BIG-IP® Access Policy Manager®: Application Access

Version 12.1

Table of Contents

Configuring App Tunnel Access

What are app tunnels?

An *app tunnel* (application tunnel) provides secure, application-level TCP/IP connections from the client to the network. App tunnels are particularly useful for users with limited privileges who attempt to access particular web applications, as app tunnels do not require that the user has administrative privileges to install.

Additionally, optimization is available for app tunnels. With compression settings for app tunnels, you can specify the available compression codecs for client-to-server connections. The server compares the available compression types configured with the available compression types on the server, and chooses the most effective mutual compression setting. You configure compression for the server in the connectivity profile.

Note: *Because app tunnels do not require administrative rights, some features of Network Access and Optimized Application tunnels are not available with app tunnels. For example, the application tunnel cannot easily resolve domain names in applications without a client-side DNS redirector, or modification of the system hosts file.*

Important: *For tunnels that access backend servers by using DNS resolution, use Optimized Application Tunnels in the Network Access menus instead. Optimized Applications require administrative rights on the local system.*

Task summary for app tunnels

To set up this configuration, perform the procedures in the task list.

Task list

Configuring an app tunnel object
Configuring an application resource item for an app tunnel
Configuring an access policy to include an app tunnel
Attaching an access policy to the virtual server for app tunnels
Verifying log settings for the access profile

Configuring an app tunnel object

When you create an app tunnel object, that object becomes a simple container that holds app tunnel resources. Once you specify those resources from within the app tunnel resource, you can then assign the resource to an access policy.

1. On the Main tab, click **Access Policy** > **Application Access** > **App Tunnels**.
   The App Tunnels screen opens.
2. Click **Create**.
   The New App Tunnel Resource screen opens.
3. Type a name and description for your app tunnel.

4. Although an ACL is automatically created for your application object, you can choose to determine the order of your ACL as it appears in the ACL list. Use the **ACL Order** list to select the placement you want.
5. Under Default Customization Settings, type a **Caption** for the app tunnel.
   This caption identifies the app tunnel and enables it to appear on a full webtop.
6. Click **Create**.

You have just created an app tunnel object.

Configuring an application resource item for an app tunnel

The application resource item specifies how to create a particular tunnel. The application field serves as a hint to Access Policy Manager® in order to help with special handling of specific protocols. Compression settings specify which compression codecs the tunnels can use, while the **Launch Application** field allows you to define an application that will run after you establish the resource tunnel.

1. On the Main tab, click **Access Policy** > **Application Access** > **App Tunnels**.
   The list of app tunnels opens.
2. Click the name of the app tunnel you created.
   The Properties screen opens.
3. Under Resource Items, click **Add**.
   The New Resource Item screen opens.
4. For the **Destination** setting, specify whether the application destination **Type** is a host or an IP address.
   You cannot use the fully qualified domain name to connect to an application resource that is configured with an IP address destination type.
   If you specify a hostname, make sure that it is DNS-resolvable. After the application tunnel is assigned to a full webtop in an access policy, the application tunnel does not appear on the full webtop if the hostname is not DNS-resolvable.
5. Specify your port or port range for the application.
6. From the **Application Protocol** list, select the application protocol.

Option	Description
None	Specifies that the app tunnel resource uses neither RPC or FTP protocols.
Microsoft RPC	Specifies that the resource uses the Microsoft® RPC protocol.
Microsoft Exchange RPC Server	Specifies that the resource uses the Microsoft Exchange RPC Server protocol.
FTP	Specifies that the resource uses FTP protocol.

7. For the **Application Path** setting, optionally specify a path for an application to start after the application access tunnel is established.
8. For the **Parameters** setting, specify any parameters associated with the application that starts with the **Application Path**. The parameters you can add are:
   - `%host%` - This is substituted with the loopback host address, for example `http://%host%/application/`.
   - `%port%` - The loopback port. Use this if the original local port has changed due to conflicts with other software.
9. Click **Finished**.

