BIG-IP® Access Policy Manager®: Portal Access

Version 11.6

Table of Contents

Legal Notices

Publication Date

This document was published on August 20, 2014.

Publication Number

MAN-0364-05

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.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

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. 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.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes Boost libraries, which are distributed under the Boost license (http://www.boost.org/LICENSE_1_0.txt).

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes libmagic software, copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

This product contains OpenLDAP software, which is distributed under the OpenLDAP v2.8 license (BSD3-like).

Chapter 1

Overview of Portal Access

Overview: What is portal access?

Portal access allows end users access to internal web applications with a web browser from outside the network. With portal access, the BIG-IP® Access Policy Manager® 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 Access Policy Manager server. With portal access, the client computer requires no specialized client software other than a web browser.

Portal access provides clients with secure access to internal web servers, such as Microsoft® Outlook®Web Access (OWA), Microsoft SharePoint®, and IBM® Domino® Web Access. Using portal access functionality, you can also provide access to most web-based applications and internal web servers.

Portal access differs from network access, which provides direct access from the client to the internal network. Network access does not manipulate or analyze the content being passed between the client and the internal network. The portal access configuration gives the administrator both refined control over the applications that a user can access through Access Policy Manager, and content inspection for the application data. The other advantage of portal access is security. Even if a workstation might not meet requirements for security for full network access, such a workstation can be passed by the access policy to certain required web applications, without allowing full network access. In a portal access policy, the client computer itself never communicates directly with the end-point application. That means that all communication is inspected at a very high level, and any attacks originating on the client computer fail because the attack cannot navigate through the links that have been rewritten by the portal access engine.

About portal access configuration elements

A portal access configuration requires several elements:

- A portal access resource including one or more portal access resource items
- An access profile
- An access policy that assigns both:
  - A portal access resource
  - A portal access or full webtop
- A rewrite profile (you can use the default rewrite profile)
- A connectivity profile
- A virtual server that assigns the access profile and a rewrite profile

Portal access elements are summarized in this diagram.

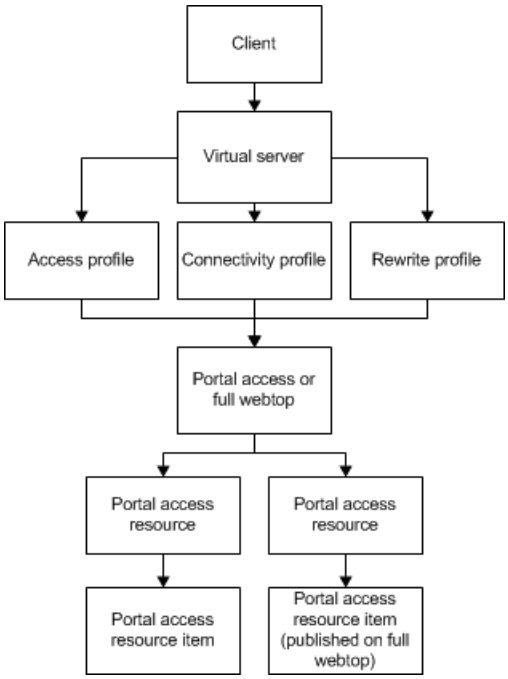

Figure 1: Portal access elements

Understanding portal access patching

Portal access patches, or rewrites, links in web content. Portal access rewrites links in complex Java®, JavaScript™, Flash®, CSS, and HTML content. In full patching mode, Access Policy Manager® retrieves content from back-end servers and rewrites links in that content so it can be presented to a web browser, as if the content originated from the Access Policy Manager. Portal access rewrites content to make intranet targets resolvable, no matter what the intranet host is.

Understanding full patching mode

In *full patching mode*, you can select one or more of the following content types in which portal access rewrites links.

Patching content type	Description
HTML patching	Rewrites links in HTML content to redirect to the Access Policy Manager®.
JavaScript patching	Rewrites link content in JavaScript code to redirect requests to the Access Policy Manager.
CSS patching	Rewrites links to CSS files, and within CSS content, to redirect to the Access Policy Manager.
Flash patching	Rewrites links in Flash movies and objects to redirect requests to the Access Policy Manager.
Java patching	Rewrites link content in Java code to redirect requests to the Access Policy Manager. Access Policy Manager can also relay and handle any socket connections required by a patched Java applet.

Understanding minimal patching mode

In *minimal patching mode*, portal access allows only minimum rewriting of web application content. Minimal patching mode is useful for troubleshooting, or when full portal access patching fails with a file or site.

In minimal patching mode, only HTML and CSS content is patched.

