BIG-IP® Access Policy Manager®: Application Access

Version 11.6

Table of Contents

Legal Notices

Publication Date

This document was published on August 20, 2014.

Publication Number

MAN-0360-03

Copyright

Trademarks

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.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Daniel Stenberg. Copyright ©1996 - 2012, Daniel Stenberg, (daniel@haxx.se). All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Chapter 1

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

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. Click **Edit Access Policy for Profile *profile_name***.
   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.

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 doesn't 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.

Chapter 2

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 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. 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. Click **Edit Access Policy for Profile** ***profile_name***.
   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.

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 doesn't 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.

Chapter 3

Configuring Webtops

About webtops

There are three webtop types you can define on Access Policy Manager® (APM®). You can define a network access as only a 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.
- A portal access webtop provides a webtop for an access policy branch to which you assign only portal access resources.
- 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 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.*

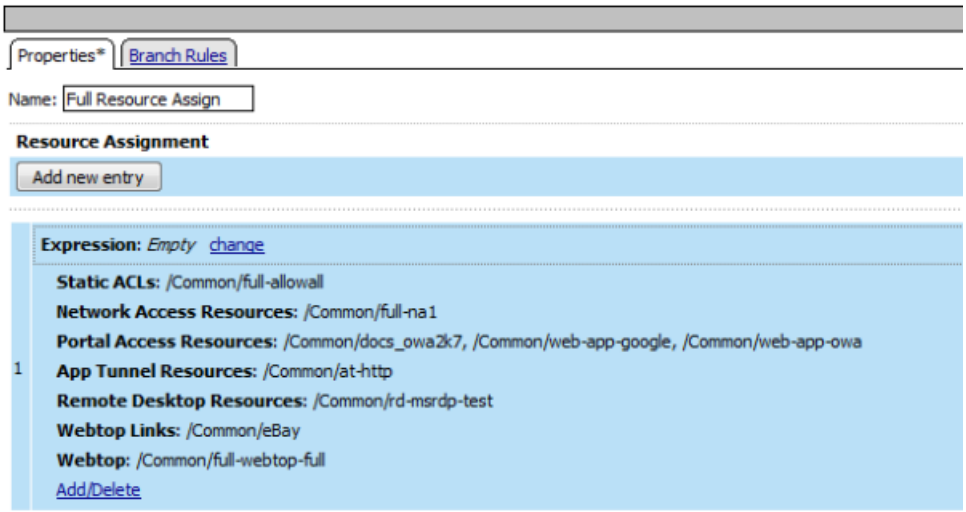

Figure 1: Resource assign action with resources and a webtop assigned

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**.
2. Click **Create** to create a new webtop.
3. Type a name for the webtop you are creating.

4. From the **Type** list, select **Full**.
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 and links 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** to create a new webtop link.
3. In the **Name** field, type a name for the new 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 and links 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 and links assign action.

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.

Adding a webtop and webtop links to an access policy

You must have an access profile set up before you can start this task.

You can add the webtop and webtop links assign action to an access policy to add a webtop and webtop links to an access policy branch. Webtop links 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. Click **Edit Access Policy for Profile *profile_name***.
   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 and Links Assign** agent and click **Add Item**.
   The Webtop and Links 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. On the Webtop & Webtop Links Assignment screen, next to the type of resource you want to add, click the **Add/Delete** link.
   Available resources are listed.
9. To assign resources, select the options you want.
10. 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.

Assigning resources to a user

Before you start this task, 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, and webtop links 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. Click **Edit Access Policy for Profile *profile_name***.
   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.
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	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.
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.

Chapter 4

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.*

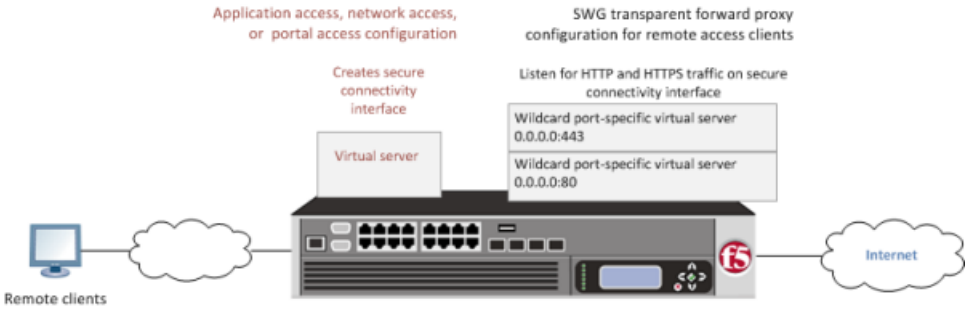

Figure 2: SWG transparent forward proxy for remote access

You should understand how these configuration 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 assign an SWG scheme for the network access session and 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.

