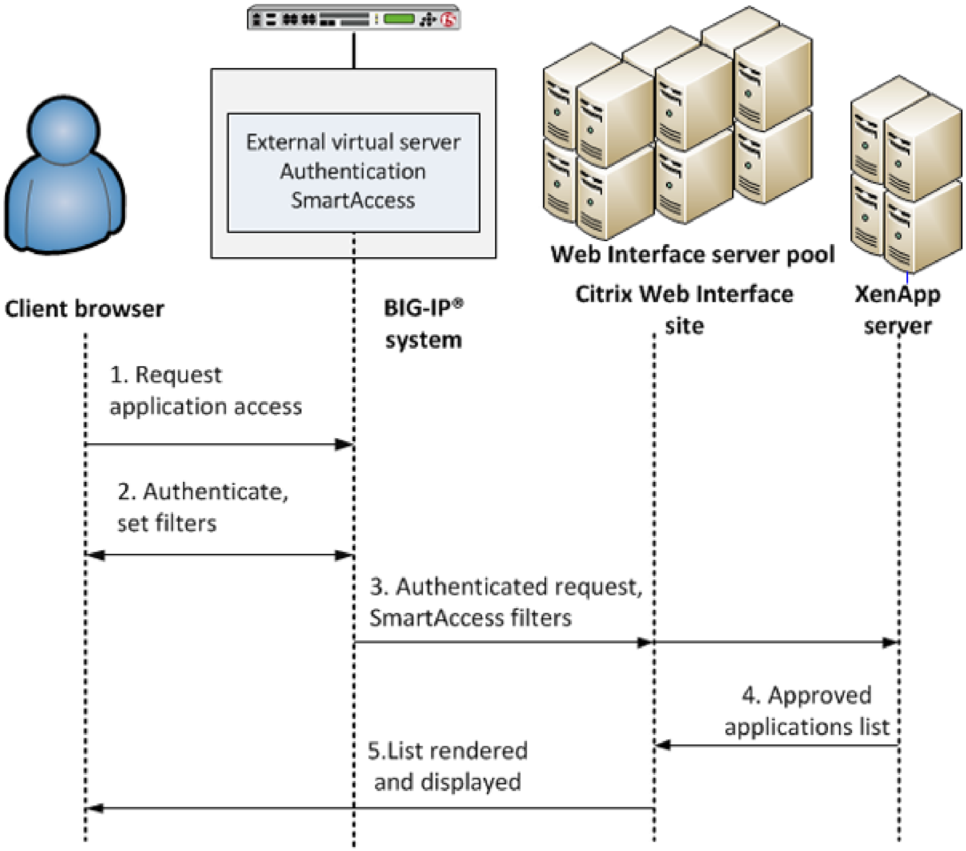

External virtual server
Authentication
SmartAccess
Web Interface server pool
Client browser
BIG-IP® system
Citrix Web Interface site
XenApp server
1. Request application access
2. Authenticate, set filters
3. Authenticated request, SmartAccess filters
4. Approved applications list
5.List rendered and displayed

Figure 1: APM Citrix Web Interface integration with SmartAccess support

The preceding figure shows a configuration with one virtual server that communicates with clients and the Web Interface site.

1. A user (client browser or Citrix Receiver) requests access to applications or features.
2. The external virtual server starts an access policy that performs authentication and sets SmartAccess filters.
3. The external virtual server sends the authenticated request and filters to the Citrix Web Interface site. The Citrix Web Interface site, in turn, forwards the information to the XML broker (XenApp server).
4. The XML Broker returns a list of allowed applications to the Citrix Web Interface site.
5. The Citrix Web Interface site renders and displays the UI to the user.

In cases where the Web Interface site cannot communicate with an external virtual server, you must configure an additional, internal, virtual server to manage requests from the Citrix Web Interface as part of Smart Access and SSO. You need an internal virtual server, for example, when the Web Interface site is behind a firewall, uses HTTP in the Authentication URL, or uses a different SSL CA certificate for establishing trust with APM than the one used by client devices.

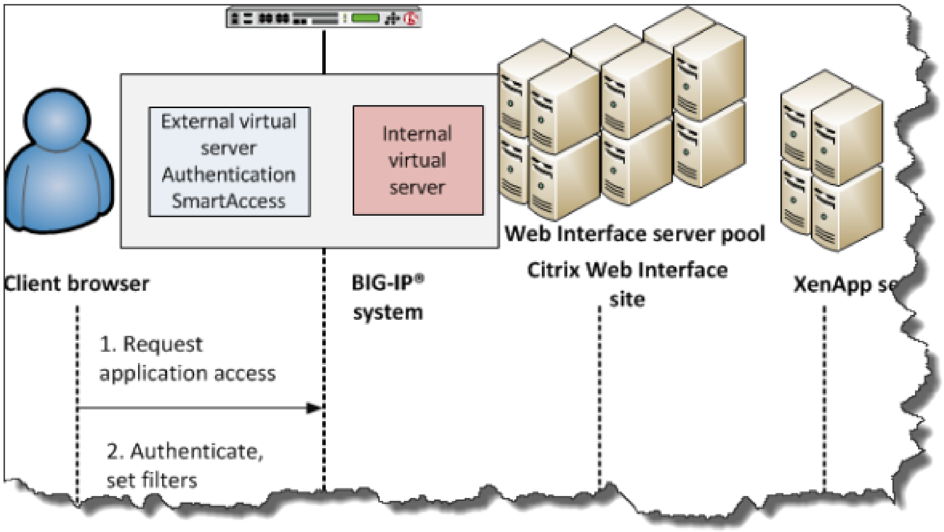

External virtual server Authentication SmartAccess
Internal virtual server
Web Interface server pool
Client browser
BIG-IP® system
Citrix Web Interface site
XenApp se
1. Request application access
2. Authenticate, set filters

Figure 2: Internal virtual server for requests from Web Interface site

Supported clients

This implementation supports web clients and Citrix Receiver (iOS, Android, Mac, Windows, and Linux) clients.

Supported authentication

For Citrix Receiver Windows and Linux clients: only Active Directory authentication is supported.

For Citrix Receiver clients for iOS, Android, and Mac: Active Directory, or both RSA and Active Directory authentication is supported.

For web clients, you are not restricted in the type of authentication you use.

About the iApp for Citrix integration with APM

An iApps® template is available for configuring Access Policy Manager® and Local Traffic Manager™ to integrate with Citrix applications. The template can be used on the BIG-IP® system to create an application service that is capable of performing complex configurations. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at `https://devcentral.f5.com/wiki/iApp.Citrix-Applications.ashx`. A deployment guide is also available there.

Task summary for APM integration with Citrix Web Interface sites

Ensure that you configure the Citrix components in the Citrix environment, in addition to configuring the BIG-IP® system to integrate with Citrix Web Interface sites.

Perform these tasks on the BIG-IP system to integrate Access Policy Manager® with a Citrix Web Interface site.

Task list

Creating an access profile
Verifying log settings for the access profile
Creating an access policy for Citrix SSO
Adding Citrix Smart Access actions to an access policy
Creating a pool of Citrix Web Interface servers
Adding a connectivity profile
Creating a custom HTTP profile
Configuring the external virtual server
Creating a data group to support a nonstandard Citrix service site
Configuring an internal virtual server

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select one of these options.
   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.

   Additional settings display.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

Note: *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   Note: *Logging is disabled when the* ***Selected*** *list is empty.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Creating an access policy for Citrix SSO

Before you can create an access policy for Citrix single sign-on (SSO), you must configure the appropriate AAA servers to use for authentication.

Note: *An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

You configure an access policy to authenticate a user and enable single sign-on (SSO) to Citrix published resources.

Note: *APM® supports different types of authentication depending on the client type. This access policy includes steps for both RSA SecurID and AD Auth authentication (supported for Citrix Receiver for iOS, Mac, and Android) or AD Auth only (supported for Citrix Receiver for Windows and Linux). Use the type of authentication for the client that you need to support.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

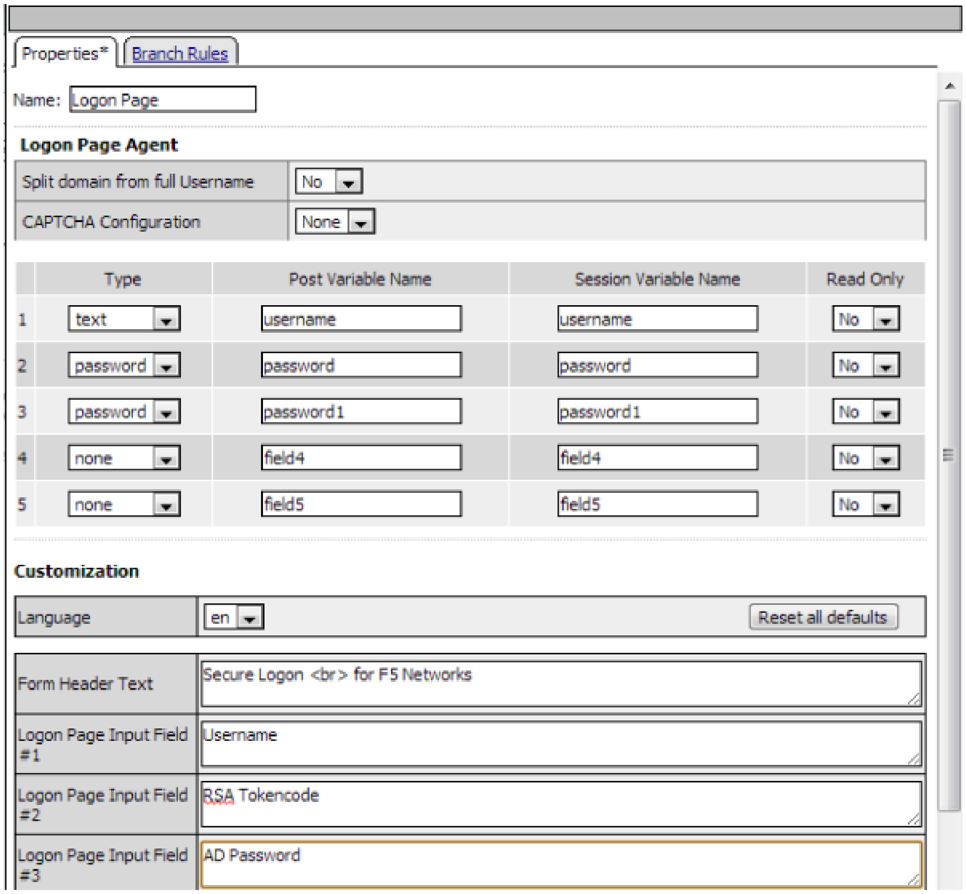
Note: Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.

A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

4. On the popup screen, on the Logon tab, specify an access policy as appropriate:
   - **Logon Page**: Select this if you allow one-factor password authentication with a single logon prompt containing one password field.
   - **Citrix Logon Prompt**: Select this if you allow two-factor password authentication with a single logon prompt containing two password fields.
5. Click **Add Item**.

   A properties screen displays.
6. To configure the Logon Page properties, specify the authentication required:
   - To support Active Directory authentication only, click **Save**.
   - To support both Active Directory and RSA SecurID authentication, configure the Logon Page to accept an RSA token and an AD password, and then click **Save**.

   In this example, Logon Page Input Field #2 accepts the RSA Token code into the `session.logon.last.password` variable (from which authentication agents read it). Logging Page Input Field #3 saves the AD password into the `session.logon.last.password1` variable.



Name: Logon Page

Logon Page Agent

Split domain from full Username	No
CAPTCHA Configuration	None

	Type	Post Variable Name	Session Variable Name	Read Only
1	text	username	username	No
2	password	password	password	No
3	password	password1	password1	No
4	none	field4	field4	No
5	none	field5	field5	No

Customization

Language	en
Form Header Text	Secure Logon for F5 Networks
Logon Page Input Field #1	Username
Logon Page Input Field #2	RSA Tokencode
Logon Page Input Field #3	AD Password

   The properties screen closes.
7. To configure the Citrix Logon Prompt properties, specify the type of authentication needed:
   - To support two-factor authentication, click **Save**.

- To support domain-only authentication, from the Citrix Authentication Type list, select **domain-only** and then click **Save**.

8. (Optional) To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:

a) From the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.

b) In the properties screen from the **Server** list, select the AAA server that you created previously and click **Save**.
The properties screen closes.

c) After the RSA SecurID action, add a Variable Assign action.

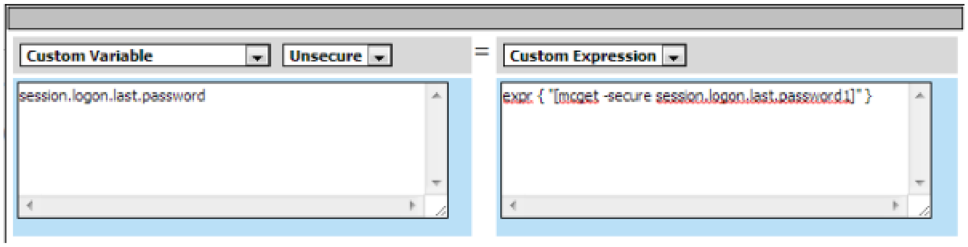
Use the Variable Assign action to move the AD password into the *`session.logon.last.password`* variable.

d) Click **Add new entry**.
An **empty** entry appears in the Assignment table.

e) Click the **change** link next to the empty entry.
A dialog box opens, where you can enter a variable and an expression.

f) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.password`.

g) From the right-side list, select **Custom Expression** (the default), and type `expr { "[mcget -secure session.logon.last.password1]" }`.



Custom Variable ▾ Unsecure ▾ = Custom Expression ▾

session.logon.last.password

expr { "[mcget -secure session.logon.last.password1]" }

The AD password is now available for use in Active Directory authentication.

h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

9. Add the AD Auth action after one of these actions:

- Variable Assign - This action is present only if you added RSA SecurID authentication.
- Logon Page - Add here if you did not add RSA SecurID authentication.

A properties screen for the AD Auth action opens.

10. Configure the properties for the AD Auth action:

a) From the **AAA Server** list, select the AAA server that you created previously.

b) To support Citrix Receiver clients, you must set **Max Logon Attempts** to 1.

c) Configure the rest of the properties as applicable to your configuration and click **Save**.

11. Click the Add Item (+) icon between **AD Auth** and **Deny**.

a) From the Assignment tab, select **SSO Credential Mapping**, and click **Add Item**.

b) Click **Save**.

The SSO Credential Mapping makes the information from the *`session.logon.last.password`* variable available (for Citrix SSO).

12. Add a Variable Assign action after the SSO Credential Mapping action.

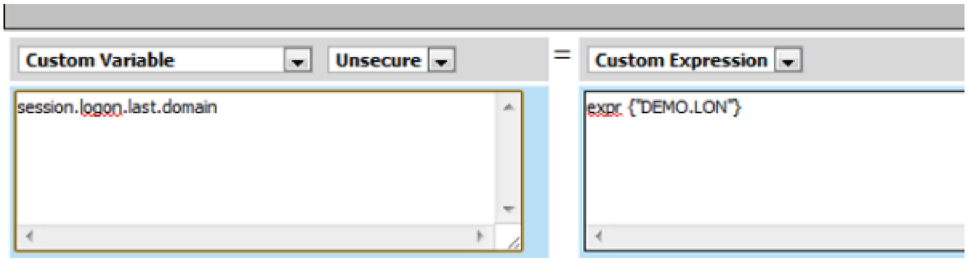
Use the Variable Assign action to pass the domain name for the Citrix Web Interface site so that a user is not repeatedly queried for it.

a) Click **Add new entry**.
An **empty** entry appears in the Assignment table.

b) Click the **change** link next to the empty entry.
A dialog box opens, where you can enter a variable and an expression.

c) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.domain`.

d) From the right-side list, select **Custom Expression** (the default), and type an expression `expr {"DEMO.LON"}`, to assign the domain name for the Citrix Web Interface site (where DEMO.LON is the domain name of the Citrix Web Interface site).



Custom Variable ▾ Unsecure ▾ = Custom Expression ▾

```
session.logon.last.domain
```

```
expr {"DEMO.LON"}
```

e) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

13. On the fallback path between the last action and **Deny**, click **Deny**, and then click **Allow** and **Save**.

14. Click **Close**.

You should have an access policy that resembles one of these examples:

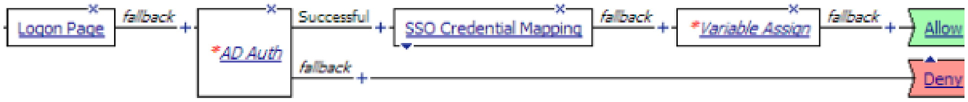


Figure 3: Example access policy with AD authentication, credential mapping, and Web Interface site domain assignment

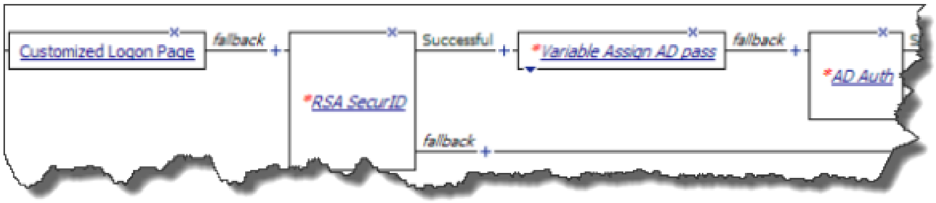


Figure 4: Configuring RSA SecurID authentication before AD authentication

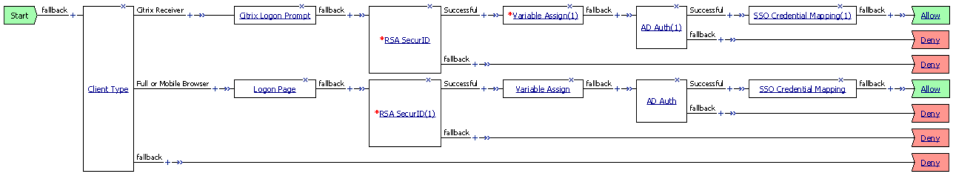


Figure 5: Example access policy with Citrix Logon Prompt

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Adding Citrix Smart Access actions to an access policy

To perform this task, first select the access profile you created previously, and open the associated access policy for edit.

You can set one or more filters per Citrix Smart Access action. If you include multiple Citrix Smart Access actions in an access policy, Access Policy Manager accumulates the SmartAccess filters that are set throughout the access policy operation.

1. Click the(+) icon anywhere in your access profile to which you want to add the Citrix Smart Access action item.
   The Add Item screen opens.
2. From **General Purpose**, select **Citrix Smart Access** and click **Add Item**.
   The Variable Assign: Citrix Smart Access properties screen opens.
3. Type the name of a Citrix SmartAccess filter in the open row under Assignment.

   A filter can be any string. Filters are not hardcoded, but must match filters that are configured in the XenApp™ server for application access control or a user policy.

   Note: *In the XenApp server, you must specify `APM` as the Access Gateway farm when you configure filters.*

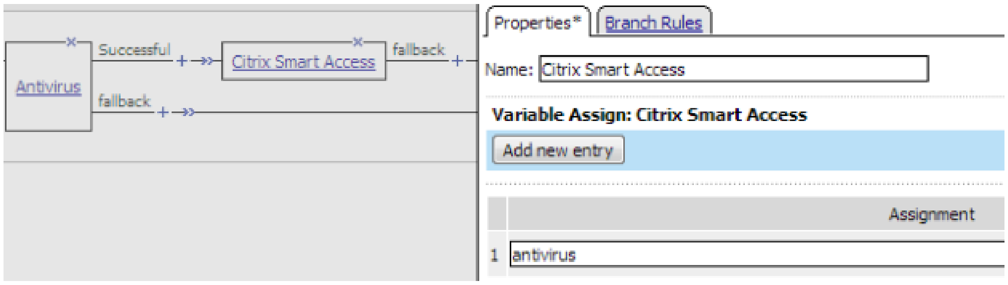
4. To add another filter, click **Add entry** and type the name of a Citrix filter in the open row under Assignment.
5. When you are done adding filters, click **Save** to return to the Access Policy.
6. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Example access policy with Citrix SmartAccess filters

Here is a typical example access policy that uses Citrix SmartAccess filters to restrict access to published applications based on the result of client inspection. Client inspection can be as simple as IP Geolocation Match or Antivirus. The figure shows an access policy being configured with a Citrix Smart Access action to set a filter to `antivirus` after an antivirus check is successful.



Name: Citrix Smart Access

Variable Assign: Citrix Smart Access

	Assignment
1	antivirus

Figure 6: Example access policy with Citrix SmartAccess action and an antivirus check

Creating a pool of Citrix Web Interface servers

Create a pool of Citrix Web Interface servers for high availability.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each resource that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select **Node List** and select an address from the list of available addresses.
   b) If access to the Web Interface site is through SSL, in the **Service Port** field type `443`; otherwise, type `80`.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Adding a connectivity profile

Create a connectivity profile to configure client connections for Citrix remote access.

Note: *A Citrix client bundle provides an installable Citrix Receiver client. The default parent connectivity profile includes a default Citrix client bundle.*

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. From the **Parent Profile** list, select the default profile, **connectivity**.
5. To use a Citrix bundle that you have configured, select **Citrix Client Settings** from the left pane and select the bundle from the **Citrix Client Bundle** list in the right pane.

   The default Citrix client bundle is included if you do not perform this step.
6. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the Connectivity Profile List.

Creating a custom HTTP profile

An HTTP profile defines the way that you want the BIG-IP® system to manage HTTP traffic.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.

2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **http**.
5. Select the **Custom** check box.
6. From the **Redirect Rewrite** list, select **All**.
7. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Configuring the external virtual server

Create a virtual server to support Citrix traffic and respond to client requests.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1/32` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`.

   Note: *If you plan to configure only one virtual server to integrate with Citrix Web Interface sites, then the authentication URL of the Web Interface site must match the IP address of this virtual server.*
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. (Optional) For the **SSL Profile (Client)** setting, select an SSL profile with an SSL certificate that is trusted by clients.
8. If you use SSL to access the Web Interface site, add an SSL profile to the **SSL Profile (Server)** field.
9. From the **HTTP Profile** list, select the custom http profile that you created previously.

   The HTTP profile must have **Redirect Rewrite** set to **All**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
12. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
13. From the **VDI Profile** list, select a VDI profile.

    You can select the default profile, **vdi**.
14. In the Resources area, from the **Default Pool** list, select the name of the pool that you created previously.
15. Click **Finished**.

The access policy is now associated with the virtual server.

Creating a data group to support a nonstandard Citrix service site

By default, APM recognizes `/Citrix/PNAgent/config.xml` as the default URL that Citrix Receiver clients request. If your Citrix Receiver clients use a value that is different from /Citrix/PNAgent/config.xml, you must configure a data group so that APM® can recognize it.

1. On the Main tab, click **Local Traffic** > **iRules** > **Data Group List**.
   The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**.
   The New Data Group screen opens.
3. In the **Name** field, type `APM_Citrix_ConfigXML`.

   Type the name exactly as shown.
4. From the **Type** list, select **String**.
5. In the Records area, create a string record.
   a) In the **String** field, type the FQDN of the external virtual server (using lowercase characters only).