The resource appears in the app tunnel object.

Configuring an access policy to include an app tunnel

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
5. 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.
6. On the Assignment tab, select the **Resource Assign** agent, and click **Add Item**.
   The Resource Assignment screen opens.
7. Next to the **App Tunnel** setting, click the **Add/Delete** link, and select the application tunnel to assign.
8. Click **Update**.
9. Click the **Save** button to save changes to the access policy item.

Your app tunnels are now assigned to the session.

To complete the process, you must assign a webtop, apply the access policy, and associate the access policy and connectivity profile with a virtual server so users can launch the app tunnel session.

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

Attaching an access policy to the virtual server for app tunnels

When creating a virtual server for an access policy, specify an IP address for a single host as the destination address.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. 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.
4. From the **HTTP Profile** list, select **http**.
5. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
6. If you are using a connectivity profile, from the **Connectivity Profile** list, select the connectivity profile.

7. If you are creating a virtual server to use with portal access resources in addition to app tunnels, from the **Rewrite Profile** list, select the default **rewrite** profile, or another rewrite profile you created.
8. If you want to provide connections to Java RDP clients for application access, allow Java rewriting for portal access, or support a per-app VPN connection that is configured on a mobile device, select the **Application Tunnels (Java & Per-App VPN)** check box.

   You must enable this setting to make socket connections from a patched Java applet. If your applet does not require socket connections, or only uses HTTP to request resources, this setting is not required.
9. If you want to provide native integration with an OAM server for authentication and authorization, select the **OAM Support** check box.

   You must have an OAM server configured in order to enable OAM support.
10. Click **Update**.

Your access policy is now associated with the virtual server.

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 Remote Desktop Access

What are remote desktops?

Remote desktops in Access Policy Manager® allow users to access the following types of internal servers in virtual desktop sessions:

- Microsoft® Remote Desktop servers
- Citrix® servers
- VMware View Connection servers

You can configure remote desktops by name or by their internal IP addresses, and grant or deny users the ability to set up their own favorites.

What is Microsoft remote desktop?

Using an Access Policy Manager® (APM®) RDP type remote desktop, clients can access a server that runs Microsoft Remote Desktop Services. Microsoft Remote Desktop servers run the Microsoft Remote Desktop Protocol (RDP) server. *RDP* is a protocol that provides a graphical interface to another computer on a network.

To provide Microsoft RDP connections natively, APM provides these alternatives.

Java Client
APM provides a Java Client option in the remote desktop configuration. The option supports native connections for Windows, Mac, and Linux clients. When this option is selected, a user on any compatible platform is presented with a simple Java Client interface to the Microsoft RDP server with reduced visual display features.

APM as a gateway for RDP clients
With proper BIG-IP® system configuration, Microsoft RDP clients can use APM as a gateway. The configuration supports Microsoft RDP clients on Windows, Mac, iOS, and Android. When a user types the address or hostname of the gateway into an RDP client and specifies a particularly configured virtual server for it, APM authorizes the client. When the client requests connections to resources on backend servers, APM authorizes the access.

For support information, refer to *BIG-IP APM Client Compatibility Matrix* on AskF5™ at `http://support.f5.com/`.

What is Citrix remote desktop?

Citrix® remote desktops are supported by Citrix XenApp™ and ICA clients. With Access Policy Manager® you can configure clients to access servers using Citrix terminal services. You provide a location from which a client can download and install a Citrix client for a Citrix ICA connection.

Task summary for remote desktops

To set up remote desktops, perform the procedures in the task list.

Task list

Configuring a resource for Citrix or Microsoft remote desktops
Configuring an access policy to include a remote desktop
Attaching an access policy to a virtual server for remote desktops
Verifying log settings for the access profile

Configuring a resource for Citrix or Microsoft remote desktops

Depending on whether you choose to configure a Microsoft or Citrix remote desktop, some options may not be available. Refer to the online help for more information about the parameters you can configure for remote desktops.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Remote Desktops List**.
   The Remote Desktops list opens.
2. Click **Create**.
   The General Properties screen opens.
3. Configure the following settings:

Option	Description
For Citrix	Specify an IP address as your **Destination**, accept or change the **Port**, and select the **ACL Order**.
For RDP	Specify your **Destination** and **Port**. All other settings are optional. To provide a cross-platform Java client for this RDP tunnel, select the **Java Client** check box.