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Configuring a per-request policy for SWG
Creating an access profile for SWG transparent forward proxy
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

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 need to have configured a working application access, network access, or portal access configuration, depending on which type of remote client you want to support.
- If you have not already done so, you must ensure that the URL database is downloaded.
- You need to have configured at least one SWG scheme and any URL filters that you want to use in addition to or instead of the default URL filters.

Configuration outline

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. An SWG scheme assignment is required in this access policy. If the per-request policy uses group or class lookup items, add queries 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 appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity 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.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.

   A per-request policy name must be unique among all per-request policy and access profile names.

   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) Click **Save**.
      The Properties screen closes. The visual policy editor displays.
6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.

   It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.
7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

   Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic,

select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.

d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.
Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

e) Click **Save**.
The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.

9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.

10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:

a) In the visual policy editor, click the name of the item.
A Properties popup screen opens.

b) Click the Branch Rules tab.

c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.

d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.

e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.

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

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

12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:

a) In the visual policy editor, click the name of the policy item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) Edit the default simple expression to specify group or class that is used in your environment.
In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.
e) Click **Finished**.
The popup screen closes.
f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.
b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.
c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.
d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

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

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

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.
7. To enable Secure Web Gateway event logging for this access profile, add log settings.
   a) Click the name of the access profile that you just created.
      The Properties screen displays.
   b) On the menu bar, click **Logs**.
      The General Properties screen displays.
   c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

   You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy that contains a **Start** and a **Deny** ending.

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

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. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
15. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
16. Click **Finished**.

Updating the access policy in the remote access configuration

Add an SWG Scheme Assign item to an access policy to assign a Secure Web Gateway (SWG) scheme to a client session. Add queries 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 are 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. Click **Edit Access Policy for Profile** ***profile_name***.
   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. On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A properties screen opens.
6. To display the available schemes, click the **Add/Delete** link.
7. Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor screen displays.
8. 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.

9. 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**.

10. 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.

11. 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 assign an SWG scheme and to support the per-request policy.

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

Implementation result

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

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session 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

Chapter 5

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.

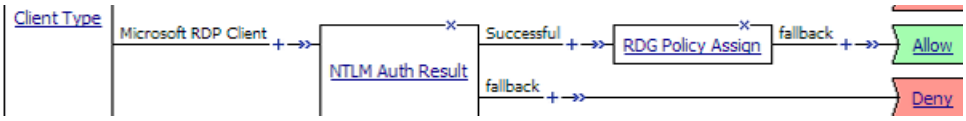

Figure 3: Sample client authorization policy

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

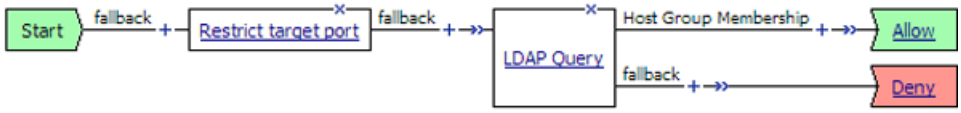

Figure 4: Sample resource authorization policy

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
Configuring an access policy for resource authorization
Creating an access profile for RDP client authorization
Configuring an access policy for an RDP client
Configuring a machine account
Creating an NTLM Auth configuration
Maintaining a machine account
Configuring a VDI profile

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

Hostname setting: The hostname or IP address of the virtual server must be specified.
Port setting: If requested, `443` must be specified.
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.
Hostname setting: Hostname of the target server.
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.

This creates an access profile with a default access policy.

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

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 is displayed.

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 is displayed.

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 is displayed.

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:
   - **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**.

Configuring an access policy for an RDP client

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

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

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

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

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

4. (Optional) Type `client` in the search field, select **Client Type** from the results list, and click **Add Item**.

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

   A properties screen opens.
5. Click **Save**.
   The properties screen closes; the **Client Type** item displays in the visual policy editor with a **Microsoft Client RDP** branch and branches for other client types.
6. On an access policy branch, click the **(+)** icon to add an item to the access policy.
7. To verify the result of client authentication:
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result**.
   c) Click **Add Item**.

   A properties screen opens.
8. Click **Save**.
   The properties screen closes and the visual policy editor displays.
9. Select the RDG-RAP access policy you configured earlier:
   a) Click the **[+]** sign on the successful branch after the authentication action.
   b) Type `RDG` in the search field.
   c) Select **RDG Policy Assign** and click **Add Item**.
   d) To display available policies, click the **Add/Delete** link.
   e) Select a policy and click **Save**.

   Without an RDG policy, APM denies access to each resource request.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Configuring a machine account

You need to 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.

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 appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity 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.

Index

S

T

V

W