      For example, type `apps.mycompany.com`.
   b) In the **Value** field, type the value that you use instead of Citrix/PNAgent/config.xml. For example, type `/`*`Connect`*`/config.xml`.
   c) Click **Add**.
6. Click **Finished**.
   The new data group appears in the list of data groups.

Configuring an internal virtual server

Before configuring an internal virtual server, you need to configure an access profile with default settings.

Configure an internal virtual server to handle requests from the Citrix Web Interface site when it is behind a firewall, using HTTP, or otherwise unable to communicate with an external virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
5. For the **Service Port** setting, select **HTTP** or **HTTPS**.

   The protocol you select must match the protocol you used to configure the authentication service URL on the Web Interface site.
6. If you are encrypting traffic between the APM and the Citrix Web Interface, for the **SSL Profile (Client)** setting, select an SSL profile that has an SSL certificate trusted by the Citrix Web Interface.
7. From the **HTTP Profile** list, select **http**.
8. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
9. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.

10. From the **VDI Profile** list, select a VDI profile.
    You can select the default profile, **vdi**.
11. Click **Finished**.

The access policy is now associated with the virtual server.

Integrating APM with Citrix XML Brokers

Overview: Integrating APM with Citrix XML Brokers with SmartAccess support

In this implementation, you integrate Access Policy Manager® (APM®) with Citrix XML Brokers and present Citrix published applications on an APM dynamic webtop.

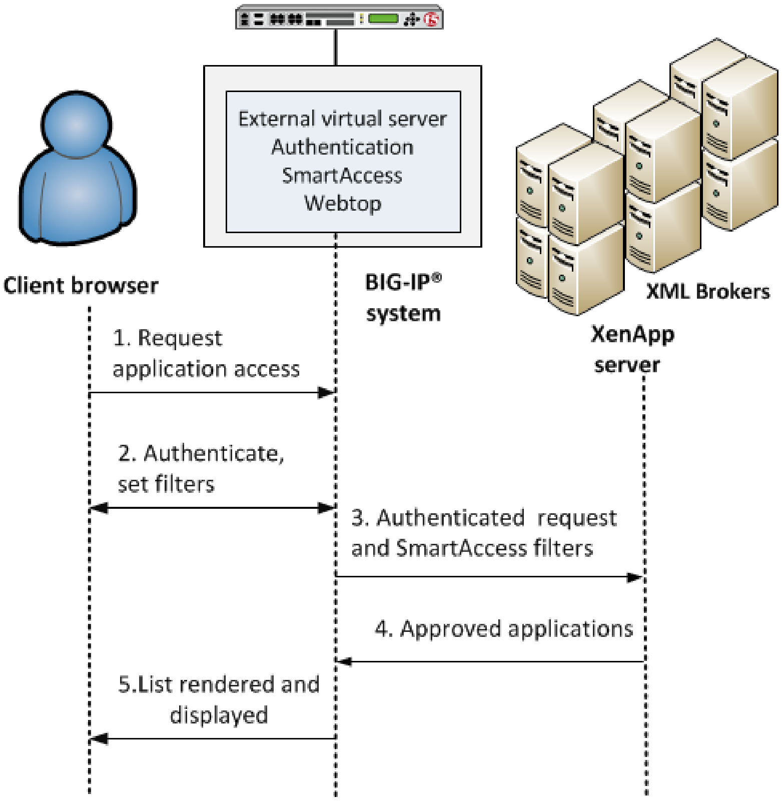

External virtual server
Authentication
SmartAccess
Webtop
Client browser
BIG-IP® system
XML Brokers
XenApp server
1. Request application access
2. Authenticate, set filters
3. Authenticated request and SmartAccess filters
4. Approved applications
5.List rendered and displayed

Figure 7: APM integration with Citrix XML Brokers

1. A user (client browser or Citrix Receiver) requests access to applications.
2. The virtual server starts an access policy that performs authentication and sets SmartAccess filters.
3. The virtual server sends the authenticated request and filters to a Citrix XML Broker.
4. An XML Broker returns a list of allowed applications to the external virtual server.
5. The virtual server renders and displays the user interface to the client on an Access Policy Manager webtop.

Supported authentication

For Citrix Receiver Windows and Linux clients: only Active Directory authentication is supported.

For Citrix Receiver clients for iOS, Android, and Mac: Active Directory, or both RSA and Active Directory authentication is supported.

For web clients, you are not restricted in the type of authentication you use.

About APM dynamic webtop for Citrix XML Brokers

A dynamic webtop enables Access Policy Manager® (APM®) to act as a presentation layer for Citrix published resources. APM communicates directly with Citrix XML Brokers, retrieves a list of published resources, and displays them to the user on a dynamic webtop.

The addresses of XML Brokers are configured in pools on APM. A pool includes addresses from one Citrix farm. You specify a pool as a destination in a Citrix remote desktop resource. Each resource logically represents a Citrix farm. You can assign multiple resources to a user, enabling the user to access Citrix applications from multiple Citrix farms.

About Client Type

The Client Type action determines whether the client is using a full browser, the BIG-IP® Edge Client, or another client to access the Access Policy Manager® (APM®). This action makes it possible to specify different actions for different client types in one access policy and, as a result, to use one virtual server for traffic from different client types. This figure shows the Client Type action as it looks when first added to an access policy.

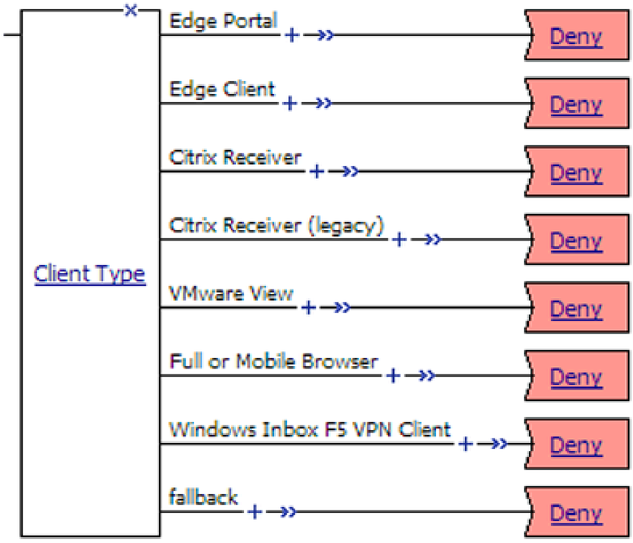


Figure 8: Client Type

By default, the Client Type action includes these branches:

Edge Portal
Indicates that the user is connecting with the BIG-IP® Edge Portal® mobile app.

Edge Client
Indicates that the user is connecting with the BIG-IP® Edge Client® or BIG-IP Edge Client app, supported on multiple devices and operating systems.

Citrix Receiver
Indicates that the user is connecting using a later Citrix Receiver client.

Citrix Receiver (legacy)
Indicates that the user is connecting using an earlier Citrix Receiver client (identified with PN Agent).

VMware View

Indicates that the user is connecting using a VMware Horizon View client.

Full or Mobile Browser

Indicates the user is connecting with a Windows web browser or a mobile browser.

Windows Inbox F5 VPN Client

Indicates the user is connecting using the Windows Inbox F5 VPN client.

fallback

Indicates the user is connecting with another method.

APM supports the client types on multiple operating systems. Refer to AskF5™ (`support.f5.com`) to look up the supported operating systems and versions in the compatibility matrix for your version of APM.

Note: *To create additional branching for a client type based on operating system, you can add a client operating system (Client OS) action on the client type branch.*

About Citrix client bundles in APM

A Citrix client bundle enables delivery of a Citrix Receiver client to a user's Windows computer when a client is not currently installed, or when a newer client is available. Access Policy Manager® (APM®) detects whether the Citrix Receiver client is present and redirects users to a download URL, or downloads a Citrix Receiver client that you have uploaded.

In Access Policy Manager, you specify the Citrix client bundle in a connectivity profile. By default, a connectivity profile includes the default Citrix bundle, `/Common/default-citrix-client-bundle`, which contains a download URL, `receiver.citrix.com`.

Note: *You can upload Citrix Receiver clients from the Application Access area of Access Policy Manager.*

About APM SSO support for Citrix clients

Access Policy Manager® (APM®) supports two single sign-on options for Citrix that provide password-less authentication:

- Kerberos - Supports any kind of password-less authentication on APM: SmartCard, RSA PIN, client SSL certificate, and so on. Citrix supports Kerberos only for XenApp.
- SmartCard - Citrix supports SmartCard for XenDesktop. Citrix also supports SmartCard for XenApp.

  Note: *When using SmartCard with XenApp, a user is prompted for a SmartCard PIN twice: once when logging in to APM and again when starting a Citrix application.*

These options work in APM only when:

- Citrix is configured to support SmartCard SSO (with Kerberos) or SmartCard.
- Citrix requirements for using SmartCard SSO or SmartCard are met.

About the iApp for Citrix integration with APM

An iApps® template is available for configuring Access Policy Manager® and Local Traffic Manager™ to integrate with Citrix applications. The template can be used on the BIG-IP® system to create an application service that is capable of performing complex configurations. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at `https://devcentral.f5.com/wiki/iApp.Citrix-Applications.ashx`. A deployment guide is also available there.

Task summary for XML Broker integration with APM

Ensure that you configure the Citrix components in the Citrix environment, in addition to configuring the BIG-IP® system to integrate with Citrix XML Brokers.

Perform these tasks on the BIG-IP system so that Access Policy Manager® can present Citrix published resources on a dynamic webtop.

Task list

Creating a pool of Citrix XML Brokers
Configuring a Citrix remote desktop resource
Configuring a dynamic webtop
Creating an access policy for Citrix SSO (APM dynamic webtop)
Assigning Citrix resources to an access policy for Citrix integration
Adding Citrix Smart Access actions to an access policy
Verifying log settings for the access profile
Adding a connectivity profile
Adding Citrix Receiver for HTML5 to a connectivity profile
Creating a virtual server to support Citrix web and mobile clients

Creating a pool of Citrix XML Brokers

Create one pool of XML Brokers for each Citrix farm that you want to support.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each resource that you want to include in the pool:
   a) Either type an IP address in the **Address** field, or select a preexisting node address from the **Node List**.
   b) If access to the XML Broker is through SSL, in the **Service Port** field, type `443` or select **HTTPS** from the list; otherwise, type `80` or select **HTTP** from the list.
   c) Click **Add**.

5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a Citrix remote desktop resource

Create one Citrix remote desktop resource for each Citrix farm that you want to support.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Remote Desktops List**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. Type a name for the remote desktop resource.
4. For the **Type** setting, retain the default **Citrix**.
5. For the **Destination** setting, select **Pool** and select the pool that you created previously.
6. In the Single Sign-On area, select the **Enable SSO** check box for single sign-on to a Citrix XML Broker after logging in to Access Policy Manager® (APM®).
   a) From the **SSO Method** list, select the type of single sign-on to use, either Password-based, Kerberos, SmartCard, or Anonymous.

      The Kerberos and SmartCard options enable password-less authentication. You cannot use either of them successfully unless Citrix is configured for SmartCard SSO (Kerberos) or SmartCard.

      The fields that are displayed vary based on this selection.
   b) In the **Username Source** field, accept the default or type the session variable to use as the source for the SSO user name.
   c) In the **Password Source** field, accept the default or type the session variable to use as the source for the SSO user password.
   d) In the **Domain Source** field, accept the default or type the session variable to use as the source for the SSO user domain.
   e) From the **Kerberos SSO** list, select a Kerberos SSO configuration that has already been configured.
7. In the Customization Settings for `language_name` area, type a **Caption**.

   The caption is the display name of the Citrix resource on the APM webtop.
8. Click **Finished**.

   All other parameters are optional.

This creates the Citrix remote desktop resource.

Configuring a dynamic webtop

A dynamic webtop allows you to see a variety of resources protected by Access Policy Manager®, including Citrix Published Applications.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtops screen displays.
2. Click **Create**.
   The New Webtop screen opens.
3. In the **Name** field, type a name for the webtop.

4. From the **Type** list, select **Full**.
   The Configuration area displays with additional settings configured at default values.
5. Click **Finished**.

The webtop is now configured, and appears in the webtop list.

Creating an access policy for Citrix SSO (APM dynamic webtop)

Before you can create an access policy for Citrix single sign-on (SSO), you must meet these requirements:

- Configure the appropriate AAA servers to use for authentication.

  Note: *An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

- Create an access profile using default settings.

You configure an access policy to authenticate a user and enable single sign-on (SSO) to Citrix published resources.

Note: *APM® supports different types of authentication depending on the client type. This access policy shows how to use the Client Type action to configure authentication for legacy Citrix Receiver clients (Windows and Linux), and later Citrix Receiver clients (iOS, Mac, and Android) in the same access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `client` in the search field, and select **Client Type** from the results.
   A properties screen displays.
5. Click **Save**.
6. On the properties screen, on the Logon tab, select an access policy as appropriate:
   - **Logon Page**: Specify this if you allow one-factor password authentication with a single logon prompt containing one password field.
   - **Citrix Logon Prompt**: Specify this if you allow two-factor password authentication with a single logon prompt containing two password fields.
7. Click **Save**.
   The properties screen closes, and the Client Type action and Logon action displays in the visual policy editor.
8. To configure actions for Citrix Receiver for Windows and Linux clients, perform these substeps.

   Note: *Citrix Receiver for Windows version 3.4 and later, and Citrix Receiver for Linux, version 13 and later, support Active Directory authentication only.*

a) Click the (+) icon on the Citrix Receiver (legacy) branch after the Client Type action.
b) On the Logon tab, select either **Logon Page** or **Citrix Logon Prompt**, and click **Add Item**.

   A properties screen displays. The default page settings are acceptable.

c) Click **Save**.
d) After the Logon Page action, add an SSO Credential Mapping action with default settings.
e) After the SSO Credential Mapping action, click the (+) icon.
f) Type `var` into the search field, select **Variable Assign** from the results, and click **Add Item**.

   Use the Variable Assign action to pass the domain name for the Citrix remote desktop resource so that a user is not repeatedly queried for it.

   A properties screen opens.
g) Click **Add new entry**.
   An **empty** entry appears in the Assignment table.
h) Click the **change** link next to the empty entry.
   A dialog box opens, where you can enter a variable and an expression.
i) From the left-side list, retain the **Custom Variable** setting, and type `session.logon.last.domain`.
j) From the right-side list, retain the **Custom Expression** setting, and type `expr {"example.com"}` to assign the domain name for the Citrix remote desktop resource (where `example.com` is the domain name of the resource).

   The Citrix remote desktop resource equates to an XML Broker that is selected from a pool.

k) Click **Finished**.
l) Click **Save**.
m) After the previous action, click the **Deny** ending, and select the **Allow** ending.

The access policy branch for legacy Citrix Receiver clients is complete.

9. To configure actions for Citrix Receiver for iOS, Android, and Mac, complete the remaining steps.

Citrix Receiver for iOS, Android, and Mac, support both RSA SecurID and AD Auth authentication. This example shows how to use both.

10. After the Client Type action, on the Citrix Receiver branch, click the (+) icon.

11. On the Logon tab, select either **Logon Page**, and click **Add Item**.

12. Customize the Logon Page to accept an RSA token and an Active Directory password:

a) In row 2: From the **Type** list, select **password**; in the **Post Variable Name** field, type `password1`; in the **Session Variable Name** field, type `password1`.

   APM stores the text that a user types into this field in the *`session.logon.last.password1`* session variable.

   You have added another password field to the logon page.
b) In **Login Page Input Field #2**, type `Password`.
   You replaced the existing prompt for the first password field.
c) In **Login Page Input Field #3**, type `Passcode`.
   You provided a prompt for the second password field.

13. To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:

a) Type `rsa` in the search field, select **RSA SecurID** from the results, and click **Add Item**.
b) From the **Server** list, select the AAA RSA SecurID server that you created previously and click **Save**.
   The properties screen closes.
c) After the RSA SecurID action, add a Variable Assign action.

   Use the Variable Assign action to move the AD password into the *`session.logon.last.password`* session variable; the authentication agent requires this.

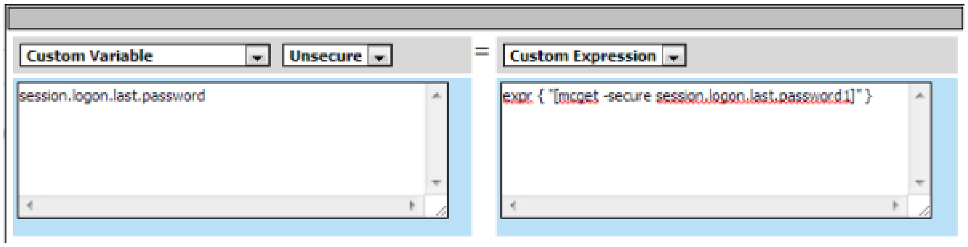
A Variable Assign properties page opens.

d) Click **Add new entry**.
An **empty** entry appears in the Assignment table.

e) Click the **change** link next to the empty entry.
A dialog box opens, where you can enter a variable and an expression.

f) From the left-side list, retain the **Custom Variable** setting, and type `session.logon.last.password`.

g) From the right-side list, retain the **Custom Expression** setting, and type `expr { "[mcget -secure session.logon.last.password1]" }`. For two-factor authentication, type `expr {[mcget {session.logon.last.password1}]} .`



Custom Variable | Unsecure = Custom Expression

session.logon.last.password

expr { "[mcget -secure session.logon.last.password1]" }

h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

i) Click **Save**.

14. After the previous action, add an AD Auth action and configure properties for it:

a) From the **AAA Server** list, select the AAA server that you created previously.

b) If you are using Android Citrix receiver with a disabled session ID rotation in APM, you must set **Max Logon Attempts** to **1**.

c) Configure the rest of the properties as applicable to your configuration, and click **Save**.

15. Click the Add Item (+) icon between **AD Auth** and **Deny**.

a) On the Assignment tab, select **SSO Credential Mapping**, and click **Add Item**.

b) Click **Save**.

The SSO Credential Mapping makes the information from the *`session.logon.last.password`* variable available for Citrix SSO.

16. Add a Variable Assign action after the SSO Credential Mapping action.

Use the Variable Assign action to pass the domain name for an XML Broker so that a user is not repeatedly queried for it.

a) Click **Add new entry**.
An **empty** entry appears in the Assignment table.

b) Click the **change** link next to the empty entry.
A dialog box opens, where you can enter a variable and an expression.

c) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.domain`.

d) From the right-side list, select **Custom Expression** (the default), and type an expression `expr {"`*`example.com`*`"}`.

e) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

17. On the fallback path between the last action and **Deny**, click **Deny**, and then click **Allow** and **Save**.
The access policy branch for the Citrix Receiver client type is complete.

18. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

19. Click **Close**.

You should have an access policy that contains actions for both Citrix Receiver client types.

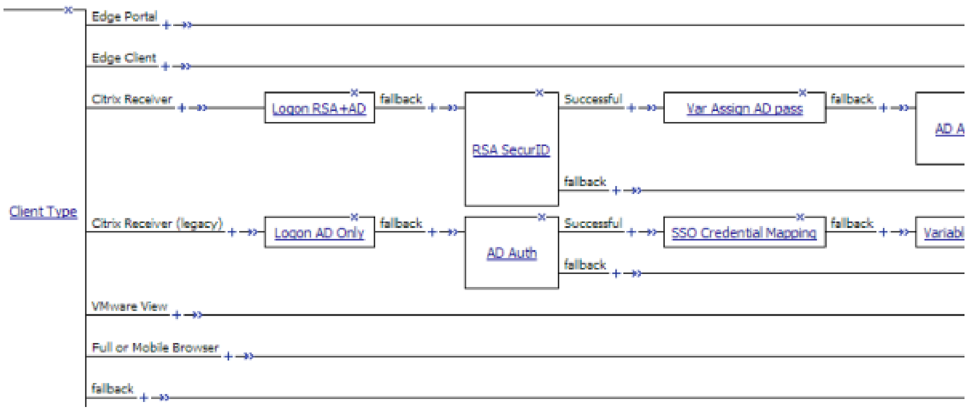


Figure 9: Example access policy for legacy Citrix Receiver clients and later Citrix Receiver clients

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Assigning Citrix resources to an access policy for Citrix integration

Before you assign Citrix resources to an access policy for integration, create or select an access profile, and open the associated access policy for edit.

Assign the webtop and Citrix remote desktop resources that you configured to a session so that XML Brokers associated with the resources can return the appropriate published resources for display on the webtop.

Note: *This access policy shows how to use the Advanced Resource Assign action item to assign the resources. Alternatively, you can use the Resource Assign and Webtop, Links and Sections Assign action items.*

1. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
2. On the Assignment tab, select **Advanced Resource Assign** and click **Add Item**.
   The properties screen opens.
3. Click **Add new entry**.
   An **Empty** entry displays.
4. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
5. Select the Remote Desktop tab.

   A list of remote desktop resources is displayed.
6. Select Citrix remote desktop resources and click **Update**.
   You are returned to the properties screen where Remote Desktop and the names of the selected resources are displayed.
7. Click **Add new entry**.
   An **Empty** entry displays.

8. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
9. Select the Webtop tab.

   A list of webtops is displayed.
10. Select a webtop and click **Update**.
    The screen changes to display properties and the name of the selected webtop is displayed.
11. Select **Save** to save any changes and return to the access policy.

Citrix remote desktop resource and an Access Policy Manager® (APM®) dynamic webtop, are now assigned to the session.

Adding Citrix Smart Access actions to an access policy

To perform this task, first select the access profile you created previously, and open the associated access policy for edit.

You can set one or more filters per Citrix Smart Access action. If you include multiple Citrix Smart Access actions in an access policy, Access Policy Manager accumulates the SmartAccess filters that are set throughout the access policy operation.

1. Click the(+) icon anywhere in your access profile to which you want to add the Citrix Smart Access action item.
   The Add Item screen opens.
2. From **General Purpose**, select **Citrix Smart Access** and click **Add Item**.
   The Variable Assign: Citrix Smart Access properties screen opens.
3. Type the name of a Citrix SmartAccess filter in the open row under Assignment.

   A filter can be any string. Filters are not hardcoded, but must match filters that are configured in the XenApp™ server for application access control or a user policy.

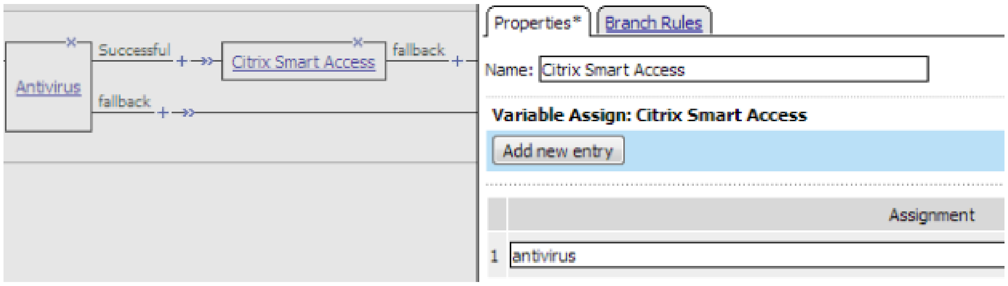
   Note: *In the XenApp server, you must specify* `APM` *as the Access Gateway farm when you configure filters.*
4. To add another filter, click **Add entry** and type the name of a Citrix filter in the open row under Assignment.
5. When you are done adding filters, click **Save** to return to the Access Policy.
6. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Example access policy with Citrix SmartAccess filters

Here is a typical example access policy that uses Citrix SmartAccess filters to restrict access to published applications based on the result of client inspection. Client inspection can be as simple as IP Geolocation Match or Antivirus. The figure shows an access policy being configured with a Citrix Smart Access action to set a filter to `antivirus` after an antivirus check is successful.