Note: *If you specify a hostname for your destination, make sure that it is DNS-resolvable. After the remote desktop is assigned to a full webtop in an access policy, the remote desktop does not appear on the full webtop if the hostname is not DNS-resolvable.*

4. Type one or more lines in the **Custom Parameters** field.
   These parameters affect the rendering of certain features for both Citrix and RDP. The format differs for each type of terminal resource.
5. Under the **Default Customization Settings** section, type a **Caption**.
   The caption identifies the remote desktop and enables it to appear on a full webtop.

Configuring an access policy to include a remote desktop

This procedure is applicable if you want to configure Access Policy Manager® for Citrix or Microsoft RDP terminal services.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.

The properties screen opens for the profile you want to edit.

3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
5. 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.
6. On the Assignment tab, select the **Resource Assign** agent, and click **Add Item**.
   The Resource Assignment screen opens.
7. Next to each type of resource that you want assign (**Network Access**, **Portal Access**, **App Tunnel**, **Remote Desktop**, or **SAML**), click the **Add/Delete** link, and select from available resources.
8. Click **Update**.
9. Click **Save**.

Your remote desktop is assigned to the session.

To complete the process, you must assign a webtop, apply the access policy, and associate the access policy and connectivity profile with a virtual server so users can launch the remote desktop session.

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

Attaching an access policy to a virtual server for remote desktops

When creating a virtual server for an access policy, specify an IP address for a single host as the destination address.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. 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.
4. For the **HTTP Profile** setting, verify that the default HTTP profile, **http**, is selected.
5. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
6. If you are using a connectivity profile, from the **Connectivity Profile** list, select the connectivity profile.
7. If you are creating a virtual server to use with portal access resources in addition to remote desktops, from the **Rewrite Profile** list, select the default **rewrite** profile, or another rewrite profile you created.
8. If you want to provide connections to Java RDP clients for application access, allow Java rewriting for portal access, or support a per-app VPN connection that is configured on a mobile device, select the **Application Tunnels (Java & Per-App VPN)** check box.

   You must enable this setting to make socket connections from a patched Java applet. If your applet does not require socket connections, or only uses HTTP to request resources, this setting is not required.

9. If you want to provide native integration with an OAM server for authentication and authorization, select the **OAM Support** check box.

   You must have an OAM server configured in order to enable OAM support.

10. Click **Update**.

The access policy is now associated with the virtual server.

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 Webtops

About webtops

There are three webtop types you can define on Access Policy Manager® (APM®). You can define a network access only webtop, a portal access webtop, or a full webtop.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode. This configuration does not work.*

- A network access webtop provides a webtop for an access policy branch to which you assign only a network access resource for starting a network access connection that provides full network access.
- A portal access webtop provides a webtop for an access policy branch to which you assign only portal access resources. When a user selects a resource, APM communicates with back-end servers and rewrites links in application web pages so that further requests from the client browser are directed back to the APM server.
- A full webtop provides an access policy ending for an access policy branch to which you can optionally assign portal access resources, app tunnels, remote desktops, and webtop links, in addition to network access tunnels. Then, the full webtop provides your clients with a web page on which they can choose resources, including a network access connection to start.

  Note: *If you add a network access resource with Auto launch enabled to the full webtop, the network access resource starts when the user reaches the webtop. You can add multiple network access resources to a webtop, but only one can have Auto launch enabled.*

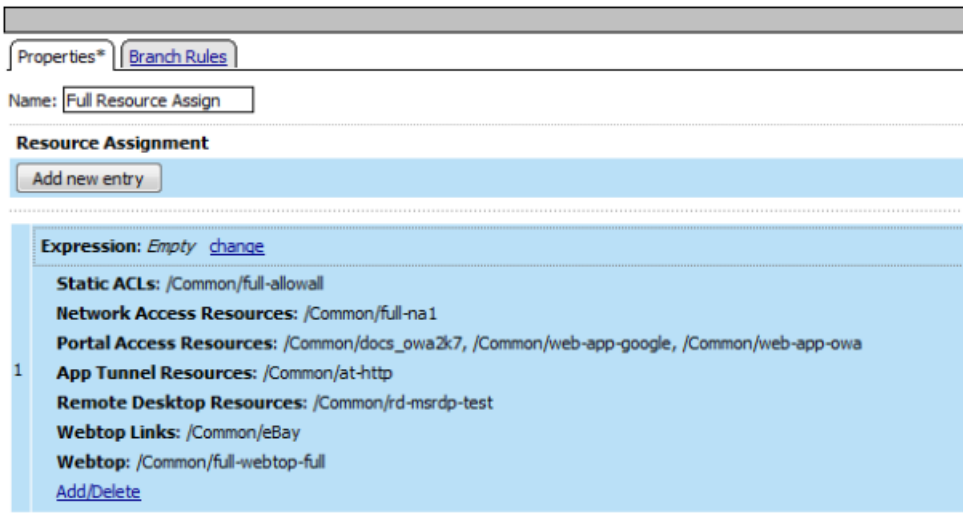

Figure 1: Resource assign action with resources and a webtop assigned

Configuring a full webtop

A full webtop allows your users to connect and disconnect from a network access connection, portal access resources, SAML resources, app tunnels, remote desktops, and administrator-defined links.

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 list. You can edit the webtop further, or assign it to an access policy.

To use this webtop, it must be assigned to an access policy with an advanced resource assign action or with a webtop, links, and sections assign action. All resources assigned to the full webtop are displayed on the full webtop.

Creating a webtop link

You can create and customize links that you can assign to full webtops. In this context, *links* are defined applications and websites that appear on a webtop, and can be clicked to open a web page or application. You can customize these links with descriptions and icons.

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Links**.
2. Click **Create**.
   The New Webtop Link screen opens.
3. In the **Name** field, type a name for the webtop link.
4. From the **Link Type** list, select whether the link is a URI or hosted content.
   - If you selected **Application URI**, in the **Application URI** field, type the application URI.
   - If you selected **Hosted Content**, select the hosted file to use for the webtop link.
5. In the **Caption** field, type a descriptive caption.

   The **Caption** field is pre-populated with the text from the **Name** field. Type the link text that you want to appear on the web link.
6. If you want to add a detailed description, type it in the **Detailed Description** field.
7. To specify an icon image for the item on the webtop, click in the **Image** field and choose an image, or click the **Browse** button.

   Click the **View/Hide** link to show or hide the currently selected image.
8. Click **Finished**.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop, links and sections assign action.

Customizing a webtop link

You can customize links that you assign to full webtops.

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Links**.
2. Click the name of the webtop link you want to customize.
   The properties screen for the webtop link appears.
3. To change the description of the link, in the **Description** field, type a new description.
4. To change the URI of the link, in the **Application URI** field, type the application URI.
5. If you made changes on the properties screen, click **Update**.
6. Click the Customization tab.
7. Select the **Language** to customize, or click the **Create** button to create a new language customization.
8. If you clicked **Create** to create a new language customization, from the **Language** list, select the language to customize.
9. In the **Caption** field, type a descriptive caption.
10. In the **Detailed Description** field, type a detailed description.
11. In the **Image** field, click **Browse** to select an image to show on the webtop to represent the webtop link. Click the **View/Hide** link to show the currently assigned image.

    A webtop link image can be a GIF, BMP, JPG or PNG image up to 32 x 32 pixels in size.
12. Click **Finished**.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop, links and sections assign action.

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.