Name: Citrix Smart Access

Variable Assign: Citrix Smart Access

1 antivirus

Figure 10: Example access policy with Citrix SmartAccess action and an antivirus check

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

Note: Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   *Note: Logging is disabled when the **Selected** list is empty.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Adding a connectivity profile

Create a connectivity profile to configure client connections for Citrix remote access.

Note: A Citrix client bundle provides an installable Citrix Receiver client. The default parent connectivity profile includes a default Citrix client bundle.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.

4. From the **Parent Profile** list, select the default profile, **connectivity**.
5. To use a Citrix bundle that you have configured, select **Citrix Client Settings** from the left pane and select the bundle from the **Citrix Client Bundle** list in the right pane.

   The default Citrix client bundle is included if you do not perform this step.
6. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the Connectivity Profile List.

Adding Citrix Receiver for HTML5 to a connectivity profile

Download the Citrix Receiver for HTML5 from the Citrix website.

You add Citrix Receiver for HTML5 to a Citrix bundle and add the bundle to a connectivity profile so that APM® can deliver Citrix Receiver for HTML5 to clients.

1. From the command line, type `msiexec /a` *`filepath to MSI file`* `/qb TARGETDIR=`*`filepath to target folder`*.
2. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Citrix Client Bundles**.
   a) In the **Name** field, type a name that includes `html5`.
   b) From the **Source** list, select **Windows Package File**.
   c) Click **Choose File** and upload the file `./Citrix/HTML5 Management/HTML5Client.zip`.
3. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   a) Click the **Connectivity Profile List** tab.
   b) Select the connectivity profile you want to update.
   c) Click **Edit Profile**.
   A popup screen opens.
   d) Click **Citrix Client Settings**.
   e) From the **Citrix Client Bundle** list, select the bundle with `html5` in its name.
4. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Profile Access**.
   a) Click the checkbox next to the Access Profile that is associated with the Citrix Virtual Server.
   b) Click **OK**.

The Citrix Receiver for HTML5 is included in a bundle with a particular connectivity profile.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Creating a virtual server to support Citrix web and mobile clients

This virtual server supports Citrix traffic and responds to web and mobile client requests.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. For the **SSL Profile (Client)** setting, from the **Available** list, select an SSL profile with an SSL certificate that the clients trust, and use the Move button to move the name to the **Selected** list.
8. If access to XML Brokers requires SSL, then for the SSL Profile (Server) setting, select an SSL profile.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
12. From the **VDI Profile** list, select a VDI profile.

    You can select the default profile, **vdi**.
13. Click **Finished**.

The access policy is now associated with the virtual server.

Overview: Giving APM users time to enter a Smart Card PIN

If you have configured Access Policy Manager® for smart card authentication and your users cannot enter a PIN before the SSL handshake times out, they can experience problems such as browser failure or errors because the BIG-IP® system sends a TCP reset after the SSL handshake times out. You can mitigate this problem by increasing the handshake timeout in the client SSL profile.

Updating the handshake timeout in a Client SSL profile

By default, a client SSL profile provides a 10-second SSL handshake timeout. You might need to modify the timeout to give users more or less time for the SSL handshake to complete.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. In the Name column, click the name of the profile you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. Scroll down to **Handshake Timeout** and select the **Custom** check box.

   Additional settings become available.
5. To limit the timeout to a number of seconds, select **Specify** from the list, and type the desired number in the **seconds** field.

   In the list, the value **Indefinite** specifies that the system continue trying to establish a connection for an unlimited time. If you select **Indefinite**, the **seconds** field is no longer available.
6. Click **Update**.

Shaping Citrix Client MultiStream ICA Traffic

Overview: Shaping traffic for Citrix clients that support MultiStream ICA

Access Policy Manager® (APM®) can perform traffic shaping for Citrix clients that support MultiStream ICA. You can add the configuration required for traffic shaping to an existing integration of APM by adding a BWC Policy action to an existing access policy.

Consult Citrix documentation for the clients and client platforms that support MultiStream ICA.

About Citrix XenApp server requirements for shaping traffic with APM

To support traffic shaping for Citrix MultiStream ICA clients with Access Policy Manager® (APM®), you must meet specific configuration requirements on the Citrix XenApp server as described here.

- Citrix MultiStream ICA must be enabled.
- A Citrix Multi-Port Policy must be configured with four MultiStream ICA ports, one for each priority (high, very high, medium, and low). This example uses ports `2598-2601`.
  - CGP default port: Default port; CGP default port priority: High

    ***Note:** CGP default port is usually `2598`.*

  - CGP port1: 2799 CGP port1 priority: Very High
  - CGP port2: 2800 CGP port2 priority: Medium
  - CGP port3: 2801 CGP port3 priority: Low

When a XenApp server is configured correctly, you can use a network monitoring utility, such as `netstat`, and see that an XTE.exe process is listening on the configured ports as shown in this example.

```
C:\> netstat -abno

Active Connections

Proto  Local Address          Foreign Address        State           PID
…
TCP    0.0.0.0:2598           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2799           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2800           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2801           0.0.0.0:0              LISTENING       6416
[XTE.exe]
```

***Note:** When you change or configure a policy, it takes effect on the XenApp server after a system restart.*

Task summary

Task list

Creating a dynamic bandwidth control policy for Citrix MultiStream ICA traffic
Adding support for Citrix traffic shaping to an access policy
Verifying log settings for the access profile

Creating a dynamic bandwidth control policy for Citrix MultiStream ICA traffic

You create a dynamic bandwidth control policy to support traffic shaping for Citrix MultiStream ICA traffic on the BIG-IP® system.

1. On the Main tab, click **Acceleration** > **Bandwidth Controllers**.
2. Click **Create**.
3. In the **Name** field, type a name for the bandwidth control policy.
4. In the **Maximum Rate** field, type a number and select the unit of measure to indicate the total throughput allowed for the resource you are managing.

   The number must be in the range from `1 Mbps` to `320 Gbps`. This value is the amount of bandwidth available to all the connections going through this static policy.
5. From the **Dynamic** list, select **Enabled**.
   The screen displays additional settings.
6. In the **Maximum Rate Per User** field, type a number and select the unit of measure to indicate the most bandwidth that each user or session associated with the bandwidth control policy can use.

   The number must be in the range from `1 Mbps` to `2 Gbps`.
7. In the **Categories** field, add four categories of traffic that this bandwidth control policy manages for Citrix: very high, high, medium, and low.

   All the categories share the specified bandwidth, in accordance with the rate specified for each category.

   The category names you specify here display in the visual policy editor when you add a bandwidth control (BWC) policy action to an access policy.

   a) In the **Category Name** field, type a descriptive name for the category.
   b) In the **Max Category Rate** field, type a value to indicate the most bandwidth that this category of traffic can use, and select **%** from the list and type a percentage from `1` to `100`.
   c) Click **Add**.
   The new category displays on the **Categories** list.
   d) Repeat these steps to add the additional categories until you have defined all four required categories.
8. Click **Finished**.

The system creates a dynamic bandwidth control policy.

> You might create a policy with a maximum rate of 20 Mbps and a maximum rate per user of 10 Mbps with categories named like this: bwcVH, bwcH, bwcM, and bwcL and with maximum category rate in percent, such as 40, 30, 20, 10 accordingly.

For the bandwidth control policy to take effect, you must apply the policy to traffic, using the BWC policy action in an access policy.

Adding support for Citrix traffic shaping to an access policy

Add actions to an existing access policy to provide traffic shaping for Citrix MultiStream ICA clients.

Note: *You need to determine where to add these actions in the access policy. You might need to precede these actions with a Client Type action to determine whether these actions are appropriate to the client.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. Add a BWC Policy action:
   a) Type BWC into the search field.

      Search is not case-sensitive.

      Results are listed.
   b) Select **BWC Policy** from the results and click **Add Item**.

      A properties screen opens.
   c) From the **Dynamic Policy** list, select the dynamic bandwidth policy that you configured previously for Citrix MultiStream ICA clients.
      Lists for these properties: **Very High Citrix BWC Category**,**High Citrix BWC Category**, **Medium Citrix BWC Category**, and **Low Citrix BWC Category** include the categories configured in the selected dynamic bandwidth policy.
   d) From the **Very High Citrix BWC Category** list, select the category that corresponds to the very high setting.
   e) For each of the remaining properties: **High Citrix BWC Category**, **Medium Citrix BWC Category**, and **Low Citrix BWC Category**, select a category that corresponds to the setting.
   f) Click **Save**.
5. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
6. Type `Var` in the search field, select **Variable Assign** from the results, and click **Add Item**.

   In this Variable Assign action, you create one entry for each of the four ports that are configured in the Citrix Multi-Port Policy on the Citrix XenApp server.

   A properties screen opens.
7. Assign a variable for the CGP port that is configured with very high priority in the Multi-Port Policy on the Citrix XenApp server.
   a) Click **Add new entry**.
      An **empty** entry displays in the Assignment table.
   b) Click the **change** link next to the empty entry.
      A dialog box, where you can enter a variable and an expression, displays.
   c) In the **Custom Variable** field, type `citrix.msi_port.very_high`.
   d) In the **Custom Expression** field, type `expr {"2599"}`.

      Replace `2599` with the port number defined for the CGP port with very high priority on the Citrix XenApp server.

e) Click **Finished**.
The popup screen closes.

8. Assign a variable for the CGP port that is configured with high priority in the Multi-Port Policy on the Citrix XenApp server.
   a) Click **Add new entry** and click the **change** link next to the new empty entry that displays.
   b) In the **Custom Variable** field, type `citrix.msi_port.high`.
   c) In the **Custom Expression** field, type `expr {"2598"}`.

      Replace `2598` with the port number defined for the CGP port with high priority on the Citrix XenApp server.
   d) Click **Finished**.
   The popup screen closes.

9. Assign a variable for the CGP port that is configured with medium priority in the Multi-Port Policy on the Citrix XenApp server.
   a) Click **Add new entry** and then click the **change** link next to the new empty entry that displays.
   b) In the **Custom Variable** field, type `citrix.msi_port.mid`.
   c) In the **Custom Expression** field, type `expr {"2600"}`.

      Replace `2600` with the port number defined for the CGP port with medium priority on the on the Citrix XenApp server.
   d) Click **Finished**.
   The popup screen closes.

10. Assign a variable for the CGP port that is configured with low priority in the Multi-Port Policy on the Citrix XenApp server.
    a) Click **Add new entry** and click the **change** link next to the new empty entry that displays.
    b) In the **Custom Variable** field, type `citrix.msi_port.low`.
    c) In the **Custom Expression** field, type `expr {"2601"}`.

       Replace `2601` with the port number defined for the CGP port with low priority on the Citrix XenApp server.
    d) Click **Finished**.
    The popup screen closes.
    e) Click **Save**.
    The properties screen closes and the visual policy editor displays.

11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

Note: *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   Note: *Logging is disabled when the **Selected** list is empty.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

APM Integration with Oracle Access Manager

About integration with supported Oracle Access Manager versions

Access Policy Manager® can provide the same functionality as an Oracle 10g WebGate. Access Policy Manager native OAM integration is built on top of Oracle® 10g's latest Access Manager SDK. When you deploy Access Policy Manager with an OAM 10g or 11g server and OAM 10g WebGates, you no longer need to deploy a WebGate proxy or WebGate agent for each OAM-protected web application.

Access Policy Manager supports multiple WebGates and can function as an Authentication WebGate (when deployed with Oracle 10g server) as well as a Resource WebGate (when deployed with either Oracle 10g or 11g server).

Authentication WebGate (AWG)
The front-end agent of the OAM server that provides the interface of authentication and authorization for the user's access request to specific web resources.

Resource WebGate (RWG)
The front-end agent of protected web servers; the RWG validates the OAM session cookie (ObSSOCookie) to determine whether the user has been authenticated and can be authorized to access the requested web resources.

Although the Oracle 11g server is backward compatible with Oracle 10g WebGates, with Oracle 11g, Access Policy Manager acts in place of OAM 10g resource webgates, but cannot act as a authentication webgate. This is because a new architecture was introduced with OAM 11g in which the OAM 11g server becomes the central management point for everything including authentication, that is, the role of AWG. Refer to *Oracle® Fusion Middleware Administrator's Guide for Oracle Access Manager 11g* for a comparison of OAM 10g and 11g architectures.

Because the Oracle 11g server handles all user authentication requests, you should take steps to prevent and mitigate Layer 7 Denial of Service (DoS) and brute force attacks by installing a Web Application Firewall in front of the Oracle 11g server. BIG-IP® Application Security Manager™ can provide you with intelligent Layer 7 protection in this case. For more information, refer to *BIG-IP® Application Security Manager™: Implementations*.

How does native integration with OAM work?

You can achieve SSO functionality with OAM for HTTP/HTTPS requests passing through a virtual server to the web application. With OAM support enabled on a Local Traffic Manager™ (LTM®) virtual server, Access Policy Manager® will be the OAM policy enforcement point (PEP) on the BIG-IP® system, while the OAM server is still the policy decision point (PDP) in the overall system architecture. When a user requests access to a protected web resource, Access Policy Manager communicates with the OAM server to determine whether the user can be authenticated/authorized for the request, and enforces the policy evaluation decision (made by OAM server) on the BIG-IP device.

These figures show a typical configuration before and after OAM native integration is enabled.

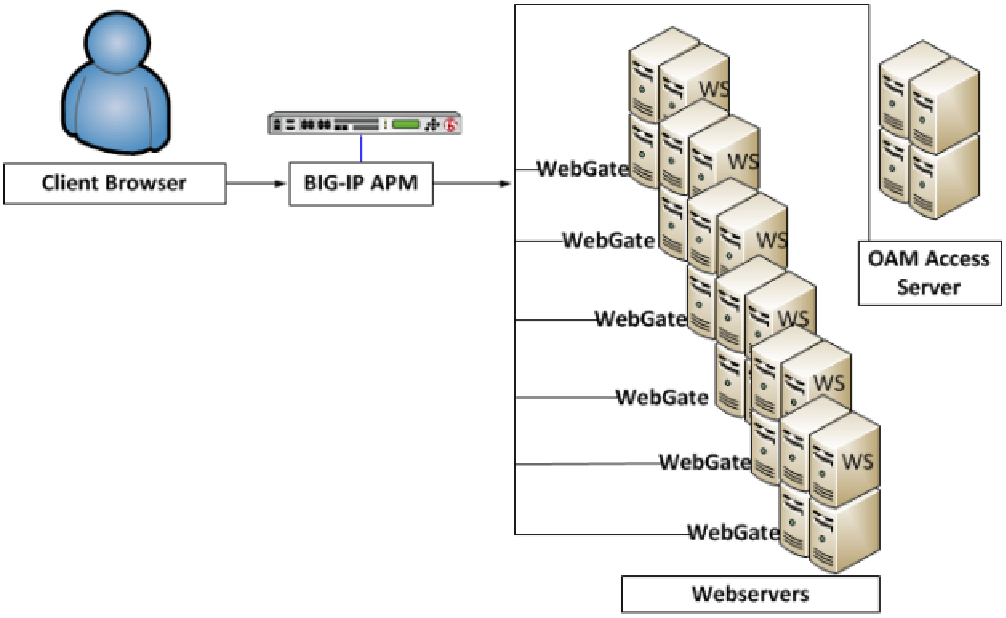


Figure 11: Typical configuration before OAM native integration is enabled on the BIG-IP system

In this figure, individual WebGates, installed on each web server, interact with the OAM Access Server.

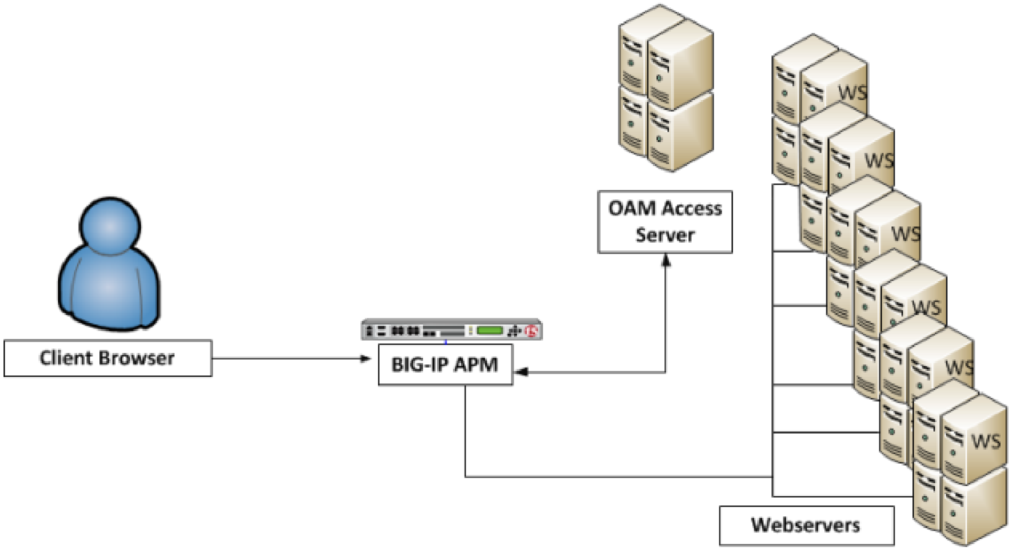


Figure 12: Typical configuration after OAM native integration is enabled on the BIG-IP system

In this figure, WebGates are no longer required on the web servers, and, even if they are installed, they are not used. Access Policy Manager acts in place of the WebGates, contacting the OAM Access Server for policy information, and enforcing the policies.

Note: *Oracle Access Manager relies on synchronized time on all Oracle Identity Management systems and BIG-IP systems. Thus, a reliable source is used on all components of a deployment. It is also recommended to use NTP servers. OAM Access Server time can be ahead of BIG-IP system time by fewer than 60 seconds, while BIG-IP system time should never be ahead of OAM Access Server time. Differences in system clocks can cause the system to reject all requests to the Identity Server.*

OAM 11g SSO integration example

Let's walk through an example deployment with Oracle 11g. You can integrate Access Policy Manager® with a Oracle 11g server whether it is configured for single sign on (SSO) single domain or SSO multi-domain. To keep this example simple, we will assume that Oracle 11g server is configured for SSO single domain. The Oracle 11g server performs all authentication. A single Resource WebGate is configured in OAM.

In Access Policy Manager on the BIG-IP® system, a AAA OAM server has been configured and includes the details of the OAM Access Server and one AccessGate. One virtual server has been configured with OAM native integration enabled. BIG-IP® Application Security Manager® (ASM) is installed in another virtual server as a web application firewall configured to prevent DoS and mitigate brute force attacks.

This figure depicts the traffic flow for the example.

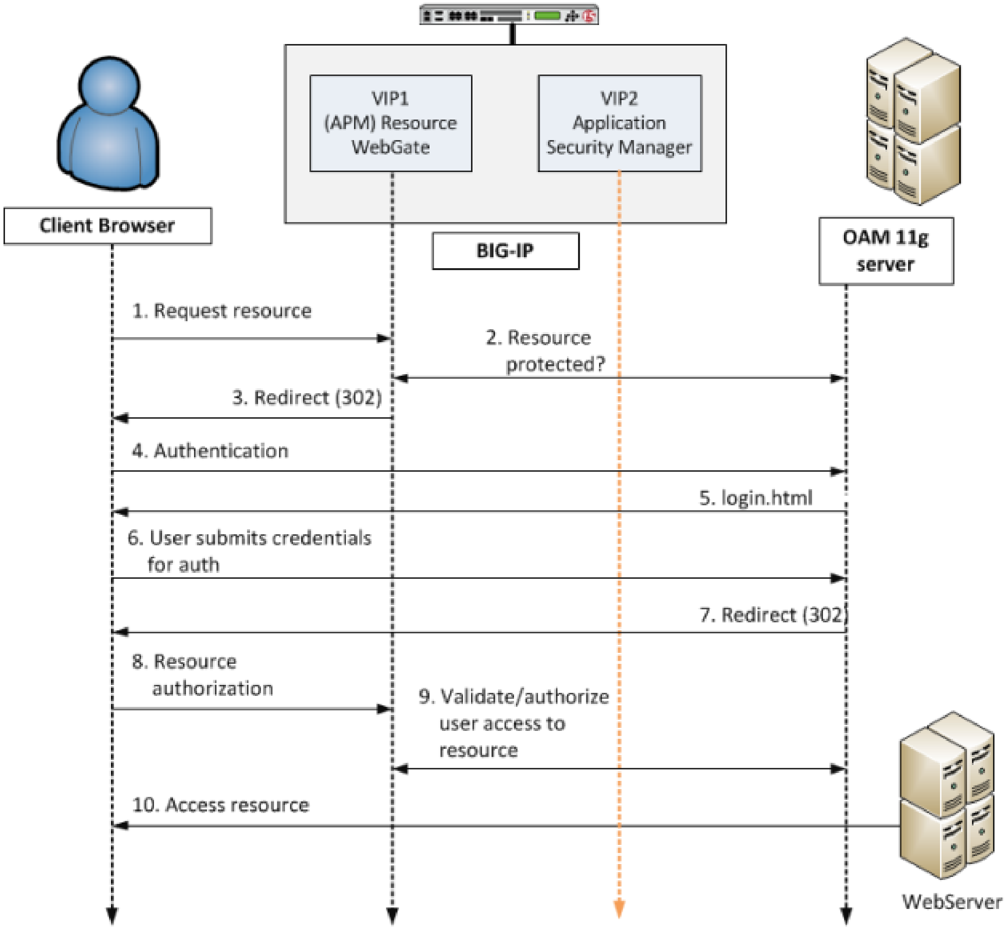


Figure 13: Accessing a protected resource using Access Policy Manager deployed with OAM 11g

1. Client requests access to a resource. The request comes to the Resource Webgate (RWG).
2. RWG checks whether the resource is protected per OAM. The resource is protected and the user has not yet authenticated.
3. RWG sends a 302 redirect to the client so that the client will be redirected to the OAM 11g server for authentication.

4. User will follow the redirect to OAM 11g server for authentication. In this example, the user has never been authenticated and form-based authentication is the authentication scheme of the OAM policy protecting the original user-requested resource.

   ***Note:** Before going to OAM, traffic is checked against security policies that are configured with anomaly protection on ASM, provided that the ASM module is enabled to protect the OAM 11g server on the BIG-IP system.*

5. OAM sends a login page to the client.
6. User submits credentials which come to OAM server where the user's credentials will be validated. In this example, it is assumed that the user submitted valid credentials.
7. After user credentials are successfully validated on the OAM 11g server, the server will send another 302 redirect, so that the user will be redirected back to the original RWG.
8. Resource request comes to RWG.
9. RWG verifies the user's original request again using the `ObSSOCookie` passed from the OAM 11g server. Upon successful authorization, the user will be allowed to access the resource.
10. The protected resource behind VIP1 will be sent back to the user.

OAM 10g SSO integration example

Let's walk through an example deployment. An Oracle 10g server is configured for SSO multi-domain; an Authentication WebGate is configured and, in another domain, a Resource WebGate is configured.

In Access Policy Manager®, an AAA OAM server has been configured and includes the details of the OAM Access Server and the two AccessGates. Two virtual servers have been configured with OAM native integration enabled.

This figure depicts the traffic flow for the example.

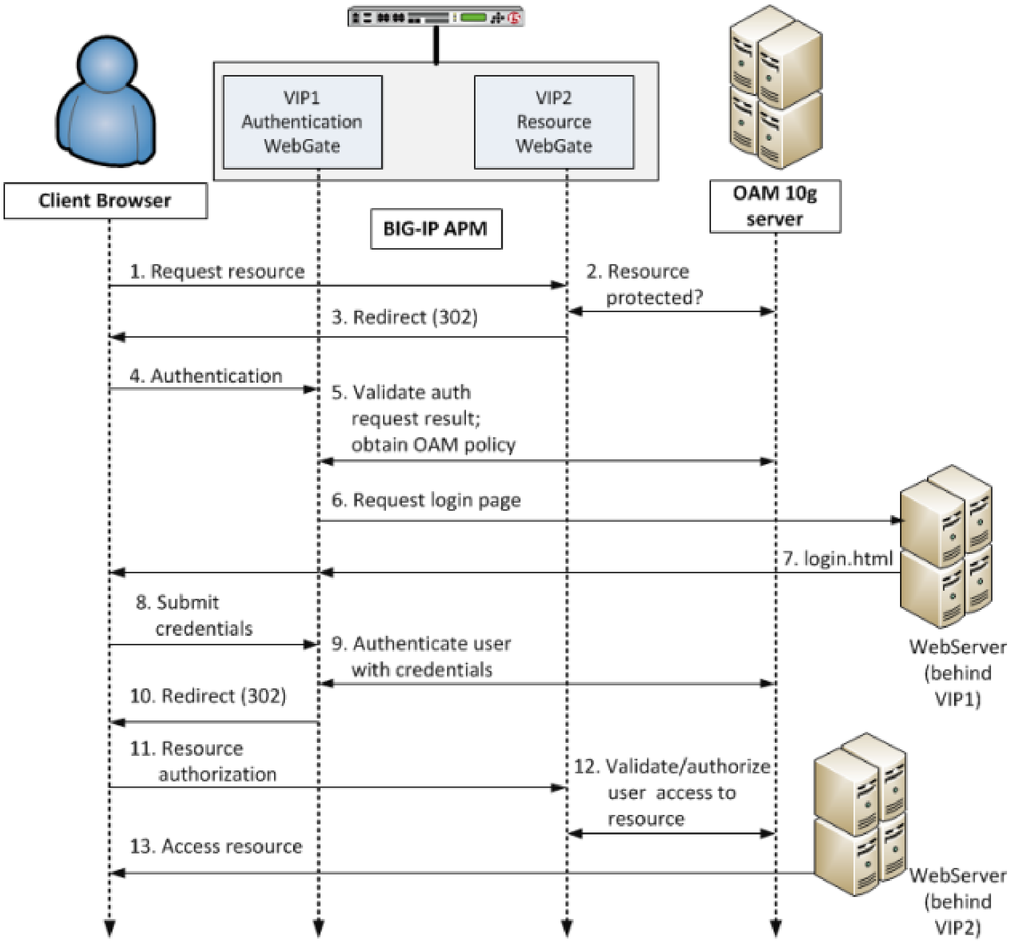


Figure 14: Accessing a protected resource via Access Policy Manager native integration with OAM 10g

1. Client requests access to a resource. The request comes to the RWG (Access Policy Manager AccessGate at VIP2).
2. RWG checks whether the resource is protected per OAM. The resource is protected and the user has not yet authenticated.
3. RWG sends a 302 redirect to the client so that the client will be redirected to the AWG for authentication.
4. Authentication request comes to the AWG (Access Policy Manager AccessGate at VIP1).
5. AWG validates user authentication status with OAM and obtains policy. In this case, the policy calls for form-based authentication and gives the location of the form.
6. For the form-based authentication scheme, AWG allows the user to access the login page hosted on a webserver behind the AWG.
7. The webserver returns the login.html file to the AWG, which sends it to the client.
8. Via login.html, the user submits credentials.
9. The AWG uses the credentials to authenticate the user with the OAM 10g server.
10. With user authentication successful, the AWG sends a 302 redirect to the client so that the client will be redirected to the original RWG.
11. Request for resource comes to the RWG again.
12. The RWG validates user access to the resource with OAM.
13. The protected resource behind VIP2 will be sent back to the user.

Integrating APM with Oracle Access Manager

About AAA OAM server configuration

You can configure only one AAA OAM server, but it can support multiple AccessGates from the same access server. When you create a AAA OAM server, its transport security mode must match the setting in the OAM access server.

Task summary for integrating Access Policy Manager with OAM

Before you begin

Before you start to integrate Access Policy Manager® with OAM, configure the Access Server and AccessGates through the Oracle Access administrative user interface. Refer to *Oracle® Access Manager Access Administration Guide* for steps.

Task list

Follow these steps to integrate Access Policy Manager with a supported OAM server.

Importing AccessGate files when transport security is set to cert
Creating an AAA OAM server
Adding AccessGates to the OAM AAA server
Creating a virtual server

Importing AccessGate files when transport security is set to cert

Check the transport security mode that is configured on the OAM access server. If transport security mode is configured to cert, copy the certificate,certificate chain, and key files (by default, `aaa_cert.pem`, `aaa_chain.pem`, and `aaa_key.pem` respectively) for each AccessGate from the OAM access server to the BIG-IP system.

Note: *If Transport Security Mode is set to open or simple, you can skip this procedure.*

You must import the certificate, certificate chain, and key files for each AccessGate into the BIG-IP system. Repeat this procedure for each AccessGate. Import certificate and certificate chain files before importing the corresponding private key file.

Note: *If a signing chain certificate (CA) is the subordinate of another Certificate Authority, both certificates, in PEM format, must be included in the file with the subordinate signer CA first, followed by the root CA, including " -----BEGIN/END CERTIFICATE-----".*

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.

2. Click the **Import** button.
3. From the **Import Type** list, select **Certificate**.
4. For the **Certificate Name** setting, select the **Create New** option, and type a unique name that enables you to identify the file as belonging to this particular AccessGate.
5. For the **Certificate Source** setting, select the **Upload File** option, and browse to the location of the certificate or the certificate chain file.

   If you kept the default filenames when you copied the files to the BIG-IP system, look for `aaa_cert.pem` or `aaa_chain.pem`.
6. Click **Import**.
   A certificate or certificate chain file has been imported for the AccessGate. To import the other (certificate or certificate chain) file for this AccessGate, repeat the steps that you have just completed before you continue.
7. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
8. Click the **Import** button.
9. From the **Import Type** list, select **Key**.
10. For the **Key Name** setting, select the **Create New** option, and type a unique name that enables you to identify the file as belonging to this particular AccessGate.

    When you import the key file, you are importing the private key that corresponds to the already imported certificate and certificate chain while renaming the file from its default name `aaa_key.pem`.
11. For the **Key Source** setting, do one of the following:
    - Select the **Upload File** option, and browse to the location of the key file.
    - Select the **Paste Text** option, and paste the key text copied from another source.
12. Click **Import**.
    The key file is imported.

Certificate, certificate chain, and key files have been imported for an AccessGate.

Repeat the procedure to import these files for any other AccessGate.

Creating an AAA OAM server

If transport security mode is configured to cert on the access server, import the certificates, keys, and CA certificate for the AccessGates into the BIG-IP system.

Create a AAA server for OAM to deploy Access Policy Manager® in place of OAM 10g WebGates.

Note: *Only one OAM server per BIG-IP system is supported. Multiple OAM 10g webgates from the same OAM server are supported.*

1. In the navigation pane, click **Access Policy** > **AAA Servers** > **Oracle Access Manager**.
   The Oracle Access Manager Server screen opens.
2. Click **Create** if no Oracle Access Manager server is defined yet,.
   The New OAM Server screen opens.
3. Type a name for the AAA OAM server.
4. For **Access Server Name**, type the name that was configured in Oracle Access System for the access server.

   For the access server name, open the OAM Access System Console and select **Access system configuration** > **Access Server Configuration**.

5. For **Access Server Hostname**, type the fully qualified DNS host name for the access server system.
6. For **Access Server Port**, accept the default `6021`, or type the port number.

   For earlier versions of OAM, the default server port is `6021`. For later versions, the default server port is `5575`.
7. For **Admin Id**, type the admin ID.

   Admin Id and Admin Password are the credentials that are used to retrieve host identifier information from OAM. Usually, these are the credentials for the administrator account of both Oracle Access Manager and Oracle Identity Manager.
8. For **Admin Password**, type the admin password.
9. For **Retry Count**, accept the default 0, or enter the number of times an AccessGate should attempt to contact the access server.
10. For **Transport Security Mode**, select the mode (open, simple, or cert) that is configured for the access server in Oracle Access System.
11. If Transport Security Mode is set to simple, type and re-type a **Global Access Protocol Passphrase**; it must match the global passphrase that is configured for the access server in OAM.
12. For **AccessGate Name**, type the name of an AccessGate; it must match the name of an AccessGate that is configured on the OAM access server.
13. For **AccessGate Password** and **Verify Password**, type the password; it must match the password that is configured for it on the OAM access server.
14. If transport security mode is set to cert, select the **Certificate**, **Key**, and **CA Certificate** that you imported for this particular AccessGate.
15. If transport security mode is set to cert and if a sign key passphrase is needed, type a **Sign Key Passphrase** and re-type it to verify it.
16. Click the **Finished** button.
    This adds the new AAA server to the AAA Servers list.

Add any other AccessGates that are configured for the OAM access server to this Oracle Access Manager AAA server. Then, for each AccessGate, configure a virtual server and enable OAM support on it for native integration with OAM.

Adding AccessGates to the OAM AAA server

You must create an Oracle Access Manager AAA server with one AccessGate before you can add other AccessGates.

Access Policy Manager can support multiple AccessGates from the same OAM access server. To enable the support, add the AccessGates to the Oracle Access Manager AAA server.

1. In the navigation pane, click **Access Policy** > **AAA Servers** > **Oracle Access Manager**.
   The Oracle Access Manager Server screen opens.
2. Click the name of the Oracle Access Manager AAA server.
   The Properties page opens.
3. Scroll down to the **AccessGate List** and click **Add**.
   The New AccessGate page opens.
4. For **AccessGate Name**, type the name of an AccessGate; it must match the name of an AccessGate that is configured on the OAM access server.
5. For **AccessGate Password** and **Verify Password**, type the password; it must match the password that is configured for it on the OAM access server.

6. If transport security mode is set to cert for the access server, select the **Certificate**,**Key**, and **CA Certificate** that you imported for this particular AccessGate.
7. If transport security mode is set to cert for the access server, and if a sign key passphrase is needed, type a **Sign Key Passphrase** and re-type it to verify it.
8. Click the **Finished** button.

The AccessGate is added.

Creating a virtual server

Configure an AAA OAM server and add AccessGates to it before you perform this task.

A virtual server represents a destination IP address for application traffic. Configure one virtual server for each AccessGate that is included on the AAA OAM server AccessGates list.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Destination Address** field, type the IP address for a host virtual server.

   The IP address you type must be available and not in the loopback network.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
4. In the **Service Port** field, type a port number or select a service name from the **Service Port** list.
5. In the Resources area of the screen, from the **Default Pool** list, select the relevant pool name.
6. Scroll down to the Access Policy section and check the **Enabled** box for OAM Support.
7. Select an AccessGate from the list.

   If you select `Default`, Access Policy Manager reads Oracle configuration information to determine which AccessGate to associate with this virtual server.
8. Click **Finished**.

A destination IP address on the Access Policy Manager® system is now available for application traffic.

Troubleshooting tips

You might run into problems with the integration of Access Policy Manager® and OAM in some instances. Follow these tips to try to resolve any issues you might encounter.

Troubleshooting tips for initial configuration

You should	Steps to take
Check network connectivity	Ping the OAM Access Server from the BIG-IP system.
Test without OAM support enabled first	Before you test with OAM support enabled, make sure that the BIG-IP system has basic connectivity to protected applications. • Disable the OAM Support property on the virtual server. • Verify that you can reach the pool and the application.

You should	Steps to take
	After succeeding, reenable OAM support on the virtual server.
Check the configuration for accuracy	• Confirm that the AAA server object is correct, particularly the OAM server section. • Confirm that the AccessGates configured on the BIG-IP system within the AAA server are correct.

Additional troubleshooting tips

You should	Steps to take
Verify access	OAM provides tools for the administrator to test how access policies respond to various requests. Use the Access Tester to test access policies with given identities and for given users. This tool can be helpful in determining whether the access provided by BIG-IP system is consistent with the policies configured under OAM.
Resolve sudden problems	Changes that have been made on the OAM server can cause mismatches on the BIG-IP system due to a configuration cache that is kept on the BIG-IP system. To resolve this problem, delete the cache configuration file of the corresponding AccessGate configuration. • Delete the config.cache file located in config/aaa/oam/<filepath>, e.g. /config/aaa/oam/Common/oamaaa1/AccessGate1/config.cache. • At the command line, restart the EAM service by typing `bigstart restart eam`.
Check logs	Enable and review the log files on the BIG-IP system. • Most relevant log items are kept in the /var/log/apm log file. This /var/log/apm log file is the primary location for messages related to the operation of OAM. • Additional logging is done in /var/log/oblog.log. This file contains AccessGate logging which might be helpful in certain circumstances.

VMware Horizon View Requirements for APM Integration

About VMware Horizon View server required settings

To integrate Access Policy Manager® with VMware Horizon View, you must meet specific configuration requirements for VMware, as described here.

SecureTunnel and PCoIP Secure Gateway disabled

Ensure that Secure Tunnel and PCoIP Secure Gateway are disabled on the VMware Horizon View server.

Blast Secure Gateway disabled

To be able to launch VMware View sessions from an APM® webtop using an HTML5 client, ensure that Blast Secure Gateway is disabled on the VMware Horizon View server.

Advanced authentication disabled

Ensure that RSA authentication and other advanced authentication types are disabled on the VMware Horizon View server.

Display a pre-login message disabled

Disable the **Display a pre-login message** setting on the VMware Horizon View server. This prevents View Connection Server from displaying another login prompt in addition to the APM logon page. Also, if the setting is enabled, remote desktop connections fail to render on the APM web top for VMWare View.

About VMware Horizon View server settings and SSL offloading

If you want to use Access Policy Manager® (APM®) to offload SSL from VMware View Horizon servers, you must configure your VMware View Horizon servers for SSL offloading. For more information, refer to the administration guide for your VMware Horizon View server and search for Off-load SSL Connections.

Note: *APM supports SSL offloading. However, it is not a requirement for integrating APM with VMware.*

Authenticating Standalone View Clients with APM

Overview: Authenticating View Clients with APM

Access Policy Manager® can present VMware View logon pages on a View Client, perform authentication, and load-balance VMware View Connection Servers. APM™ supports the PCoIP (PC over IP) display protocol for the virtual desktop.

A View Client makes connections to support different types of traffic between it and a View Connection Server. APM supports these connections with two virtual servers that share the same destination IP address. You must configure one virtual server to serve each of these purposes:

- View Client authentication and View Connection Server load-balancing
- Handle PCoIP traffic

Task summary

Creating a pool of View Connection Servers
Configuring a VMware View remote desktop resource
Configuring a full webtop
Creating an access profile
Verifying log settings for the access profile
Creating an access policy for View Client authentication
Creating a connectivity profile
Verifying the certificate on a View Connection Server
Configuring an HTTPS virtual server for View Client authentication
Configuring a UDP virtual server for PCoIP traffic
Configuring virtual servers that use a private IP address

About the iApp for VMware Horizon View integration with APM

An iApps® template is available for configuring Access Policy Manager® and Local Traffic Manager™ to integrate with VMware Horizon View. The template can be used on the BIG-IP® system to create an application service that is capable of performing complex configurations. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at `https://devcentral.f5.com/wiki/iApp.VMware-Applications.ashx`. A deployment guide is also available there.

Creating a pool of View Connection Servers

You create a pool of View Connection Servers to provide load-balancing and high-availability functions.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.

The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each View Connection Server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) In the **Service Port** field, type `443` (if your View Connection Servers use HTTPS), or type `80` (if your View Connection Servers use HTTP).

      By default, View Connection Servers use HTTPS. However, if you configure your View Connection Servers for SSL offloading, they use HTTP.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

Configure a VMware View remote desktop resource so that you can log on to a View Connection Server and gain access to a standalone View Client, or launch a View desktop from an Access Policy Manager® (APM®) webtop, depending on the access policy.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Remote Desktops List**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. For the **Type** setting, select **VMware View**.
4. For the **Destination** setting, select **Pool** and from the **Pool Name** list, select a pool of View Connection Servers that you configured previously.
5. For the **Server Side SSL** setting:
   - Select the **Enable** check box if your View Connection Servers use HTTPS (default).
   - Clear the **Enable** check box if your View Connection Servers use HTTP; that is, they are configured for SSL offloading.
6. In the Single Sign-On area, select the **Enable SSO** check box for single sign-on to a View Connection Server after logging in to APM®.

   Additional fields display. The **SSO Method** list displays **Password-based**; you must also configure credential sources.
   a) In the **Username Source** field, accept the default or type the session variable to use as the source for the SSO user name.
   b) In the **Password Source** field, accept the default or type the session variable to use as the source for the SSO user password.
   c) In the **Domain Source** field, accept the default or type the session variable to use as the source for the SSO user domain.
7. In the Customization Settings for *`language_name`* area, type a **Caption**.

   The caption is the display name of the VMware View resource on the APM full webtop.
8. Click **Finished**.

   All other parameters are optional.

This creates the VMware View remote desktop resource. To use it, you must assign it along with a full webtop in an access policy.

Configuring a full webtop

You can use a full webtop to provide web-based access to VMware View and other resources.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtops screen displays.
2. Click **Create**.
   The New Webtop screen opens.
3. In the **Name** field, type a name for the webtop.
4. From the **Type** list, select **Full**.
   The Configuration area displays with additional settings configured at default values.
5. Click **Finished**.

The webtop is now configured and appears in the webtop list.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select one these options:
   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.
   - **SSO**: Select to configure matching virtual servers for Single Sign-On (SSO).

     Note: *No access policy is associated with this type of access profile*

   - **RDG-RAP**: Select to validate connections to hosts behind APM when APM acts as a gateway for RDP clients.
   - **SWG - Explicit**: Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent**: Select to configure access using Secure Web Gateway transparent forward proxy.
   - **System Authentication**: Select to configure administrator access to the BIG-IP® system (when using APM as a pluggable authentication module).
   - **Identity Service**: Used internally to provide identity service for a supported integration. Only APM creates this type of profile.

> ***Note:*** *You can edit Identity Service profile properties.*

> ***Note:*** *Depending on licensing, you might not see all of these profile types.*

Additional settings display.

5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

> ***Note:*** *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   > ***Note:*** *Logging is disabled when the* ***Selected*** *list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Creating an access policy for View Client authentication

Before you can create this access policy, configure the AAA server (or servers) to use for authentication.

> ***Note:*** *The View Client supports authentication with Active Directory domain credentials (required) and with an RSA SecureID PIN (optional).*

Create an access policy so that a View Client can use a View desktop after logging on and authenticating with Access Policy Manager® (APM®).

1. On the Main tab, click **Access Policy** > **Access Profiles**.

The Access Profiles List screen opens.

2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `client` in the search field, select **Client Type** from the results list, and click **Add Item**.

   The Client Type action identifies clients and enables branching based on the client type.

   A properties screen opens.
5. Click **Save**.
   The properties screen closes. The visual policy editor displays the Client Type action. A VMware View branch follows it. Add the remaining actions on the VMware View branch.
6. Configure logon and authentication actions for Active Directory:

   Active Directory authentication is required.

   a) Click the (+) sign on the VMware View branch. An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on
   b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

      A properties screen displays.
   c) From the **VMware View Logon Screen Type** list, retain the default setting **Windows Password**.
   d) In the **VMware View Windows Domains** field, type domain names separated by spaces to use for Active Directory authentication.

      Type at least one domain name. These domains names are displayed on the View Client.
   e) Click **Save**.
      The properties screen closes and the visual policy editor displays.
   f) Click the plus (+) icon after the previous VMware View Logon Page action.
      A popup screen opens.
   g) On the **Authentication** tab, select **AD Auth**, and click **Add Item**.
   h) From the **Server** list, select an AAA server and click **Save**.
      The properties screen closes.
7. Assign a full webtop and the VMware View remote desktop resource that you configured previously.

   a) Click the (+) sign after the previous action.
   b) Type **adv** in the search field, select **Advanced Resource Assignment** from the results, and click **Add Item**.

      A properties screen displays.
   c) Click **Add new entry**.
      A new line is added to the list of entries.
   d) Click the **Add/Delete** link below the entry.
      The screen changes to display resources on multiple tabs.
   e) On the Remote Desktop tab, select the VMware View remote desktop resource that you configured previously.
   f) On the Webtop tab, select a full webtop and click **Update**.
      The properties screen closes and the resources you selected are displayed.
   g) Click **Save**.
      The properties screen closes and the visual policy editor displays.

8. To use RSA SecurID authentication in addition to Active Directory authentication, insert logon and authentication actions for RSA SecurID:
   a) Click the **(+)** icon anywhere in your access profile to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

   A properties screen displays.
   c) From the **VMware View Logon Screen Type** list, select **RSA SecurID**.
   d) In the **VMware View Windows Domains** field, type the domain names to use for logon.
   e) Click **Save**.
   The properties screen closes and the visual policy editor displays.
   f) Click the plus (+) icon after the previous VMware View Logon Page action.
   A popup screen opens.
   g) On the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.
   h) From the **Server** list, select the AAA server that you created previously and click **Save**.
   The properties screen closes.

9. (Optional) If you want to display a message to the user inside of the View Client (for example, a disclaimer or acceptable terms of use), this is how you do it:
   a) Click the **(+)** icon anywhere in your access profile to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

   A properties screen displays.
   c) From **VMware View Logon Screen Type**, select **Disclaimer**
   d) In the Customization area from the **Language** list, select the language for the message.
   e) In the **Disclaimer message** field, type the message to display on the logon page.
   f) Click **Save**.
   The properties screen closes and the visual policy editor displays.

   You have configured a logon page that displays a logon page with a message on a View Client.
10. On the fallback branch between the last action and **Deny**, select the **Deny** check box, click **Allow**, and click **Save**.
11. Click **Apply Access Policy**.

You have an access policy that displays at least one logon page, and authenticates a View Client against Active Directory before assigning resources to the session. At most, the policy displays three logon pages and performs two-factor authentication before assigning resources to the session.