Adding a webtop, links, and sections to an access policy

You must have an access profile set up before you can add a webtop, links, and sections to an access policy.

You can add an action to an access policy to add a webtop, webtop links, and webtop sections to an access policy branch. Webtop links and webtop sections are displayed on a full webtop.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode; this configuration does not work.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
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. On the Assignment tab, select the **Webtop, Links and Sections Assign** agent and click **Add Item**.
   The Webtop, Links and Sections Assignment screen opens.
7. In the **Name** field, type a name for the access policy item.
   This name is displayed in the action field for the access policy.
8. For each type of resource that you want assign:
   a) Click the **Add/Delete** link next to the resource type (**Webtop Links**, **Webtop Sections**, or **Webtop**).
      Available resources are listed.
   b) Select from the list of available resources.
      Select only one webtop.
   c) Click **Save**.
9. Click the **Save** button to save changes to the access policy item.

You can now configure further actions on the successful and fallback rule branches of this access policy item.

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

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

Assigning resources to a user

Before you can assign resources to a user, you must have created an access profile.

You can add the advanced resource assign action to an access policy to add a network access resource, portal access resources, application tunnel resources, SAML resources, and remote desktop resources to an access policy branch. You can also assign ACLs, webtops, webtop links, and webtop sections with the advanced resource assign action.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode; this configuration does not work.*

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
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. On the Assignment tab, select **Advanced Resource Assign** and click the **Add Item** button.
   The Advanced Resource Assign popup screen opens.
7. In the **Name** field, type a name for the access policy item.
   This name is displayed in the action field for the access policy.
8. Click the **Add new entry** button.
   A new resource line is added to the list.
9. To assign resources, in the Expression area, click the **Add/Delete** link.
   The Resource Assignment popup screen opens.
10. Assign resources to the access policy using the available tabs.

Tab	Description
Static ACLs	Allows you to select one or more ACLs defined on the system. Each ACL you select is assigned to the access policy branch on which this resource assign action operates.
Network Access	Allows you to select a single network access resource from the system. You can select only one network access resource. The network access resource you select is assigned to the access policy branch on which this resource assign action operates.
Portal Access	Allows you to select one or more portal access resources from the system. The portal access resources you select are assigned to the access policy branch on which this resource assign action operates.
App Tunnel	Allows you to select one or more application tunnel resources from the system. The application tunnel resources you select are assigned to the access policy branch on which this resource assign action operates.
Remote Desktop	Allows you to select one or more remote desktop (terminal server) resources from the system. The remote desktop resources you select are assigned to the access policy branch on which this resource assign action operates.
SAML	Allows you to select one or more SAML resources from the system. The SAML resources you select are assigned to the access policy branch on which this resource assign action operates. Select a full webtop to display SAML resources.

Tab	Description
Webtop	Allows you to select a webtop from the system. The webtop resource you select is assigned to the access policy branch on which this resource assign action operates. You can select a webtop that matches the resource type, or a full webtop.
Webtop Links	Allows you to select links to pages and applications defined on the system to display on the full webtop. A full webtop must be assigned to display webtop links.
Webtop Sections	Allows you to select one or more sections into which to organize the selected resources on the webtop. A full webtop must be assigned to display webtop sections.
Static Pool	Allows you to dynamically assign a predefined LTM® pool to a session. This value takes precedence over any existing assigned pool attached to the virtual server. The static pool you select is assigned to the access policy branch on which this resource assign action operates.

Note: *You can also search for a resource by name in the current tab or all tabs.*

11. Click the **Save** button to save changes to the access policy item.

You can now configure further actions on the successful and fallback rule branches of this access policy item.

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

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.

Webtop properties

Use these properties to configure a webtop.