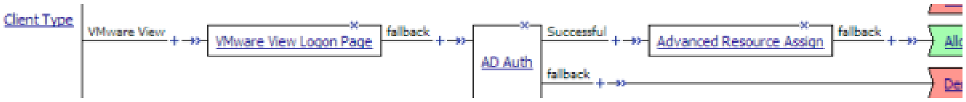


Figure 15: Example access policy with single-factor authentication for View Client

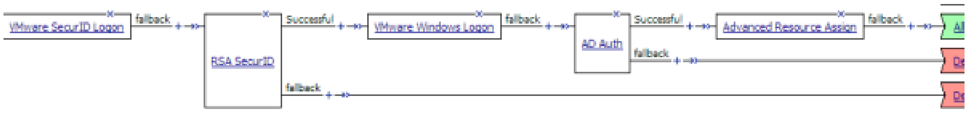


Figure 16: Example access policy with two-factor authentication for View Client

To apply this access policy to network traffic, add the access profile to a virtual server.

***Note:** To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.

   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile displays in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Verifying the certificate on a View Connection Server

Before you start, obtain the CA certificate that was used to sign the SSL certificate on View Connection Servers and obtain a Certificate Revocation List (CRL).

You install the CA certificate and CRL, then update the server SSL profile to use them only if you want the BIG-IP system to check the validity of the certificate on the View Connection Server.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
2. Click the **Import** button.
3. From the **Import Type** list, select **Certificate**.
4. For the **Certificate Name** setting, do one of the following:
   - Select the **Create New** option, and type a unique name in the field.
   - Select the **Overwrite Existing** option, and select a certificate name from the list.
5. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
6. Click **Import**.
   The SSL Certificate List screen displays. The certificate is installed.
7. Click the **Import** button.
8. From **Import Type** list, select **Certificate Revocation List**.
9. For **Certificate Revocation List Name**, type a name.
10. For **Certificate Revocation List Source**, select **Upload File** and browse to select the CRL you obtained earlier.

11. Click **Import**.
    The SSL Certificate List screen displays. The CRL is installed.
12. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
    The SSL Server profile list screen opens.
13. Click the name of the server SSL profile you created previously.
    The Properties screen displays.
14. Scroll down to the Server Authentication area.
15. From the **Server Certificate** list, select **require**.
16. From the **Trusted Certificate Authorities** list, select the name of the certificate you installed previously.
17. From the **Certificate Revocation List (CRL)** list, select the name of the CRL you installed previously.
18. Click **Update**.

The BIG-IP system is configured to check the validity of the certificate on the View Connection Server.

Configuring an HTTPS virtual server for View Client authentication

Before you start configuring an HTTPS virtual server for View Client authentication, create a connectivity profile in Access Policy Manager®. (Default settings are acceptable.)

Create this virtual server to support View Client authentication. This is the virtual server that users will specify in the View Client.

Note: *This is one of two virtual servers that you must configure for View Client connections. Use the same destination IP address for each one.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Use this same IP address for the virtual servers you create to handle PCoIP and UDP traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, in the **Available** box, select a profile name, and using the Move button, move the name to the **Selected** box.
8. For the **SSL Profile (Server)** setting, select **pcoip-default-serverssl**.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. From the **Connectivity Profile** list, select the connectivity profile.
12. From the **VDI Profile** list, select a VDI profile.

    You can select the default profile, **vdi**.
13. Locate the Resources area of the screen and from the **Default Persistence Profile** list, select one of these profiles:

    - **cookie** - This is the default cookie persistence profile. Cookie persistence is recommended.

- **source_addr** - This is the default source address translation persistence profile. Select it only when the cookie persistence type is not available.

14. Click **Finished**.

A virtual server handles View Client access and handles XML protocol data.

Configuring a UDP virtual server for PCoIP traffic

Create this virtual server to support a PC over IP (PCoIP) data channel for View Client traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address.

   Note: *Type the same IP address as the one for the View Client authentication virtual server.*

5. In the **Service Port** field, type `4172`.
6. From the **Protocol** list, select **UDP**.
7. From the **Source Address Translation** list, select **Auto Map**.
8. In the Access Policy area, from the **VDI Profile**list, select a VDI profile.

   You can select the default profile, **vdi**.
9. Click **Finished**.

This virtual server is configured to support PCoIP transport protocol traffic for VMware View Clients.

Configuring virtual servers that use a private IP address

If you configured the HTTPS and UDP virtual servers with a private IP address that is not reachable from the Internet, but instead a publicly available device (typically a firewall or a router) performs NAT for it, you need to perform these steps.

You update the access policy by assigning the variable *`view.proxy_addr`* to the IP address that the client uses to reach the virtual server. Otherwise, a View Client cannot connect when the virtual servers have a private IP address.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.
6. In the Custom Variable field, type `view.proxy_addr`.
7. In the Custom Expression field, type `expr {"`*`proxy address`*`"}` where proxy address is the IP address that the client uses to reach the virtual server.
8. Click **Finished** to save the variable and expression and return to the Variable Assign action popup screen.
9. Click **Save**.
   The properties screen closes and the visual policy editor displays.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Presenting a View Desktop on an APM Webtop

Overview: Accessing a View Desktop from an APM webtop

In this implementation, you integrate Access Policy Manager® (APM®) with View Connection Servers and present View Desktops on an APM dynamic webtop. APM authenticates to a View Connection Server and renders the View Desktops. APM load balances the View Connection Servers for high availability.

APM supports the necessary connections with two virtual servers that share the same destination IP address.

Task summary

Creating a pool of View Connection Servers
Configuring a VMware View remote desktop resource
Configuring a full webtop
Creating an access profile
Verifying log settings for the access profile
Creating an access policy for a dynamic webtop
Assigning resources to the access policy
Creating a connectivity profile
Verifying the certificate on a View Connection Server
Configuring an HTTPS virtual server for a dynamic webtop
Configuring a UDP virtual server for PCoIP traffic
Configuring virtual servers that use a private IP address

About client requirements to launch View Client from a webtop

If you want to use Access Policy Manager® (APM®) to launch a View Client from an APM webtop, you must install the standalone View Client on your client. The standalone View Client is available from VMware.

About the iApp for VMware Horizon View integration with APM

An iApps® template is available for configuring Access Policy Manager® and Local Traffic Manager™ to integrate with VMware Horizon View. The template can be used on the BIG-IP® system to create an application service that is capable of performing complex configurations. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at `https://devcentral.f5.com/wiki/iApp.VMware-Applications.ashx`. A deployment guide is also available there.

Creating a pool of View Connection Servers

You create a pool of View Connection Servers to provide load-balancing and high-availability functions.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each View Connection Server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) In the **Service Port** field, type `443` (if your View Connection Servers use HTTPS), or type `80` (if your View Connection Servers use HTTP).

      By default, View Connection Servers use HTTPS. However, if you configure your View Connection Servers for SSL offloading, they use HTTP.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

Configure a VMware View remote desktop resource so that you can log on to a View Connection Server and gain access to a standalone View Client, or launch a View desktop from an Access Policy Manager® (APM®) webtop, depending on the access policy.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Remote Desktops List**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. For the **Type** setting, select **VMware View**.
4. For the **Destination** setting, select **Pool** and from the **Pool Name** list, select a pool of View Connection Servers that you configured previously.
5. For the **Server Side SSL** setting:
   - Select the **Enable** check box if your View Connection Servers use HTTPS (default).
   - Clear the **Enable** check box if your View Connection Servers use HTTP; that is, they are configured for SSL offloading.
6. In the Single Sign-On area, select the **Enable SSO** check box for single sign-on to a View Connection Server after logging in to APM®.

   Additional fields display. The **SSO Method** list displays **Password-based**; you must also configure credential sources.
   a) In the **Username Source** field, accept the default or type the session variable to use as the source for the SSO user name.
   b) In the **Password Source** field, accept the default or type the session variable to use as the source for the SSO user password.
   c) In the **Domain Source** field, accept the default or type the session variable to use as the source for the SSO user domain.
7. In the Customization Settings for *`language_name`* area, type a **Caption**.

The caption is the display name of the VMware View resource on the APM full webtop.

8. Click **Finished**.

   All other parameters are optional.

This creates the VMware View remote desktop resource. To use it, you must assign it along with a full webtop in an access policy.

Configuring a full webtop

You can use a full webtop to provide web-based access to VMware View and other resources.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtops screen displays.
2. Click **Create**.
   The New Webtop screen opens.
3. In the **Name** field, type a name for the webtop.
4. From the **Type** list, select **Full**.
   The Configuration area displays with additional settings configured at default values.
5. Click **Finished**.

The webtop is now configured and appears in the webtop list.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select one these options:

   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.
   - **SSO**: Select to configure matching virtual servers for Single Sign-On (SSO).

     Note: *No access policy is associated with this type of access profile*

   - **RDG-RAP**: Select to validate connections to hosts behind APM when APM acts as a gateway for RDP clients.
   - **SWG - Explicit**: Select to configure access using Secure Web Gateway explicit forward proxy.

- **SWG - Transparent**: Select to configure access using Secure Web Gateway transparent forward proxy.
- **System Authentication**: Select to configure administrator access to the BIG-IP® system (when using APM as a pluggable authentication module).
- **Identity Service**: Used internally to provide identity service for a supported integration. Only APM creates this type of profile.

  ***Note:** You can edit Identity Service profile properties.*

***Note:** Depending on licensing, you might not see all of these profile types.*

Additional settings display.

5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

***Note:** Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   ***Note:** Logging is disabled when the **Selected** list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Creating an access policy for a dynamic webtop

Before you can create an access policy for an Access Policy Manager® (APM®) dynamic webtop, you must configure AAA server objects in APM to use for authentication. (You can use any type of authentication.)

***Note:** An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

Configure an access policy to authenticate a user and enable APM dynamic webtop.

***Note:** This example access policy shows how to use RSA SecurID and Active Directory authentication. However, you can use any type of authentication.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   ***Note:** Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. From the Logon Page tab, select **Logon Page**, and click **Add Item**.

   A properties screen displays.
5. Configure the Logon Page properties.

   To support Active Directory authentication only, no changes are required. To support both Active Directory and RSA SecurID authentication, an additional password field is required and the labels for the password fields require change.

   a) In the Logon Page Agent table row 3, for **Type**, select **password**.
   b) In the **Post Variable Name** field, type `password1`.
   c) In the **Session Variable Name** field, type `password1`.
   d) In the Customization Area in **Logon Page Input Field #2**, type `RSA Tokencode`.

      RSA Tokencode replaces the default label, Password.
   e) In the Customization Area in **Logon Page Input Field #3**, type `AD Password`.
   f) Click **Save**.

   The properties screen closes.

   The Logon Page is configured to display Username, RSA Tokencode, and AD Password. **Logon Page Input Field #2** accepts the RSA Tokencode into the *`session.logon.last.password`* variable (from which authentication agents read it). **Logon Page Input Field #3** saves the AD password into the *`session.logon.last.password1`* variable.
6. (Optional) To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:

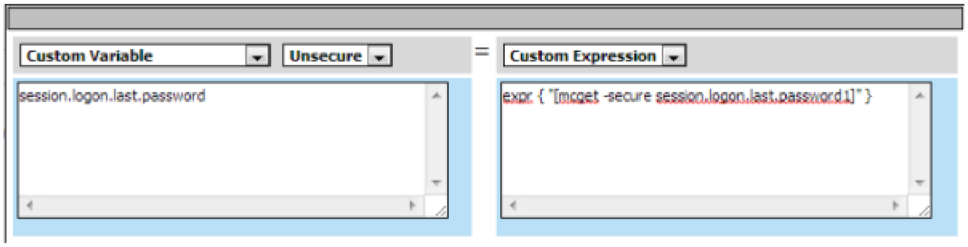
   a) From the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.
   b) In the properties screen from the **Server** list, select the AAA server that you created previously and click **Save**.
      The properties screen closes.
   c) After the RSA SecurID action, add a Variable Assign action.

      Use the Variable Assign action to move the AD password into the *`session.logon.last.password`* variable.
   d) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.

e) Click the `change` link next to the **empty** entry.
   A popup screen displays, where you can enter a variable and an expression.

f) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.password`.

g) From the right-side list, select **Custom Expression** (the default), and type `expr { "[mcget -secure session.logon.last.password1]" }`.



Custom Variable | Unsecure = Custom Expression

```
session.logon.last.password
```

```
expr { "[mcget -secure session.logon.last.password1]" }
```

   The AD password is now available for use in Active Directory authentication.

h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

7. Add the AD Auth action after one of these actions:
   - **Variable Assign** - This action is present only if you added RSA SecurID authentication.
   - **Logon Page** - Add here if you did not add RSA SecurID authentication.

   A properties screen for the AD Auth action opens.
8. Configure the properties for the AD Auth action:
   a) From the **AAA Server** list, select the AAA server that you created previously.
   b) Configure the rest of the properties as applicable to your configuration and click **Save**.
9. On the fallback path between the last action and **Deny**, click the **Deny** link, and then click **Allow** and **Save**.
10. Click **Close**.

You have an access policy that is configured to enable APM dynamic webtop after the appropriate authentication checks.

Assigning resources to the access policy

Before you start assigning resources to an access policy, open the existing access policy for edit.

Assign the full webtop and VMware View remote desktop resource that you configured previously to a session so that users can log into View Connection Servers and launch a View Desktop from the webtop.

Note: *This access policy shows how to use the Advanced Resource Assign action item to assign the resources. Alternatively, you can use the Resource Assign and Webtop, Links and Sections Assign action items.*

1. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
2. On the Assignment tab, select **Advanced Resource Assign** and click **Add Item**.
   The properties screen opens.

3. Click **Add new entry**.
   An **Empty** entry displays.
4. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
5. Select the Remote Desktop tab.

   A list of remote desktop resources is displayed.
6. Select VMware View remote desktop resources and click **Update**.
   You are returned to the properties screen where Remote Desktop and the names of the selected resources are displayed.
7. Click **Add new entry**.
   An **Empty** entry displays.
8. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
9. Select the Webtop tab.

   A list of webtops is displayed.
10. Select a webtop and click **Update**.
    The screen changes to display properties and the name of the selected webtop is displayed.
11. Select **Save** to save any changes and return to the access policy.

A VMware View remote desktop resource and an Access Policy Manager® dynamic webtop are assigned to the session when the access policy runs.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.

   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile displays in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Verifying the certificate on a View Connection Server

Before you start, obtain the CA certificate that was used to sign the SSL certificate on View Connection Servers and obtain a Certificate Revocation List (CRL).

You install the CA certificate and CRL, then update the server SSL profile to use them only if you want the BIG-IP system to check the validity of the certificate on the View Connection Server.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
2. Click the **Import** button.
3. From the **Import Type** list, select **Certificate**.
4. For the **Certificate Name** setting, do one of the following:
   - Select the **Create New** option, and type a unique name in the field.
   - Select the **Overwrite Existing** option, and select a certificate name from the list.
5. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
6. Click **Import**.
   The SSL Certificate List screen displays. The certificate is installed.
7. Click the **Import** button.
8. From **Import Type** list, select **Certificate Revocation List**.
9. For **Certificate Revocation List Name**, type a name.
10. For **Certificate Revocation List Source**, select **Upload File** and browse to select the CRL you obtained earlier.
11. Click **Import**.
    The SSL Certificate List screen displays. The CRL is installed.
12. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
    The SSL Server profile list screen opens.
13. Click the name of the server SSL profile you created previously.
    The Properties screen displays.
14. Scroll down to the Server Authentication area.
15. From the **Server Certificate** list, select **require**.
16. From the **Trusted Certificate Authorities** list, select the name of the certificate you installed previously.
17. From the **Certificate Revocation List (CRL)** list, select the name of the CRL you installed previously.
18. Click **Update**.

The BIG-IP system is configured to check the validity of the certificate on the View Connection Server.

Configuring an HTTPS virtual server for a dynamic webtop

Before configuring an HTTPS virtual server for a dynamic webtop, create a connectivity profile in Access Policy Manager®. (Default settings are acceptable.)

Create this virtual server to support launching a View Desktop from an APM® dynamic webtop. This is the virtual server that users will specify in the browser.

Note: *This is one of two virtual servers that you must configure. Use the same destination IP address for each one.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

Use this same IP address for the virtual servers you create to handle PCoIP and UDP traffic.

5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, in the **Available** box, select a profile name, and using the Move button, move the name to the **Selected** box.
8. For the **SSL Profile (Server)** setting, select **pcoip-default-serverssl**.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. From the **Connectivity Profile** list, select the connectivity profile.
12. From the **VDI Profile** list, select a VDI profile.

    You can select the default profile, **vdi**.
13. Locate the Resources area of the screen and from the **Default Persistence Profile** list, select one of these profiles:
    - **cookie** - This is the default cookie persistence profile. Cookie persistence is recommended.
    - **source_addr** - This is the default source address translation persistence profile. Select it only when the cookie persistence type is not available.
14. Click **Finished**.

This virtual server handles access and handles XML protocol data.

Configuring a UDP virtual server for PCoIP traffic

Create this virtual server to support a PC over IP (PCoIP) data channel for View Client traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address.

   Note: *Type the same IP address as the one for the View Client authentication virtual server.*
5. In the **Service Port** field, type `4172`.
6. From the **Protocol** list, select **UDP**.
7. From the **Source Address Translation** list, select **Auto Map**.
8. In the Access Policy area, from the **VDI Profile**list, select a VDI profile.

   You can select the default profile, **vdi**.
9. Click **Finished**.

This virtual server is configured to support PCoIP transport protocol traffic for VMware View Clients.

Configuring virtual servers that use a private IP address

If you configured the HTTPS and UDP virtual servers with a private IP address that is not reachable from the Internet, but instead a publicly available device (typically a firewall or a router) performs NAT for it, you need to perform these steps.

You update the access policy by assigning the variable *`view.proxy_addr`* to the IP address that the client uses to reach the virtual server. Otherwise, a View Client cannot connect when the virtual servers have a private IP address.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.
6. In the Custom Variable field, type `view.proxy_addr`.
7. In the Custom Expression field, type `expr {"`*`proxy address`*`"}` where proxy address is the IP address that the client uses to reach the virtual server.
8. Click **Finished** to save the variable and expression and return to the Variable Assign action popup screen.
9. Click **Save**.
   The properties screen closes and the visual policy editor displays.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

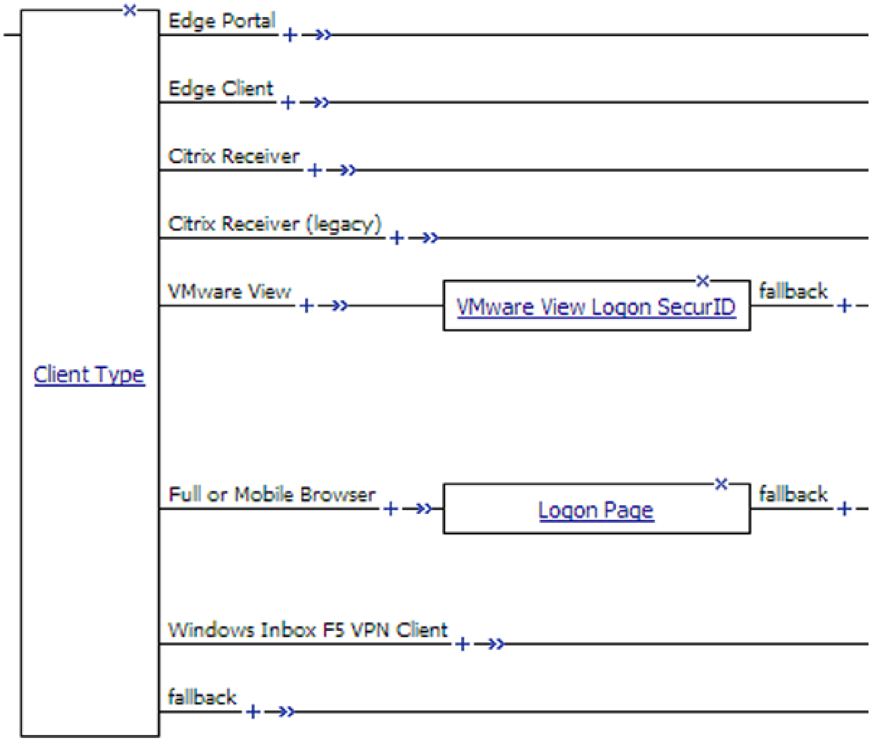
Tips for Standalone View Client and Dynamic Webtop Integration

Example access policy for standalone View Client and View on webtop

You can configure one access policy that can provide access to a standalone View Client and can launch View from a webtop depending on the client type.

Client Type action branch rules

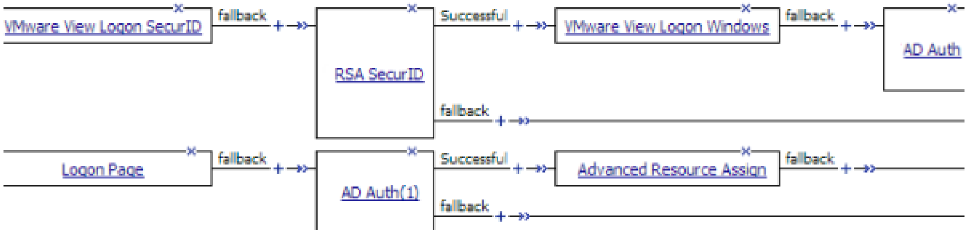
Place actions for the standalone View Client on the VMware View branch, and place actions for launching View from a dynamic webtop on the Full or Mobile Browser branch.



Example access policy continued: Logon and authentication

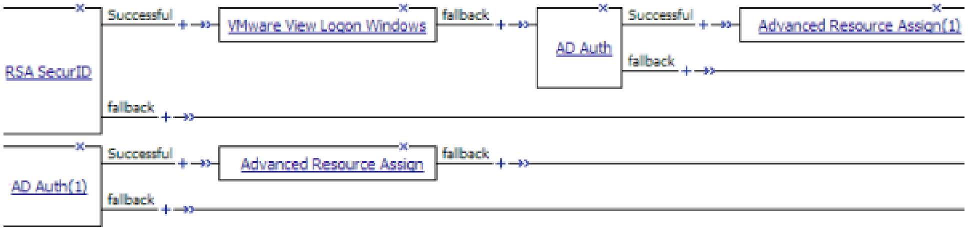
To support a standalone View Client, you must provide a VMware View Logon page and Active Directory authentication. This example shows RSA SecurID authentication followed by Active Directory (AD) authentication. (SecurID authentication is optional for a standalone View Client; it can follow or precede the AD Auth action.)

To support launching View from a webtop, you can provide a Logon Page and any authentication type. This example includes AD Auth.



Example access policy completed: Resource assignment

After successful authentication, assign resources to the session.



Note: *You might choose to configure your access policy differently. For example, you might not use SecurID authentication for a standalone View Client at all, and you might choose a different type of authentication, or multiple types of authentication, before launching View from a webtop.*

About a configuration for standalone View Client and View on webtop

When you configure Access Policy Manager® (APM®) to support standalone View Client authentication and to support launching View from a dynamic webtop, the instructions specify the same type of configuration objects for either case. You can use the same objects for both cases if you begin the access policy with the Client Type action. Then configure actions for View Client authentication on the VMware View branch and configure actions for the webtop on the Full or Mobile Browser branch.

Smart Card Authentication for VMware View Clients

Overview: Supporting smart card authentication for VMware View

On a BIG-IP® system configured as a SAML Identity Provider (IdP), APM® supports smart card authentication for VMware View Horizon Server browser-based clients and View Clients. The configuration uses SSL client certificate validation mechanisms. For a successful configuration, use these instructions and the settings specified in them.

Task summary

Creating a client SSL profile for certificate inspection
Creating a virtual server for a BIG-IP (as SAML IdP) system
Configuring IdP service for VMware View smart card SSO
Creating an access profile
Updating the Access Policy settings and resources on the virtual server
Configuring a UDP virtual server for PCoIP traffic
Configuring virtual servers that use a private IP address

About virtual servers required for View Client traffic

A View Client makes connections to support different types of traffic between it and a View Connection Server. For APM to support these connections, it requires two virtual servers that share the same destination IP address. One virtual server processes HTTPS traffic and performs authentication for the View Client. An addition virtual server processes PC over IP (PCoIP) traffic.

Creating a client SSL profile for certificate inspection

Before you start this task, import the CA certificate for VMware View Horizon server to the BIG-IP® system certificate store.

You create a custom client SSL profile to request an SSL certificate from the client at the start of the session. This enables a Client Cert Inspection item in an access policy to check whether a valid certificate was presented.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.

   The default settings for the profile specify a 10-second SSL handshake timeout. Some users with smart cards cannot authenticate within that time. You can increase the timeout if this is the case at your site.
5. From the **Configuration** list, select **Advanced**.

6. If you have VMware View clients on Mac OS X, disable TLS 1.2 in the Options List area:
   a) In the **Available Options** list, select **No TLS 1.2**.
   b) Click **Enable**.
7. If you change the values for the **Cache Size** or the **Cache Timeout** setting, do not specify a value of zero (0) for either setting.

   When these values are 0, the client must supply a PIN on each browser page refresh.
8. Scroll down to **Handshake Timeout** and select the **Custom** check box.

   Additional settings become available.
9. To limit the timeout to a number of seconds, select **Specify** from the list, and type the desired number in the **seconds** field.

   In the list, the value **Indefinite** specifies that the system continue trying to establish a connection for an unlimited time. If you select **Indefinite**, the **seconds** field is no longer available.
10. Scroll down to the Client Authentication area.
11. Select the **Custom** check box for **Client Authentication**.
    The settings become available.
12. From the **Client Certificate** list, select **request**.

    Do not select **require**.
13. From the **Trusted Certificate Authorities** and **Advertised Certificate Authorities**, select the certificates you imported previously.
14. Click **Finished**.

Creating a virtual server for a BIG-IP (as SAML IdP) system

Specify a host virtual server to use as the SAML IdP.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. For the **HTTP Profile** setting, verify that the default HTTP profile, **http**, is selected.
7. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL profile you previously created, and using the Move button, move the name to the **Selected** list.
8. For the **SSL Profile (Server)** setting, select **pcoip-default-serverssl**.
9. From the **Source Address Translation** list, select **Auto Map**.
10. Click **Finished**.

The virtual server for the BIG-IP® system configured as an IdP now appears on the Virtual Server List. The virtual server destination is available for use in the SAML IdP service configuration.

Configuring IdP service for VMware View smart card SSO

Configure a SAML Identity Provider (IdP) service for Access Policy Manager® (APM®), as a SAML IdP, to provide single sign-on authentication to VMware View clients with a smart card.

1. On the Main tab, click **Access Policy** > **SAML** > **BIG-IP as IdP**.
   The BIG-IP as IdP screen displays a list of SAML IdP services.
2. Click **Create**.
   The Create New IdP Service popup screen displays.
3. In the **IdP Service Name** field, type a unique name for the SAML IdP service.
4. In the **IdP Entity ID** field, type a unique identifier for the IdP (this BIG-IP® system).

   Typically, the ID is a URI that points to the BIG-IP virtual server that is going to act as a SAML IdP. If the entity ID is not a valid URL, the **Host** field is required.

   For example, type `https://siterequest.com/idp`, where the path points to the virtual server you use for BIG-IP system as a SAML IdP.
5. If the **IdP Entity ID** field does not contain a valid URI, you must provide one in the IdP Name Settings area:
   a) From the **Scheme** list select **https** or **http**.
   b) In the **Host** field, type a host name.
   For example, type `siterequest.com` in the **Host** field.
6. Select **SAML Profiles** from the left pane and select the **Enhanced Client or Proxy Profile (ECP)** check box.
7. To specify an artifact resolution service, click **Endpoint Settings** from the left pane and select a service from the **Artifact Resolution Service** list.

   Note: *APM does not use the artifact resolution service, but one must be included in the IdP metadata. If you leave the* ***Artifact Resolution Service*** *list blank, you can edit the IdP metadata later to add an artifact resolution service to it.*
8. Select **Assertion Settings** from the left pane.

   The applicable settings display.

   a) From the **Assertion Subject Type** list, select **Persistent Identifier**.
   b) From the **Assertion Subject Value** list, type the name of the custom session variable into which you stored the user principal name (UPN).

   You must type a percent sign (%) first and then enclose the session variable name in curly braces ({}).

   For example, type *`%{session.custom.certupn}`*.
   c) In the **Authentication Context Class Reference field**, select a URI reference that ends with **PasswordProtectedTransport**.

   The URI reference identifies an authentication context class that describes an authentication context declaration.
   d) In the **Assertion Validity (in seconds)** field type the number of seconds for which the assertion is valid.
9. From the left pane, select **SAML Attributes**.
   a) Click **Add**.
   A Create New SAML Attribute popup screen displays.
   b) In the **Name** field, type **disclaimer**.

c) Click **Add**.
Entry fields display in the table.

d) In the **Value(s)** field, type **false** and click **Update**.

This value must not be encrypted.

e) Click **OK**.
The Create New SAML Attribute popup screen closes.

The disclaimer attribute set to false is required. You can add additional attributes if needed.

10. From the left pane, select **Security Settings** and select a certificate and a key from the BIG-IP system store to use for signing the assertion.

    a) From the **Signing Key** list, select the key from the BIG-IP system store.

    None is selected by default.

    b) From the **Signing Certificate** list, select the certificate from the BIG-IP system store.

    When selected, the IdP (the BIG-IP system) publishes this certificate to the service provider so the service provider can verify the assertion. **None** is selected by default.

11. Click **OK**.
The popup screen closes. The new IdP service appears on the list.

Exporting unsigned SAML IdP metadata from APM

You need to convey the SAML Identity Provider (IdP) metadata from APM to the external service providers that use the SAML IdP service. Exporting the IdP metadata for a SAML IdP service to a file provides you with the information that you need to do this.

1. On the Main tab, click **Access Policy** > **SAML** > **BIG-IP as IdP**.
The BIG-IP as IdP screen displays a list of SAML IdP services.
2. Select a SAML IdP service from the table and click **Export Metadata**.
A popup screen opens, with **No** selected on the **Sign Metadata** list.
3. Select **OK**.
APM downloads an XML file.

An XML file that contains IdP metadata is available.

Editing the IdP metadata for VMware Horizon View

You need to edit the SAML Identity Provider (IdP) metadata XML file that you exported from APM® to make it conform to the requirements of the VMware View Connection Server (VCS).

1. Locate the IdP metadata XML file that you downloaded onto your system.
2. Use a text editor to open the file.
3. If you did not create an artifact resolution service, add a line to the file to define the service.

```
<ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://165.160.15.20:443/saml/idp/profile/soap/ars" index="0"
isDefault="true"></ArtifactResolutionService>
```

   APM does not use the artifact resolution service, but the VCS requires it.

4. Find the `<Key Descriptor>` element and copy and paste its contents.

   VCS requires two `<Key Descriptor>` elements.

5. Edit each `<Key Descriptor>` element; add `use="signing"` to one (`<KeyDescriptor use="signing">`) and `use="encryption"` to the other.

```
<KeyDescriptor use="signing">
           <ds:KeyInfo>
               <ds:X509Data>
                   <ds:X509Certificate><key_data></ds:X509Certificate>
               </ds:X509Data>
           </ds:KeyInfo>
       </KeyDescriptor>
       <KeyDescriptor use="encryption">
           <ds:KeyInfo>
               <ds:X509Data>
                   <ds:X509Certificate><key_data></ds:X509Certificate>
               </ds:X509Data>
           </ds:KeyInfo>
       </KeyDescriptor>
```

6. Save the XML file and exit the text editor.

Example edited IdP metadata file for VMware Horizon View

The metadata contains two KeyDescriptor elements, one for use in signing and one for use in encryption. It also includes an ArtifactResolutionService element.

```
 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="Ie662e22302a165c" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="https://siterequest.com/idp">
  <IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   <KeyDescriptor use="signing">
    <ds:KeyInfo>
     <ds:X509Data>
      <ds:X509Certificate>key_data</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </KeyDescriptor>
   <KeyDescriptor use="encryption">
    <ds:KeyInfo>
     <ds:X509Data>
      <ds:X509Certificate>key_data</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </KeyDescriptor>
   <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://165.160.13.20:443/saml/idp/profile/soap/ars" index="0"
isDefault="true">
   </ArtifactResolutionService>
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://siterequest.com/saml/idp/profile/post/sls"
ResponseLocation="https://siterequest.com/saml/idp/profile/post/slr"
isDefault="true">
   </SingleLogoutService>

<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>

   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://siterequest.com/saml/idp/profile/ecp/sso">
   </SingleSignOnService>
   <saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
Name="disclaimer">
   </saml:Attribute>
  </IDPSSODescriptor>
</EntityDescriptor>
```

Creating an iRule to respond with IdP metadata to a URI

You can use iRules® to respond with SAML Identity Provider (IdP) XML metadata for a particular URI.

Note: *For complete and detailed information iRules syntax, see the F5® Networks DevCentral™ web site (`http://devcentral.f5.com`).*

1. On the Main tab, click **Local Traffic** > **iRules**.
   The iRule List screen opens, displaying any existing iRules.
2. Click **Create**.
   The New iRule screen opens.
3. In the **Name** field, type a unique name for the iRule.

   The full path name of the iRule cannot exceed 255 characters.
4. In the **Definition** field, type the syntax for the iRule using Tool Command Language (Tcl) syntax.
   This example specifies a URI, `/SAAS/API/1.0/GET/metadata/`, and includes the content of the SAML IdP metadata in the response. (The example elides the metadata for brevity.)

```
when HTTP_REQUEST {
if { [HTTP::path] contains "/SAAS/API/1.0/GET/metadata/" and [HTTP::method]
 equals "GET" } {
    HTTP::respond 200 content {<?xml version="1.0" encoding="UTF-8" ?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="Ie662e22302a165c" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="https://siterequest.com/idp">
    <IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        .
        .
        .
    </IDPSSODescriptor>
</EntityDescriptor>}
    }
}
```

5. Click **Finished**.
   The new iRule appears in the list of iRules on the system.

You must add this iRule to the virtual server that processes the traffic from the SAML service provider (SP).

Establishing APM as a trusted SAML IdP for VMware Horizon View

From VMware View Connection Server (VCS), create a SAML Authenticator that points to APM® so that VCS can recognize APM as a trusted SAML Identity Provider (IdP).

1. Using the VMware software that you use to administer a VCS, create a new SAML Authenticator with these properties:
   a) For **SAML Authenticator**, type the FQDN of your virtual server.
   b) For **Metadata URL**, type the URI where VCS can get the SAML IdP metadata.

Normally, the VCS should attempt to request the metadata and verify it.

For example, type **https://sitrerequest.com/SAAS/API/1.0/GET/metadata/**, where `https://siterequest.com` is the virtual server for the SAML IdP service, and `/SAAS/API/1.0/GET/metadata/` is the URI for which the iRule on the virtual server responds with SAML IdP metadata.

2. To apply the changes after choosing a new SAML Authenticator, you must restart VCS.

Configuring a SAML SP connector for VMware VCS

Configure a SAML service provider (SP) connector with settings specified here so that APM® can recognize the VMware View Connection Server (VCS) as a supported consumer of SAML assertions.

Note: *Do not import the SAML service provider metadata file from the VCS in place of performing these steps. The metadata file does not meet the requirements for this configuration.*

1. On the Main tab, click **Access Policy** > **SAML** > **BIG-IP as IdP**.
   The BIG-IP as IdP screen displays a list of SAML IdP services.
2. On the menu bar, click **External SP Connectors**.
   A list of SAML SP connectors displays.
3. Click **Create**.
   The Create New SAML SP Connector screen opens.
4. In the **Service Provider Name** field, type a unique name for the SAML SP connector.
5. In the **SP Entity ID** field, type a unique identifier for the service provider.

   This is usually a unique URI that represents the service provider. You should obtain this value from the service provider.
6. Select **Endpoint Settings** from the left pane.

   The appropriate settings are displayed.
7. In the Assertion Consumer Services area, specify one assertion consumer service with PAOS binding.
   a) Click **Add**.
   A new row displays in the table.
   b) In the **Index** field, type the index number, zero (0) or greater.
   c) Select the **Default** check box.
   d) In the **Assertion Consumer Service URL** field, type the URL where the IdP can send an assertion to this service provider.
   e) From the **Binding** list, select **PAOS**.
   f) Click **Update**.
8. Select **Security Settings** from the left pane.
   a) Clear the **Require Signed Authentication Request** check box.
   b) Select the **Response must be signed** and **Assertion must be signed** check boxes, and then select an algorithm from the **Signing Algorithm** list.
9. Click **OK**.
   The popup screen closes.

The new SAML SP connector is available to bind to the SAML IdP service.

Binding a SAML IdP service to one SP connector

Bind a SAML Identity Provider (IdP) service and a SAML service provider (SP) connector so that the BIG-IP® system can provide authentication (SAML IdP service) to the external SAML service provider.

1. On the Main tab, click **Access Policy** > **SAML** > **BIG-IP as IdP**.
   The BIG-IP as IdP screen displays a list of SAML IdP services.
2. Select a SAML IdP service from the list.

   Select an IdP service that you configured for use with one particular SP connector only.
3. Click **Bind/Unbind SP Connectors**.
   The screen displays a list of available SAML SP connectors.
4. Select the one SAML SP connector that you want to pair with this IdP service.
5. Select **OK**.
   The screen closes.

The SAML SP connector that you selected is bound to the SAML IdP service.

Configuring a SAML resource for VMware View clients

To support users that log in using the VMware View client, you must configure a SAML resource.

1. On the Main tab, click **Access Policy** > **SAML** > **SAML Resources**.
   The SAML Resources list screen opens.
2. Click the **Create** button.
   The SAML Resource New Resource screen opens.
3. In the **Name** field, type a unique name for the SAML resource.
4. Clear the **Publish on Webtop** check box.

   You must clear the check box to support VMware View smart card authentication with this SAML resource.
5. In the Configuration area from the **SSO Configuration** list, select the SAML IdP service that is bound to the SAML SP connector with the resources you want.
6. In the **Customization Settings for English** area, and in the **Caption** field, type a caption for this SAML resource.
7. Click **Finished**.
   The SAML resource is created and associated with a SAML IdP service.

Configuring a VMware View resource for SAML SSO

Configure a VMware View remote desktop resource for SAML SSO to support smart card authentication.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Remote Desktops List**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. For the **Type** setting, select **VMware View**.
4. For the **Destination** setting, select **Pool** and from the **Pool Name** list, select a pool of View Connection Servers that you configured previously.

5. For the **Server Side SSL** setting, select the **Enable** check box.

   View Connection Servers must use HTTPS (default) to support smart card authentication.
6. In the Single Sign-On area, select the **Enable SSO** check box.

   Enable SSO to a View Connection Server after logging in to APM®.
7. From the **SSO Method** list, select **SAML**.
8. From the **SAML Resource** list, select the SAML resource that you configured previously.
9. In the Customization Settings for the `language_name` area, type a **Caption**.

   The caption is the display name of the VMware View resource on the APM full webtop.
10. Click **Finished**.

    All other parameters are optional.

This creates the VMware View remote desktop resource. To use it, you must assign it along with a full webtop in an access policy.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*
4. From the **Profile Type** list, select **All**.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Example access policy: smart card authentication for VMware View

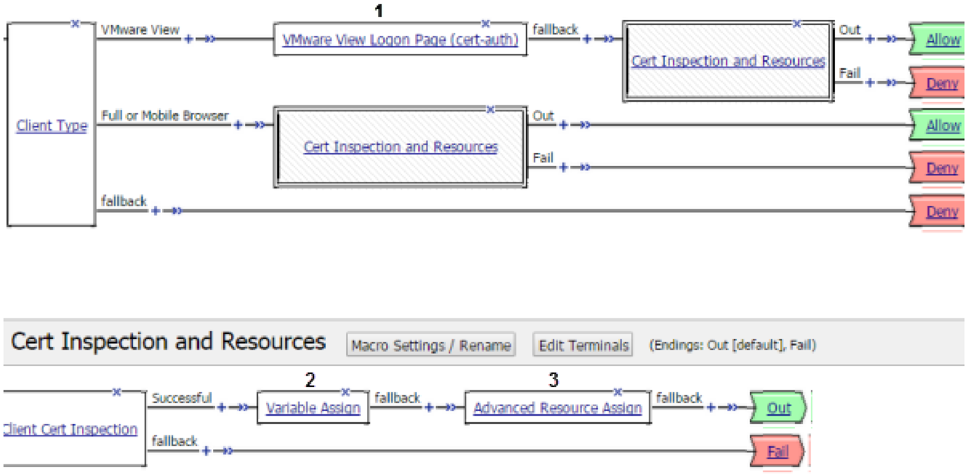


Figure 17: Access Policy requires Smart Card authentication with SAML SSO for VMware View

1	Agent properties specify **Smart Card** for **VMware View Logon Screen** property.
2	Extracts the User Principal Name from SSL certificate information and stores it in a custom session variable.
3	Assigns a full webtop and a VMware View remote desktop resource configured for SAML SSO.

Creating an access policy for VMware View smartcard authentication

Access Policy Manager® (APM®) supports this configuration when the BIG-IP® system, configured as a SAML Identity Provider (IdP), provides SSO authentication service that is consumed by a VMware View Connection Server (VCS), configured as a SAML service provider.

Create an access policy so that a VMware View client can use a smart card for authenticating with Access Policy Manager.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `client` in the search field, select **Client Type** from the results list, and click **Add Item**.

   The Client Type action identifies clients and enables branching based on the client type.

   A properties screen opens.
5. Click **Save**.

The properties screen closes. The visual policy editor displays the **Client Type** action. The **VMware View** branch applies to VMware View client access and the **Full/Mobile** branch applies to HTML-based access.

6. To accept Smart Card logon from the VMware View client, add a smart card logon screen:
   a) Add a **VMware View Logon Page** action to the policy.
   A properties screen opens.
   b) From the **VMware View Logon Screen** list, select **Smart Card**.
   c) Click **Save**.
   The properties screen closes and the visual policy editor displays.

7. Add **Client Cert Inspection** agent to the access policy on one or more branches as appropriate.

   The agent verifies the result of the SSL handshake request that occurs at the start of the session and makes SSL certificate information available to the policy.

8. Add an action to the access policy to obtain the User Principal Name (UPN) on one or more branches as appropriate.

   You might add a Variable Assign action and configure it to extract the UPN from the certificate information or configure an AD Query that retrieves the UPN.

9. After successful authentication and successful retrieval of the UPN, assign resources to the session.
   a) Click the (+) sign after the previous action.
   b) Type `adv` in the search field, select **Advanced Resource Assignment** from the results, and click **Add Item**.

      A properties screen displays.
   c) Click **Add new entry**.
   A new line is added to the list of entries.
   d) Click the **Add/Delete** link below the entry.
   The screen changes to display resources on multiple tabs.
   e) On the Remote Desktop tab, select the VMware View remote desktop resource that you configured for SAML SSO previously.
   f) On the Webtop tab, select a full webtop and click **Update**.
   The properties screen closes and the resources you selected are displayed.
   g) Click **Save**.
   The properties screen closes and the visual policy editor displays.

10. To grant access at the end of any branch, change the ending from **Deny** to **Allow**:
    a) Click **Deny**.

       The default branch ending is **Deny**.

       A popup screen opens.
    b) Select **Allow** and click **Save**.
    The popup screen closes. The **Allow** ending displays on the branch.

11. Click **Apply Access Policy**.

Depending on the access policy branches that you configured, you have an access policy that supports Smart Card authentication for a VMware View client or for a HTML-based client accessing VMware of for both.

To apply this access policy to network traffic, add the access profile to a virtual server.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Using variable assign to extract the UPN from the SSL certificate

You must supply the User Principal Name (UPN) as the Assertion Subject Value for the SAML Identity Provider (IdP) service.

Note: *This example adds a Variable Assign action to the access policy. The action uses a Tcl expression that extracts the UPN from the X509 certificate for the client and stores it in a user-defined session variable.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the **(+)** icon

   The Variable Assign action must occur after a Client Cert Inspection action runs successfully. The Variable Assign action relies on X509 information that the Client Cert Inspection action provides.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. On the left side of the variable assign properties screen, select **Custom Variable** from the list and in the field, type the name of a custom session variable.
   For example, type `session.custom.certupn`.

   Remember the session variable name; you must use it as the assertion subject value for the IdP. You will need to enter it into the IdP service configuration later.
6. On the right side of the variable assignment properties screen, select **Custom Expression** from the list and in the field, type a Tcl expression to extract the UPN from the X509 certificate as shown here.

```
foreach x [split [mcget {session.ssl.cert.x509extension}] "\n"] {
  if { [string first "othername:UPN" $x] >= 0 } {
    return [string range $x [expr { [string first "<" $x] + 1 }] [expr {
[string first ">" $x] - 1 }]];
  }
};
return "";
```

7. Click **Save**.
   The properties screen closes and the visual policy editor displays.

The Variable Assign action is added to the access policy. You probably need to configure additional actions in the access policy.

Updating the Access Policy settings and resources on the virtual server

You associate an access profile, connectivity profile, VDI profile, and an iRule with the virtual server so that Access Policy Manager® can apply them to incoming traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server that you want to update.

3. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
4. From the **Connectivity Profile** list, select a connectivity profile.
5. From the **VDI Profile** list, select a VDI profile.

   You can select the default profile, **vdi**.
6. In the Resources area, for the **iRules** setting, from the **Available** list, select the name of the iRule that you want to assign, and move the name into the **Enabled** list.
7. Click **Update**.

Your access policy and the iRule are now associated with the virtual server.

Configuring a UDP virtual server for PCoIP traffic

Create this virtual server to support a PC over IP (PCoIP) data channel for View Client traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address.

   Note: *Type the same IP address as the one for the View Client authentication virtual server.*
5. In the **Service Port** field, type `4172`.
6. From the **Protocol** list, select **UDP**.
7. From the **Source Address Translation** list, select **Auto Map**.
8. In the Access Policy area, from the **VDI Profile**list, select a VDI profile.