Property setting	Value	Description
Type	**Network Access**, **Portal Access**, or **Full**	• Use **Network Access** for a webtop to which you assign only a single network access resource. • Use **Portal Access** for a webtop to which you assign only portal access resources. • Use **Full** for a webtop to which you assign one or more network access resources, multiple portal access resources, and multiple application access application tunnel resources, or any combination of the three types.
Portal Access Start URI	URI.	Specifies the URI that the web application starts. For full webtops, portal access resources are published on the webtop with the associated URI you define when you select the **Publish on Webtop** option.
Minimize to Tray	**Enable** or **Disable**.	If this check box is selected, the webtop is minimized to the system tray automatically after the network access connection starts. With a network access webtop, the webtop automatically minimizes to the tray. With a full webtop, the webtop minimizes to the system tray only after the network access connection is started.

Integrating Application Access and Secure Web Gateway

Overview: Configuring SWG transparent forward proxy for remote access

Secure Web Gateway (SWG) can be configured to support remote clients that connect using application access, network access, or portal access.

Note: *Using a distinct SWG transparent forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

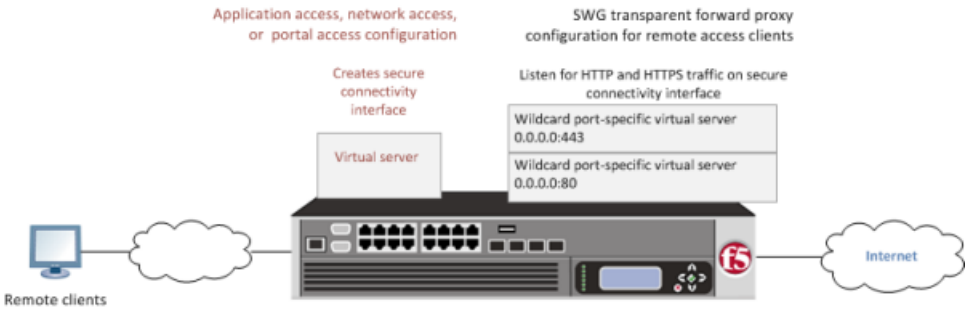

Figure 2: SWG transparent forward proxy for remote access

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Creating an access profile for SWG transparent forward proxy
Verifying log settings for the access profile
Creating a wildcard virtual server for HTTP traffic on the connectivity interface
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the connectivity interface
Updating the access policy in the remote access configuration

Prerequisites for SWG transparent forward proxy for remote access

Before you start to create a Secure Web Gateway (SWG) transparent forward proxy configuration to support remote access clients, you must have completed these tasks.

- You must have a working Network Access, Portal Access, or Application Access configuration.
- You need a per-request policy configured for forward proxy.
- On a BIG-IP® system with an SWG subscription, you must ensure that the URL database is downloaded and you need to have configured any URL filters that you want to use in addition to, or instead of, the default URL filters.

- On a BIG-IP® system without an SWG subscription to use URL categories and filters, you must have created user-defined URL categories and URL filters.

Configuration outline for SWG transparent forward proxy for remote access

Tasks for integrating an Access Policy Manager® (APM®) remote access configuration with a Secure Web Gateway (SWG) transparent forward proxy configuration follow this order.

- First, update the existing application access, network access, or portal access configuration to add a secure connectivity profile to the virtual server if one is not already specified.
- Next, create an SWG transparent forward proxy configuration. The per-request policy is part of this configuration.
- Finally, update the access policy in the existing application access, network access, or portal access configuration if needed. If the per-request policy uses group or class lookup items, add queries to the access policy to populate the session variables on which the lookup items rely.

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.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Creating an access profile for SWG transparent forward proxy

You create an access profile to supply an access policy.

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 per-request policy names.*

4. From the **Profile Type** list, select **SWG-Transparent**.
   Additional fields display set to default values.
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 Profiles list screen displays.

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

You do not need to add any actions or make any changes to the access policy.

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 a wildcard virtual server for HTTP traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect.

You configure a virtual server to process web traffic on the secure connectivity interface for a remote access client.

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 `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

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. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.

g) In the **Confirm CA Passphrase** field, type the passphrase again.
h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.

   You can update this setting later but only while the profile is not assigned to a virtual server.