   You can select the default profile, **vdi**.
9. Click **Finished**.

This virtual server is configured to support PCoIP transport protocol traffic for VMware View Clients.

Configuring virtual servers that use a private IP address

If you configured the HTTPS and UDP virtual servers with a private IP address that is not reachable from the Internet, but instead a publicly available device (typically a firewall or a router) performs NAT for it, you need to perform these steps.

You update the access policy by assigning the variable *`view.proxy_addr`* to the IP address that the client uses to reach the virtual server. Otherwise, a View Client cannot connect when the virtual servers have a private IP address.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

Note: Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.

A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.
6. In the Custom Variable field, type `view.proxy_addr`.
7. In the Custom Expression field, type `expr {"`*`proxy address`*`"}` where proxy address is the IP address that the client uses to reach the virtual server.
8. Click **Finished** to save the variable and expression and return to the Variable Assign action popup screen.
9. Click **Save**.
   The properties screen closes and the visual policy editor displays.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Overview: Giving APM users time to enter a Smart Card PIN

If you have configured Access Policy Manager® for smart card authentication and your users cannot enter a PIN before the SSL handshake times out, they can experience problems such as browser failure or errors because the BIG-IP® system sends a TCP reset after the SSL handshake times out. You can mitigate this problem by increasing the handshake timeout in the client SSL profile.

Updating the handshake timeout in a Client SSL profile

By default, a client SSL profile provides a 10-second SSL handshake timeout. You might need to modify the timeout to give users more or less time for the SSL handshake to complete.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. In the Name column, click the name of the profile you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. Scroll down to **Handshake Timeout** and select the **Custom** check box.

   Additional settings become available.
5. To limit the timeout to a number of seconds, select **Specify** from the list, and type the desired number in the **seconds** field.

   In the list, the value **Indefinite** specifies that the system continue trying to establish a connection for an unlimited time. If you select **Indefinite**, the **seconds** field is no longer available.
6. Click **Update**.

Using APM as a Gateway for RDP Clients

Overview: Configuring APM as a gateway for Microsoft RDP clients

Access Policy Manager® (APM®) can act as a gateway for Microsoft RDP clients, authorizing them on initial access and authorizing access to resources that they request after that. The APM configuration includes these elements.

APM as gateway

From a configuration point of view, this is a virtual server that accepts SSL traffic from Microsoft RDP clients and is associated with an access policy that authorizes the client.

Client authorization access policy

This access policy runs when the RDP client initiates a session with the gateway (APM). Only NTLM authentication is supported. This access policy should verify that NTLM authentication is successful and must assign an additional access policy to use for resource authorization throughout the session.

Resource authorization access policy

This access policy runs when the authorized RDP client requests access to a resource. The access policy must contain logic to determine whether to allow or deny access to the target server and port.

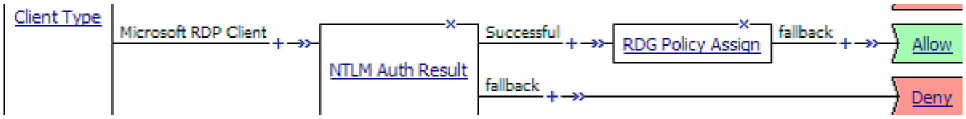


Figure 18: Sample client authorization policy

Notice the RDG Policy Assign item; it is used to specify the resource authorization policy.

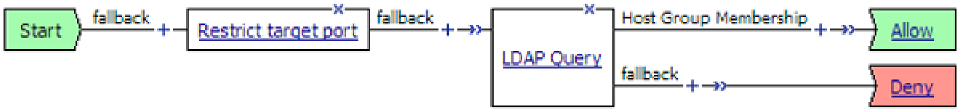


Figure 19: Sample resource authorization policy

Task summary

If you already have configured them, you can use existing configuration objects: a machine account, an NTLM authentication configuration, a VDI profile, a connectivity profile, and a client SSL profile.

Task list

Configuring an access profile for resource authorization
Verifying log settings for the access profile
Configuring an access policy for resource authorization

About supported Microsoft RDP clients

Supported Microsoft RDP clients can use APM® as a gateway. The configuration supports Microsoft RDP clients on Windows, Mac, iOS, and Android.

Refer to *BIG-IP® APM® Client Compatibility Matrix* on the AskF5™ web site at `http://support.f5.com/kb/en-us.html` for the supported platforms and operating system versions for Microsoft RDP clients.

About Microsoft RDP client configuration

Before a supported Microsoft RDP client connects to Access Policy Manager® (APM®) as a gateway for RDP clients, installation of the BIG-IP®client SSL certificate (specified in the virtual server) is required.

Note: *No APM software components are required or downloaded onto the client.*

About Microsoft RDP client login to APM

On a Microsoft RDP client, a user types in settings for a gateway and a connection. The names for the settings vary depending on the Microsoft RDP client.

RDP client gateway settings

1. Hostname setting: The hostname or IP address of the virtual server must be specified.
2. Port setting: If requested, `443` must be specified.
3. Credentials: Selection of specific logon method and entry of a user name and password should be avoided. In this implementation, APM® supports only NTLM authentication.

RDP client connection settings

Gateway setting: On some clients, you must configure a name and address for the gateway and at login type the gateway name. If requested, the gateway name must be specified as configured on the client.

1. Hostname setting: Hostname of the target server.
2. Port setting: Port on the target server.

Configuring an access profile for resource authorization

Configure an RDG-RAP type of access profile for Access Policy Manager® (APM®) before you create an access policy to authorize resource requests from Microsoft RDP clients.

Note: *After APM authorizes a Microsoft RDP client, subsequent resource requests are sent to APM.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select **RDG-RAP**.
5. Click **Finished**.
   The new access profile displays on the list.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

You must configure an access policy that determines whether to deny or allow access to a resource.

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

Note: *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   Note: *Logging is disabled when the **Selected** list is empty.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Configuring an access policy for resource authorization

Configure this access policy to perform resource authorization every time an RDP client requests access to a new resource.

Note: *The requested resource is specified in these session variables:* `session.rdg.target.host` *and* `session.rdg.target.port`*.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the RDG-RAP type access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. To restrict the target port to the RDP service only, perform these substeps:

   Note: *F5® strongly recommends this action.*

   a) In the search field, type **emp**, select **Empty** from the result list, and then click **Add Item**.
      A popup Properties screen opens.
   b) Click the Branch Rule tab.
   c) Click **Add Branch Rule**.
      A new entry with **Name** and **Expression** settings displays.
   d) In the **Name** field, replace the default name by typing a new name.

      The name appears on the branch in the access policy.
   e) Click the **change** link in the new entry.
      A popup screen opens.
   f) Click the Advanced tab.
   g) In the field, type this expression: `expr { [mcget {session.rdg.target.port}] == 3389 }`
   h) Click **Finished**.

      The popup screen closes.
   i) Click **Save**.
      The properties screen closes and the visual policy editor displays.

5. To verify group membership for the requested host, add an **LDAP Query** to the access policy and configure properties for it:

   Adding an LDAP Query is one option. The visual policy editor provides additional items that you can use to determine whether to allow the client to access the resource.

   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Type queries in the **SearchFilter** field.

This query matches hosts with the fully qualified domain name (FQDN) of the host. `(DNSHostName=%{session.rdg.target.host})` When clients request a connection, they must specify the FQDN.
This query matches hosts with the host name or with the FQDN of the host. `(|(name=%{session.rdg.target.host})(DNSHostName=%{session.rdg.target.host}))` When clients request a connection, they can specify a host name or an FQDN.

c) Click **Save**.
The properties screen closes and the visual policy editor displays.

6. To verify that the target host is a member of an Active Directory group, add a branch rule to the LDAP query item:
   a) In the visual policy editor, click the **LDAP Query** item that you want to update.
   A popup Properties screen displays.
   b) Click the Branch Rules tab, click **Add Branch Rule**, and type a descriptive name for the branch in the **Name** field.
   c) Click the **change** link in the new entry.
   A popup screen displays.
   d) Click the Advanced tab.
   e) Type an expression in the field.
   This expression matches the last LDAP memberOf attribute with an Active Directory group, *RDTestGroup*. `expr { [mcget {session.ldap.last.attr.memberOf}] contains "CN=`*`RDTestGroup`*`" }` The hypothetical members of the group in this example are the hosts to which access is allowed.
   f) Click **Finished**.

   The popup screen closes.
   g) Click **Save**.
   The properties screen closes and the visual policy editor displays.

7. Click **Save**.
The properties screen closes and the visual policy editor displays.
8. Add any other items to the access policy and change any appropriate branch ending to **Allow**.
9. Click **Apply Access Policy** to save your configuration.

Important: *Do not specify this access policy in a virtual server definition. Select it from an RDG Policy Assign item in an access policy that authorizes Microsoft RDP clients.*

Creating an access profile for RDP client authorization

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.
2. Click **Create**.
The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select one of these options.
   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.

   Additional settings display.
5. Select the **Custom** check box.
6. In the **Access Policy Timeout** field, type the number of seconds that should pass before the access profile times out because of inactivity.

   The timeout needs to be at least 15 minutes long because an RDP client sends a keepalive to the gateway every 15 minutes.

   Important: *To prevent a timeout, type `0` to set no timeout or type `900` or greater. 900 indicates a 15-minute timeout, which is enough time for the keepalive to prevent the timeout.*
7. Click **Finished**.

Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

Note: *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   Note: *Logging is disabled when the **Selected** list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Configuring an access policy for an RDP client

Configure an access policy to authorize Microsoft RDP clients and to specify the access policy that APM® should use to authorize access to resources as the client requests them.

***Note:** NTLM authentication occurs before an access policy runs. If NTLM authentication fails, an error displays and the access policy does not run.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.

   ***Note:** Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. (Optional) Type `client` in the search field, select **Client Type** from the results list, and click **Add Item**.

   The Client Type action identifies clients and enables branching based on the client type.

   A properties screen opens.
5. Click **Save**.
   The properties screen closes; the **Client Type** item displays in the visual policy editor with a **Microsoft Client RDP** branch and branches for other client types.
6. On an access policy branch, click the **(+)** icon to add an item to the access policy.
7. To verify the result of client authentication:
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result**.
   c) Click **Add Item**.

   A properties screen opens.
8. Click **Save**.
   The properties screen closes and the visual policy editor displays.
9. Select the RDG-RAP access policy you configured earlier:
   a) Click the **[+]** sign on the successful branch after the authentication action.
   b) Type `RDG` in the search field.
   c) Select **RDG Policy Assign** and click **Add Item**.
   d) To display available policies, click the **Add/Delete** link.
   e) Select a policy and click **Save**.

   Without an RDG policy, APM denies access to each resource request.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

***Note:** To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Configuring a machine account

You configure a machine account so that Access Policy Manager® (APM®) can establish a secure channel to a domain controller.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   A new Machine Account screen opens.
2. In the Configuration area, in the **Machine Account Name** field, type a name.
3. In the **Domain FQDN** field, type the fully qualified domain name (FQDN) for the domain that you want the machine account to join.
4. (Optional) In the **Domain Controller FQDN** field, type the FQDN for a domain controller.
5. In the **Admin User** field, type the name of a user who has administrator privilege.
6. In the **Admin Password** field, type the password for the admin user.

   APM uses these credentials to create the machine account on the domain controller. However, APM does not store the credentials and you do not need them to update an existing machine account configuration later.
7. Click **Join**.

This creates a machine account and joins it to the specified domain. This also creates a non-editable **NetBIOS Domain Name** field that is automatically populated.

Note: *If the **NetBIOS Domain Name** field on the machine account is empty, delete the configuration and recreate it. The field populates.*

Creating an NTLM Auth configuration

Create an NTLM Auth configuration to specify the domain controllers that a machine account can use to log in.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **NTLM Auth Configuration**.
   A new NTLM Auth Configuration screen opens.
2. In the **Name** field, type a name.
3. From the **Machine Account Name** list, select the machine account configuration to which this NTLM Auth configuration applies.

   You can assign the same machine account to multiple NTLM authentication configurations.
4. For each domain controller, type a fully qualified domain name (FQDN) and click **Add**.

   Note: *You should add only domain controllers that belong to one domain.*

   By specifying more than one domain controller, you enable high availability. If the first domain controller on the list is not available, Access Policy Manager® tries the next domain controller on the list, successively.
5. Click **Finished**.

This specifies the domain controllers that a machine account can use to log in.

Maintaining a machine account

In some networks, administrators run scripts to find and delete outdated machine accounts on the domain controllers. To keep the machine account up-to-date, you can renew the password periodically.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   The Machine Account screen opens.

2. Click the name of a machine account.
   The properties screen opens and displays the date and time of the last update to the machine account password.
3. Click the **Renew Machine Password** button.
   The screen refreshes and displays the updated date and time.

This changes the machine account last modified time.

Configuring a VDI profile

Configure a VDI profile to specify NTLM authentication for Microsoft RDP clients that use APM® as a gateway.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **VDI Profiles**.
   The VDI Profiles list opens.
2. Click **Create**.
   A popup screen opens with **General Information** selected in the left pane and settings displayed in the right pane.
3. In the **Profile Name** field, type a name.
4. From the **Parent Profile** field, select an existing VDI profile.

   A VDI profile inherits properties from the parent profile. You can override them in this profile.
5. In the left pane, click **MSRDP Settings**.
   Settings in the right pane change.
6. From the **MSRDP NTLM Configuration** list, select an NTLM authentication configuration.
7. Click **OK**.
   The popup screen closes.

The VDI profile displays on the screen.

To apply the VDI profile, you must specify it in a virtual server.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.

   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile displays in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Creating a custom Client SSL profile

You create a custom Client SSL profile when you want the BIG-IP® system to terminate client-side SSL traffic for the purpose of:

- Authenticating and decrypting ingress client-side SSL traffic
- Re-encrypting egress client-side traffic

By terminating client-side SSL traffic, the BIG-IP system offloads these authentication and decryption/encryption functions from the destination server.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select **clientssl** in the **Parent Profile** list.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. Select the **Custom** check box for **Client Authentication**.
   The settings become available.
8. From the **Configuration** list, select **Advanced**.
9. Modify the settings, as required.
10. Click **Finished**.

Creating a virtual server for SSL traffic

Define a virtual server to process SSL traffic from Microsoft RDP clients that use APM® as a gateway.

***Note:** Users must specify the IP address of this virtual server as the gateway or RDG gateway from the RDP client that they use.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
5. For the **Service Port**, do one of the following:
   - Type `443` in the field.
   - Select **HTTPS** from the list.
6. In the **SSL Profile (Client)** list, select an SSL profile.
7. In the Access Policy area, from the **Access Profile** list, select the access profile for RDP client authorization that you configured earlier.

8. From the **Connectivity Profile** list, select a profile.
9. From the **VDI Profile** list, select the VDI profile you configured earlier.
10. Click **Finished**.

Implementation result

Supported Microsoft RDP clients can specify a virtual server on the BIG-IP® system to use as a remote desktop gateway. Access Policy Manager® (APM®) can authorize the clients and authorize access to target servers as the clients request them.

Overview: Processing RDP traffic on a device with SWG

If you configure Access Policy Manager® APM® as a gateway for RDP clients and configure Secure Web Gateway (SWG) explicit forward proxy on the same BIG-IP® system, you need to complete an additional configuration step to ensure that APM can process the RDP client traffic. The recommended SWG configuration for explicit forward proxy includes a catch-all virtual server, which listens on all IP addresses and all ports, on an HTTP tunnel interface.

When a programmatic API queries listeners for a specific IP and port, the query covers all interfaces and tunnels. As a result, the catch-all virtual server will always match. Sending traffic using this tunnel results in all packets being dropped because this virtual server is configured as a reject type of virtual server.

To prevent RDP client traffic from being dropped, add an additional wildcard port-specific virtual server on the HTTP tunnel interface.

Note: *Removing the catch-all virtual server from the HTTP tunnel interface is not recommended because doing so is counterproductive for security.*

About wildcard virtual servers on the HTTP tunnel interface

In the recommended Secure Web Gateway explicit forward proxy configuration, client browsers point to a forward proxy server that establishes a tunnel for SSL traffic. Additional wildcard virtual servers listen on the HTTP tunnel interface. The listener that best matches the web traffic directed to the forward proxy server handles the traffic.

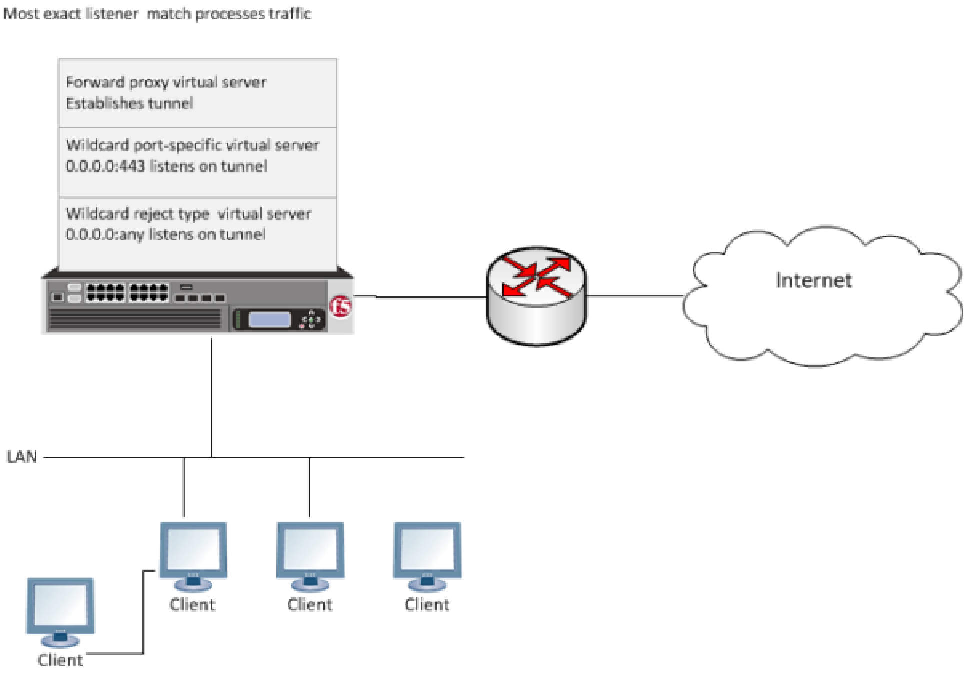

Most exact listener match processes traffic
Forward proxy virtual server
Establishes tunnel
Wildcard port-specific virtual server
0.0.0.0:443 listens on tunnel
Wildcard reject type virtual server
0.0.0.0:any listens on tunnel
Internet
LAN
Client
Client
Client
Client

Figure 20: Explicit forward proxy configuration

Creating a virtual server for RDP client traffic

You specify a port-specific wildcard virtual server to match RDP client traffic on the HTTP tunnel interface for the Secure Web Gateway (SWG) explicit forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `3389`.
6. From the **Configuration** list, select **Advanced**.
7. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
8. For the **VLANs and Tunnels** setting, move the HTTP tunnel interface used in the SWG explicit forward proxy configuration to the **Selected** list.

   The default tunnel is **http-tunnel**.

   This must be the same tunnel specified in the HTTP profile for the virtual server for forward proxy.
9. For the **Address Translation** setting, clear the **Enabled** check box.
10. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Configuring AAA Servers in APM

About VMware View and APM authentication types

You can authenticate View Clients in Access Policy Manager® (APM®) using the types of authentication that View Clients support: Active Directory authentication (required) and RSA SecurID authentication (optional). APM supports these authentication types with AAA servers that you configure in APM.

For more information, refer to *BIG-IP® Access Policy Manager®: Authentication and Single-Sign On* at `http://support.f5.com`.

Task summary

You need at least one AAA Active Directory server object in APM to support AD authentication for VMware View. If you also want to collect RSA PINs, you need at least one AAA SecurID server object in APM.

Task list

Configuring an Active Directory AAA server
Configuring a SecurID AAA server in APM

Configuring an Active Directory AAA server

You configure an Active Directory AAA server in Access Policy Manager® (APM®) to specify domain controllers for APM to use for authenticating users.

1. On the Main tab, click **Access Policy** > **AAA Servers** > **Active Directory**.
   The Active Directory Servers list screen opens.
2. Click **Create**.
   The New Server properties screen opens.
3. In the **Name** field, type a unique name for the authentication server.
4. In the **Domain Name** field, type the name of the Windows domain.
5. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
6. If you selected **Direct**, type a name in the **Domain Controller** field.
7. If you selected **Use Pool**, configure the pool:
   a) Type a name in the **Domain Controller Pool Name** field.
   b) Specify the **Domain Controllers** in the pool by typing the IP address and host name for each, and clicking the **Add** button.

c) To monitor the health of the AAA server, you have the option of selecting a health monitor: only the **gateway_icmp** monitor is appropriate in this case; you can select it from the **Server Pool Monitor** list.

8. In the **Admin Name** field, type a case-sensitive name for an administrator who has Active Directory administrative permissions.

   An administrator name and password are required for an AD Query access policy item to succeed when it includes particular options. Credentials are required when a query includes an option to fetch a primary group (or nested groups), to prompt a user to change password, or to perform a complexity check for password reset.
9. In the **Admin Password** field, type the administrator password associated with the Domain Name.
10. In the **Verify Admin Password** field, retype the administrator password associated with the **Domain Name** setting.
11. In the **Group Cache Lifetime** field, type the number of days.

    The default lifetime is 30 days.
12. In the **Password Security Object Cache Lifetime** field, type the number of days.

    The default lifetime is 30 days.
13. From the **Kerberos Preauthentication Encryption Type** list, select an encryption type.

    The default is **None**. If you specify an encryption type, the BIG-IP® system includes Kerberos preauthentication data within the first authentication service request (AS-REQ) packet.
14. In the **Timeout** field, type a timeout interval (in seconds) for the AAA server. (This setting is optional.)
15. Click **Finished**.
    The new server displays on the list.

This adds the new Active Directory server to the Active Directory Servers list.

Configuring a SecurID AAA server in APM

Configure a SecurID AAA server for Access Policy Manager® (APM®) to request RSA SecurID authentication from an RSA Manager authentication server.

1. On the Main tab, click **Access Policy** > **AAA Servers**.
   The AAA Servers list screen opens.
2. On the menu bar, click **AAA Servers By Type**, and select **SecurID**.
   The SecurID screen opens and displays the servers list.
3. Click **Create**.
   The New Server properties screen opens.
4. In the **Name** field, type a unique name for the authentication server.
5. In the Configuration area, for the **Agent Host IP Address (must match the IP address in SecurID Configuration File)** setting, select an option as appropriate:

   - **Select from Self IP List**: Choose this when there is no NAT device between APM and the RSA Authentication Manager. Select an IP from the list of those configured on the BIG-IP® system (in the Network area of the Configuration utility).
   - **Other**: Choose this when there is a NAT device in the network path between Access Policy Manager and the RSA Authentication Manager server. If selected, type the address as translated by the NAT device.

> ***Note:*** *This setting does not change the source IP address of the packets that are sent to the RSA SecurID server. (Layer 3 source addresses remain unchanged.) The agent host IP address is used only in Layer 7 (application layer) information that is sent to the RSA SecurID server.*

6. For the **SecurID Configuration File** setting, browse to upload the `sdconf.rec` file.

   Consult your RSA Authentication Manager administrator to generate this file for you.
7. Click **Finished**.
   The new server displays on the list.

This adds a new RSA SecurID server to the AAA Servers list.

Webtop Sections

Overview: Organizing resources on a full webtop

At your option, you can override the default display for resources on a full webtop by organizing resources into user-defined sections. A *webtop section* specifies a caption, a list of resources that can be included in the section, and a display order for the resources. The order in which to display webtop sections is also configurable.

Task summary

Creating a webtop section
Specifying resources for a webtop section

About the default order of resources on a full webtop

By default, resources display on a webtop in these sections: Applications and Links, and Network Access. Within the sections, resources display in alphabetical order.

Creating a webtop section

Create a webtop section to specify a caption to display on a full webtop for a list of resources. Specify the order of the webtop section relative to other webtop sections.

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Sections**.
   The Webtop Sections screen displays.
2. In the **Name** field, type a name for the webtop section.
3. From the **Display Order** list, select one the options.

   Specify the display order of this webtop section relative to others on the webtop.

   - **First**: Places this webtop section first.
   - **After**: When selected, an additional list displays; select a webtop section from it to place this webtop section after it in order.
   - **Specify**: When selected, an additional field displays. Type an integer in it to specify the absolute order for this webtop section.
4. From the **Initial State** list, select the initial display state:
   - **Expanded**: Displays the webtop section with the resource list expanded.
   - **Collapsed**: Displays the webtop section with the resource list collapsed.
5. Click **Finished**.

The webtop section is created.

Specify resources for this webtop section.

Specifying resources for a webtop section

Specify the resources to display in a webtop section.

Note: *When these resources are assigned to a session along with the webtop section, they display in the section on the webtop.*

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Sections**.
   The Webtop Sections screen displays.
2. In the table, click the name of the webtop section that you want to update.
   The Properties screen displays.
3. Repeat these steps until you have added all the resources that you require:
   a) Click **Add**.
      A properties screen displays the list of resources.
   b) Locate the appropriate resources, select them, and click **Update**.
      The Webtop Sections screen displays.

Webtop sections can be assigned in an access policy using Webtop, Links and Sections, or Advanced Resource Assign actions.

Logging and Reporting

Overview: Configuring remote high-speed APM and SWG event logging

You can configure the BIG-IP® system to log information about Access Policy Manager® (APM®) and Secure Web Gateway events and send the log messages to remote high-speed log servers.

When configuring remote high-speed logging of events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Log Setting	Add event logging for the APM system and configure log levels for it or add logging for URL filter events, or both. Settings include the specification of up to two log publishers: one for access system logging and one for URL request logging.
Access profile	Add log settings to the access profile. The log settings for the access profile control logging for the traffic that comes through the virtual server to which the access profile is assigned.

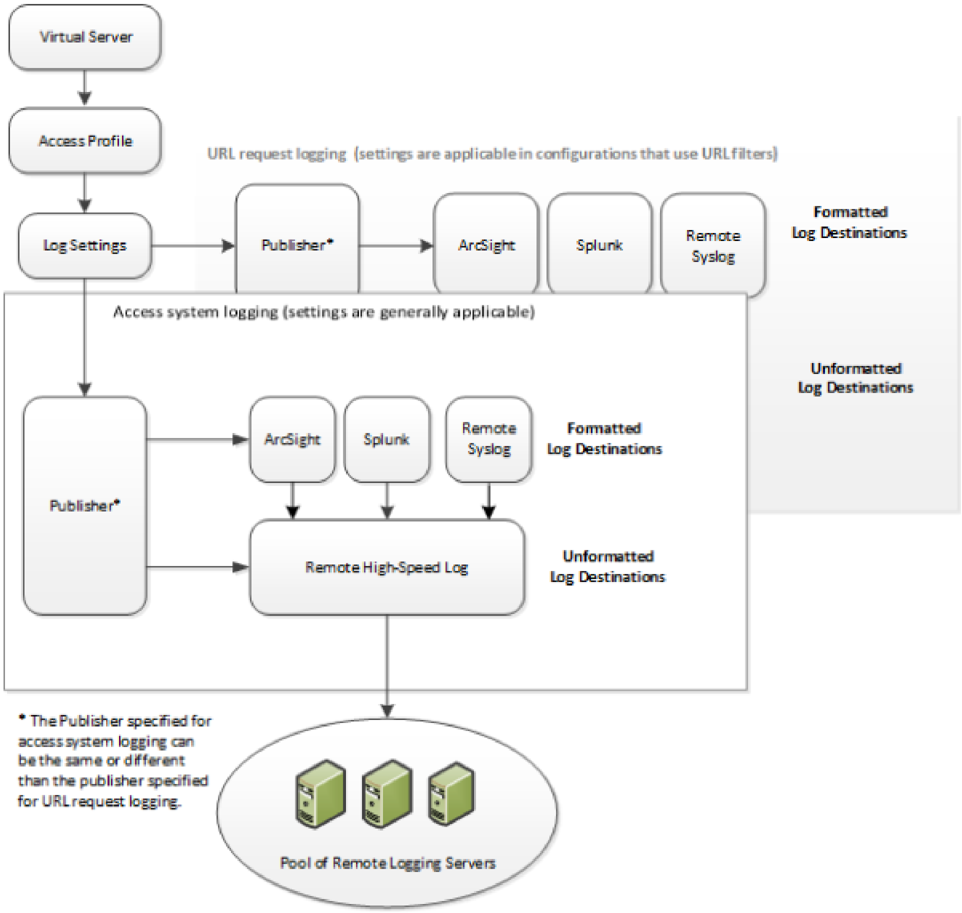

Virtual Server
Access Profile
Log Settings
URL request logging (settings are applicable in configurations that use URL filters)
Publisher*
ArcSight
Splunk
Remote Syslog
Formatted Log Destinations
Unformatted Log Destinations
Access system logging (settings are generally applicable)
Publisher*
ArcSight
Splunk
Remote Syslog
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destinations
* The Publisher specified for access system logging can be the same or different than the publisher specified for URL request logging.
Pool of Remote Logging Servers

Figure 21: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed APM and SWG event logging on the BIG-IP system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Task list

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Configuring log settings for access system and URL request events
Disabling logging

About the default-log-setting

Access Policy Manager® (APM®) provides a default-log-setting. When you create an access profile, the default-log-setting is automatically assigned to it. The default-log-setting can be retained, removed, or replaced for the access profile. The default-log-setting is applied to user sessions only when it is assigned to an access profile.

Regardless of whether it is assigned to an access profile, the default-log-setting applies to APM processes that run outside of a user session. Specifically, on a BIG-IP® system with an SWG subscription, the default-log-setting applies to URL database updates.

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port `514`.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.

7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **Remote Syslog**, **Splunk**, or **ArcSight**.

   The Splunk format is a predefined format of key value pairs.

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*
6. If you selected **Splunk** from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.

   The Splunk format is a predefined format of key value pairs.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*
5. Click **Finished**.

Configuring log settings for access system and URL request events

Create log settings to enable event logging for access system events or URL filtering events or both. Log settings specify how to process event logs for the traffic that passes through a virtual server with a particular access profile.

1. On the Main tab, click **Access Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
2. Select a log setting and click **Edit** or click **Create** for a new APM® log setting.
   A popup screen opens with General Information selected in the left pane.
3. For a new log setting, in the **Name** field, type a name.
4. To specify logging, select one or both of these check box options:
   - **Enable access system logs** - This setting is generally applicable. It applies to access policies, per-request policies, Secure Web Gateway processes, and so on. When you select this check box, **Access System Logs** becomes available in the left pane.
   - **Enable URL request logs** - This setting is applicable for logging URL requests when you have set up a BIG-IP® system configuration to categorize and filter URLs. When you select this check box, **URL Request Logs** becomes available in the left pane.

   Important: *When you clear either of these check boxes and save your change, you are not only disabling that type of logging, but any changes you made to the settings are also removed.*
5. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
6. For access system logging, from the **Log Publisher** list select the log publisher of your choice.

   A log publisher specifies one or more logging destinations.

   Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*
7. For access system logging, retain the default minimum log level, **Notice**, for each option.

   You can change the minimum log level, but **Notice** is recommended.

Option	Description
Access Policy	Events that occur while an access policy runs.
Per-Request Policy	Events that occur while a per-request policy runs.
ACL	Events that occur while applying APM access control lists.
SSO	Events that occur during single-sign on.
Secure Web Gateway	Events that occur during URL categorization on a BIG-IP® system with an SWG subscription.
ECA	Events that occur during NTLM authentication for Microsoft Exchange clients.

8. To configure settings for URL request logging, select **URl Request Logs** from the left pane.
   URL Request Settings settings display in the right panel.
9. For URL request logging, from the **Log Publisher** list, select the log publisher of your choice.

   A log publisher specifies one or more logging destinations.

Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

10. To log URL requests, you must select at least one check box option:

    - **Log Allowed Events** - When selected, user requests for allowed URLs are logged.
    - **Log Blocked Events** - When selected, user requests for blocked URLs are logged.

    Whether a URL is allowed or blocked depends on both the URL category into which it falls, and the URL filter that is applied to the request in the per-request policy.

11. (Optional) To assign this log setting to multiple access profiles now, perform these substeps:

    Note: *Up to three log settings for access system logs can be assigned to an access profile. If you assign multiple log settings to an access profile, and this results in duplicate log destinations, logs are also duplicated.*

    a) Select **Access Profiles** from the left pane.
    b) Move access profiles between the **Available** and the **Selected** lists.

    Note: *You can delete (and add) log settings for an access profile on the Logs page for the access profile.*

    Note: *You can configure the log destinations for a log publisher from the Logs page in the System area of the product.*

12. Click **OK**.
    The popup screen closes. The table displays.

To put a log setting into effect, you must assign it to an access profile. Additionally, the access profile must be assigned to a virtual server.

Disabling logging

Disable event logging when you need to suspend logging for a period of time or you no longer want the BIG-IP® system to log specific events.

Note: *Logging is enabled by adding log settings to the access profile.*

1. To clear log settings from access profiles, on the Main tab, click **Access Policy** > **Access Profiles**.
2. Click the name of the access profile.
   Access profile properties display.
3. On the menu bar, click **Logs**.
4. Move log settings from the **Selected** list to the **Available** list.
5. Click **Update**.

Logging is disabled for the access profile.

About event log levels

Event log levels are incremental, ranging from most severe (**Emergency**) to least severe (**Debug**). Setting an event log level to **Warning** for example, causes logging to occur for warning events, in addition to events for more severe log levels. The possible log levels, in order from highest to lowest severity are:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice** (the default log level)
- **Informational**
- **Debug**

Note: *Logging at the* ***Debug*** *level can increase the load on the BIG-IP® system.*

APM log example

The table breaks a typical Access Policy Manager® (APM®) log entry into its component parts.

An example APM log entry

```
Feb  2 12:37:05 site1 notice tmm[26843]: 01490500:5: /Common/for_reports:Common:
 bab0ff52: New session from
client IP 10.0.0.1 (ST=/CC=/C=) at VIP 20.0.0.1 Listener /Common/site1_http
(Reputation=Unknown)
```

Information Type	Example Value	Description
Timestamp	**Feb 2 12:37:05**	The time and date that the system logged the event message.
Host name	**site1**	The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest.
Log level	**notice**	The text value of the log level for the message.
Service	**tmm**	The process that generated the event.
PID	**[26843]**	The process ID.
Log ID	**01490500**	A code that signifies the product, a subset of the product, and a message number.
Level	**5**	The numeric value of the log level for the message.
Partition	**/Common/for_reports:Common**	The partition.to which configuration objects belong.
Session ID	**bab0ff52**	The ID associated with the user session.

Information Type	Example Value	Description
Log message	**New session from client IP 10.0.0.1 (ST=/CC=/C=) at VIP 20.0.0.1 Listener /Common/site1_http (Reputation=Unknown)**	The generated message text.

About local log destinations and publishers

The BIG-IP® system provides two local logging destinations:

local-db

Causes the system to store log messages in the local MySQL database. Log messages published to this destination can be displayed in the BIG-IP Configuration utility.

local-syslog

Causes the system to store log messages in the local Syslog database. Log messages published to this destination are not available for display in the BIG-IP Configuration utility.

Note: *Users cannot define additional local logging destinations.*

The BIG-IP system provides a default log publisher for local logging, sys-db-access-publisher; initially, it is configured to publish to the local-db destination and the local-syslog destination. Users can create other log publishers for local logging.

Configuring a log publisher to support local reports

APM® provides preconfigured reports that are based on log data. To view the reports and to display log data from the BIG-IP® Configuration utility, configure a publisher to log to the local-db destination.

Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, select **local-db** from the **Available** list, and move the destination to the **Selected** list.
4. Click **Finished**.

To use a log publisher, specify it in an access policy log setting, ensure that the access profile selects the log setting, and assign the access profile to a virtual server.

Note: *Log settings are configured in the* ***Access Policy*** *>* ***Event Logs*** *area of the product.*

Viewing an APM report

If Access Policy Manager® (APM®) events are written to the local database on the BIG-IP® system, they can be viewed in APM reports.

Create a report to view event log data.

1. On the Main tab, click **Access Policy** > **Event Logs** > **Access System Logs**.

   The Reports Browser displays in the right pane. The Report Parameters popup screen opens and displays a description of the current default report and default time settings.
2. (Optional) Select the appropriate **Restrict by Time** settings.
3. Click **Run Report**.
   The popup screen closes. The report displays in the Reports Browser.

You can select and run various system-provided reports, change the default report, and create custom reports.

Viewing URL request logs

To view URL request logs from the user interface, your access profile log setting must enable URL request logs. The log setting must also specify a log publisher that publishes to the local-db log destination.

You can display, search, and export URL request logs.

1. On the Main tab, click **Access Policy** > **Event Logs** > **URL Request Logs**.

   Any logs for the last hour are displayed.

   Note: *APM® writes logs for blocked requests, allowed requests, or both, depending on selections in the access profile log setting.*
2. To view logs for another time period, select it from the list.
3. To search the logs, type into the field and click **Search** or click **Custom Search** to open a screen where you can specify multiple search criteria.
4. To export the logs for the time period and filters, click **Export to CSV**.

Configuring a log publisher to supply local syslogs

If you must have syslog files available on the local device, configure a publisher to log to the local-syslog destination.

Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, select **local-syslog** from the **Available** list, and move the destination to the **Selected** list.
4. Click **Finished**.

To use a log publisher, specify it in an access policy log setting, ensure that the access profile selects the log setting, and assign the access profile to a virtual server.

Note: *Log settings are configured in the* ***Access Policy*** > ***Event Logs*** *area of the product.*

Preventing logging to the /var/log/apm file

To stop logs from being written to the /var/log/apm file, remove the local-syslog destination from log publishers that are specified for access system logging in APM® log settings.

Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, if the **Selected** list contains **local-syslog**, move it to the **Available** list.
4. Click **Finished**.

To use a log publisher, specify it in an APM log setting, ensure that the log setting is assigned to an access profile, and assign the access profile to a virtual server.

Note: *Log settings are configured in the Event Logs area of the product.*

About local log storage locations

The BIG-IP® system publishes logs for portal access traffic and for connections to virtual desktops (VDI) to the `/var/log/rewrite*` files. APM® cannot publish these logs to remote destinations.

APM can publish URL request logs to remote or local destinations. Logs published to the local-db destination are stored in the local database and are available for display from the Configuration utility. Logs published to the local-syslog destination are stored in the `/var/log/urlfilter.log` file.

APM can publish access system logs to remote or local destinations. Logs published to the local-db destination are stored in the local database. Logs in the local database are available for display in APM reports. Logs published to the local-syslog destination are stored in the `/var/log/apm` file.

Code expansion in Syslog log messages

The BIG-IP® system log messages contain codes that provide information about the system. You can run the Linux command `cat` *`log`* `|bigcodes |less` at the command prompt to expand the codes in log messages to provide more information. For example:

```
   Jun 14 14:28:03 sccp bcm56xxd [ 226 ] : 012c0012 : (Product=BIGIP
Subset=BCM565XXD) : 6: 4.1 rx [ OK 171009 Bad 0 ] tx [ OK 171014 Bad 0 ]
```

About configurations that produce duplicate log messages

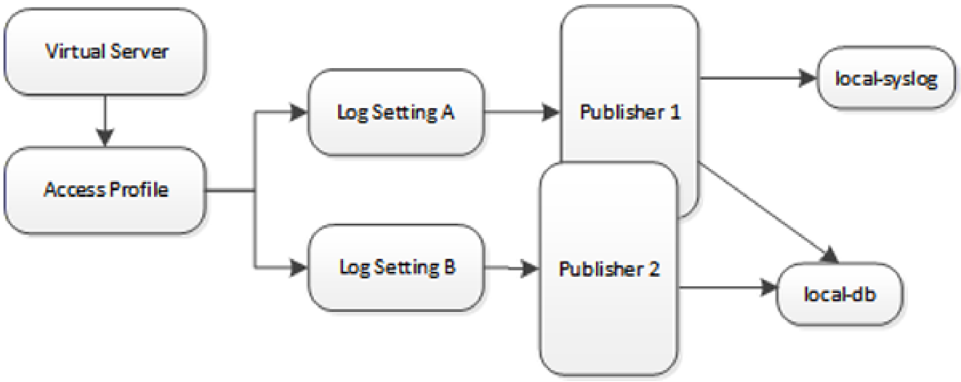


Figure 22: Event log duplication

The figure illustrates a configuration that writes duplicate logs. Two log publishers specify the same log destination, local-db. Each log publisher is specified in one of the log settings that are assigned to an access profile. Logs are written to the local-db destination twice.

Methods to prevent or eliminate duplicate log messages

Duplicate log messages are written when the same log destination is specified by two or more log publishers and more than one of the log publishers is specified in the log settings that are assigned to an access profile.

One way to avoid or eliminate this problem is to specify only one log setting for each access profile. Another is to ensure that the log publishers you associate with log settings for an access profile do not contain duplication log destinations.

About log level configuration

Log levels can be configured in various ways that depend on the specific functionality. Log levels for access portal traffic and for connections to virtual desktops are configured in the System area of the product. The log level for the URL database download is configured in the default-log-setting in the Access Policy Event Logs area of the product. The log level for NTLM authentication of Microsoft Exchange clients is configured using the ECA option in any log setting. Other access policy (and Secure Web Gateway) log levels are configured in any log setting.

Updating the log level for NTLM for Exchange clients

Before you follow these steps, you should have a working configuration of NTLM authentication for Microsoft Exchange clients. The configuration should include a log setting that enables logging for Access Policy Manager® and is assigned to the access profile.

You can change the level of logging for NTLM authentication for Microsoft Exchange clients.

Note: *Logging at the default level,* ***Notice****, is recommended.*

1. On the Main tab, click **Access Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
2. Select the check box for the log setting that you want to update and click **Edit**.
   A popup screen displays.
3. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
4. For the **ECA** setting, select a log level.

   Note: *Setting the log level to* ***Debug*** *can adversely impact system performance.*

5. Click **OK**.
   The popup screen closes.

Configuring logging for the URL database

Configure logging for the URL database so that log messages are published to the destinations, and at the minimum log level, that you specify. (Logging for the URL database occurs at the system level, not the session level, and is controlled using the default-log-setting log setting.)

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

1. On the Main tab, click **Access Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
2. From the table, select **default-log-setting** and click **Edit**.
   A log settings popup screen displays.
3. Verify that the **Enable access system logs** check box is selected.
4. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
5. From the **Log Publisher** list, select the log publisher of your choice.

   A log publisher specifies one or more logging destinations.

   Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

6. To change the minimum log level, from the **Secure Web Gateway** list, select a log level.

   Note: *Setting the log level to* ***Debug*** *can adversely impact system performance.*

   The default log level is **Notice**. At this level, logging occurs for messages of severity Notice and for messages at all incrementally greater levels of severity.

7. Click **OK**.
   The popup screen closes. The table displays.

Setting log levels for portal access and VDI events

Change the logging level for access policy events when you need to increase or decrease the minimum severity level at which Access Policy Manager® (APM®) logs that type of event. Follow these steps to change the log level for events that are related to portal access traffic or related to connections to virtual desktops (VDI).

Note: *You can configure log levels for additional APM options in the Event Logs area.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Options**.
2. Scroll down to the Access Policy Logging area.

   The options **Portal Access** and **VDI** display; each displays a selected logging level.

   Note: *The log settings that you change on this page impact only the access policy events that are logged locally on the BIG-IP® system.*

3. For each option that you want to change, select a logging level from the list.

   Note: *Setting the log level to* ***Debug*** *affects the performance of the BIG-IP® system.*

4. Click **Update**.

APM starts to log events at the new minimum severity level.

Resources and Documentation

Additional resources and documentation for BIG-IP Access Policy Manager

You can access all of the following BIG-IP® system documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`.

Document	Description
BIG-IP® Access Policy Manager®: Application Access	This guide contains information for an administrator to configure application tunnels for secure, application-level TCP/IP connections from the client to the network.
BIG-IP® Access Policy Manager®: Authentication and Single-Sign On	This guide contains information to help an administrator configure APM for single sign-on and for various types of authentication, such as AAA server, SAML, certificate inspection, local user database, and so on.
BIG-IP® Access Policy Manager®: Customization	This guide provides information about using the APM customization tool to provide users with a personalized experience for access policy screens, and errors. An administrator can apply your organization's brand images and colors, change messages and errors for local languages, and change the layout of user pages and screens.
BIG-IP® Access Policy Manager®: Edge Client and Application Configuration	This guide contains information for an administrator to configure the BIG-IP® system for browser-based access with the web client as well as for access using BIG-IP Edge Client® and BIG-IP Edge Apps. It also includes information about how to configure or obtain client packages and install them for BIG-IP Edge Client for Windows, Mac, and Linux, and Edge Client command-line interface for Linux.
BIG-IP® Access Policy Manager®: Implementations	This guide contains implementations for synchronizing access policies across BIG-IP systems, hosting content on a BIG-IP system, maintaining OPSWAT libraries, configuring dynamic ACLs, web access management, and configuring an access policy for routing.
BIG-IP® Access Policy Manager®: Network Access	This guide contains information for an administrator to configure APM Network Access to provide secure access to corporate applications and data using a standard web browser.
BIG-IP® Access Policy Manager®: Portal Access	This guide contains information about how to configure APM Portal Access. In Portal Access, APM communicates with back-end servers, rewrites links in application web pages, and directs additional requests from clients back to APM.
BIG-IP® Access Policy Manager®: Secure Web Gateway Implementations	This guide contains information to help an administrator configure Secure Web Gateway (SWG) explicit or transparent forward proxy and apply URL categorization and filtering to Internet traffic from your enterprise.
BIG-IP® Access Policy Manager®: Third-Party Integration Implementations	This guide contains information about integrating third-party products with Access Policy Manager (APM®). It includes implementations for integration with VMware Horizon View, Oracle Access Manager, Citrix Web Interface site, and so on.

Document	Description
BIG-IP® Access Policy Manager®: Visual Policy Editor	This guide contains information about how to use the visual policy editor to configure access policies.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

Index