   Additional settings display.
l) For **Default Bypass Action**, retain the default value **Intercept**.

   You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

---

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server 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. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a wildcard virtual server for SSL traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect. Also, if you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the secure connectivity interface for a remote access client.

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 `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. For the **Address Translation** setting, clear the **Enabled** check box.
15. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
16. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
17. Click **Finished**.

Updating the access policy in the remote access configuration

Add queries to the access policy to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that can only be populated in this access policy.*

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. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
4. 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.
5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   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) Specify the **SearchDN**, and **SearchFilter** settings.
      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.
      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.
8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:
   a) From the **LocalDB Instance** list, select a local user database.

b) In the **User Name** field, retain the default session variable.
c) Click **Add new entry**
A new line is added to the list of entries with the Action set to **Read** and other default settings.
d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
e) In the Source column from the **DB Property** list, select **groups**.
f) Click **Save**.

This item populates the `session.localdb.groups` session variable.

The access policy is configured to support the per-request policy.

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

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

Implementation result

The Secure Web Gateway (SWG) transparent proxy configuration is ready to process web traffic from remote access clients.

About configuration elements for transparent forward proxy (remote access)

When you configure Secure Web Gateway (SWG) transparent forward proxy for use by remote access clients, you might want to understand how these objects fit into the overall configuration.

Secure connectivity interface

In a remote access configuration, a connectivity profile is required on the virtual server to specify a secure connectivity interface for traffic from the client. In the SWG configuration, SWG wildcard virtual servers must listen on the secure connectivity interface for traffic from remote access clients.

Per-request policy

In any SWG configuration, the determination of whether a user can access a URL must be made in a per-request access policy. A per-request access policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the remote access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must populate any session variables used in the per-request policy. An access profile of the SWG-Transparent type is required in the SWG configuration; however, it is not necessary to include any items in the access policy.

Per-request policy items that read session variables

This table lists per-request policy items that read session variables and lists the access policy items that populate the variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

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.

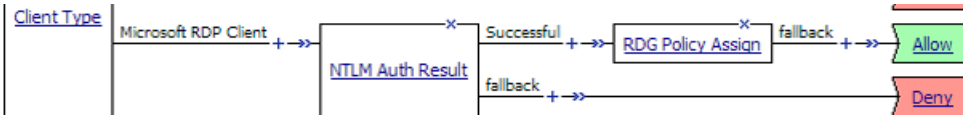

Figure 3: Sample client authorization policy

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

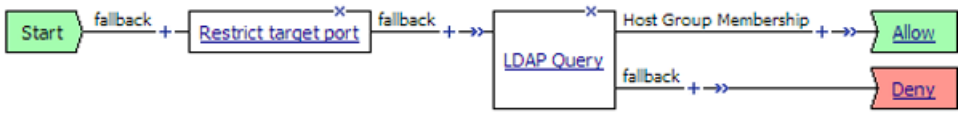

Figure 4: Sample resource authorization policy

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) On the Endpoint Security (Server-Side) tab, select **Client Type**, 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.

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.

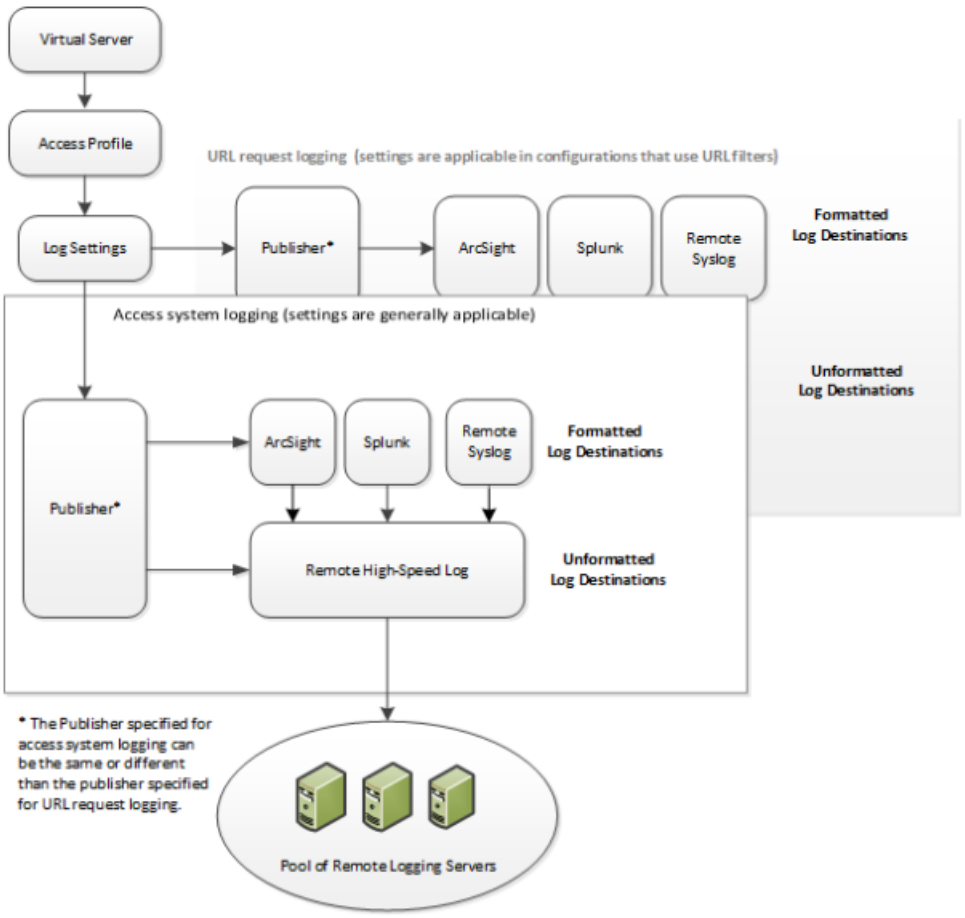

Figure 5: Association of remote high-speed logging configuration objects

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.
    - **Log Confirmed Events** - When selected, user requests for confirmed URLs are logged.

    Whether a URL is allowed, blocked, or confirmed 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, confirmed requests, allowed requests, or all three, 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

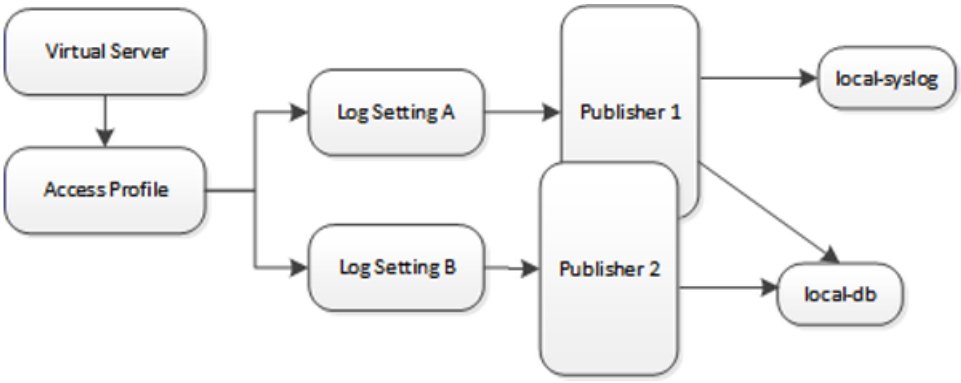

Figure 6: Event log duplication

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.*

   Warning: *F5® recommends that you do not set the log level for **Portal Access** to **Debug**. Portal Access can stop working. The BIG-IP system can become slow and unresponsive.*

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	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	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.

Legal Notices

Legal notices

Publication Date

This document was published on May 9, 2016.

Publication Number

MAN-0360-05

Copyright

Trademarks

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks/*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *http://www.f5.com/about/guidelines-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.

Index

M

N

P

R

S

T

U

V

W