To use minimal patching, the following conditions must be met:

- You must create a local traffic pool for the application server or servers, and select it as the default pool in the virtual server definition.
- You must add a portal access resource item to the portal access resource, and configure it with host `*`, and port `0` (or any). In addition, the path /* must be specified in the resource item.
- You must configure the scheme `any`, not `http` or `https`.
- Minimal patching does not use a webtop, and will fail if one is assigned. For this reason, you must disable the **Publish on webtop** option, and you can not assign a webtop to the minimal patching access policy branch.

Important: *In minimal patching mode, if your web application sets cookies, the cookie domain must match the virtual server domain.*

Important: *If your web application does not use SSL, do not configure the virtual server with the Server SSL profile* `serverssl`.

Patching mode	Description
Scheme patching	Specifies a method of patching that replaces all HTTP scheme addresses with HTTPS scheme addresses.
Host Patching	Specifies a method of patching where one or multiple hosts (typically the actual application server host name) are replaced with another host, the Access Policy Manager® virtual server. You can specify multiple hosts separated with spaces for host search strings. The host replace string must be the Access Policy Manager virtual server IP address or fully qualified domain name (FQDN).

Chapter 2

Configuring Resources for Portal Access

Creating a portal access configuration

1. On the Main tab, click **Access Policy** > **Portal Access** > **Portal Access List**.
   The Portal Access List screen opens.
2. Click the **Create** button.
   The New Resource screen opens.
3. Type the name and an optional description.
4. From the **ACL Order** list, specify the placement for the resource.

Option	Description
Last	Select this option to place the new portal access resource last in the ACL list.
After	Select this option to select, from the list of configured ACLs, the ACL that this portal access resource should follow in sequence.
Specify	Select this option to specify an order number, for example, `0` or `631`for the ACL.

5. From **Configuration**, select **Basic** or **Advanced**.
   The **Advanced** option provides additional settings so you can configure a proxy host and port.
6. For the **Match Case for Paths** setting, select **Yes** to specify that portal access matches alphabetic case when matching paths in the portal access resource.
7. From the **Patching Type** list, select the patching type for the web application.
   For both full and minimal patching types, you can select or clear patching methods specific to your selection.
8. If you selected **Minimal Patching** and the **Host Patching** option, type a host search string, or multiple host search strings separated with spaces, and the host replace string, which must be the Access Policy Manager® virtual server IP address or fully qualified domain name.
9. To publish a link for the web application on the full webtop, or to use hosted content files, for the **Publish on Webtop** setting, select the **Enable** check box.

   Important: *Do not enable the* ***Publish on Webtop*** *setting if you are configuring the portal access resource for minimal patching.*

10. If you enabled **Publish on Webtop**, select whether the **Link Type** is an application URI or a file uploaded to the hosted content repository.
    - **Application URI:** This is the main URI used to start this portal access resource. You can configure other URIs with specific caching and compression settings by adding resource items to the portal access resource, after the main resource is configured.
    - **Hosted Content:** Use content uploaded to the hosted content repository to present on the webtop. When you select a hosted content file (typically a web-browser readable file), that file becomes the main destination for this webtop link.

      Note: *In the* ***Resource Items*** *area, you must add all resources that you have uploaded to the hosted content repository that apply to this particular hosted content link.*

11. In the Customization Settings for English area, in the **Caption** field, type a caption.
    The caption appears on the full webtop, and is required. This field is required even if you do not select the **Publish on webtop** option.

12. Optionally, in the **Detailed Description** field type a description for the web application.
13. In the **Image** field, specify an icon for the web application link. Click the **View/Hide** link to show the current icon.
14. If your application is behind a proxy server, to specify a proxy host and port, you must select **Advanced** for the configuration to display additional fields, and type the proxy host and proxy port.
15. Click the **Create** button.

This completes the portal access resource configuration.

Add resource items to the portal access resource to provide functionality for your web applications.

Creating a portal access resource item

You create a portal access resource item to add a port, path, and other portal access functionality to a portal access resource. If your portal access resource is a hosted content file (for example, a web application) you must add that file, and all related files from the hosted content repository that are used with the hosted content file. For example, you might add image files, CSS, and scripts that are required by the web page or application. You typically use resource items to refine the behavior for web application directories; for example, you might specify `No Compression` and a `Cache All` caching policy for the **/attachment** directory for a portal access resource.

1. On the Main tab, click **Access Policy** > **Portal Access** > **Portal Access List**.
   The Portal Access List screen opens.
2. Click the name of a portal access resource.
   The Portal Access Properties screen for that resource opens.
3. In the Resource Items area, click the **Add** button.
   A New Resource Item screen for that resource opens.
4. Select whether the resource item is application paths or hosted content.
   - **Paths:** If you select this option, set the host name or IP address, URI paths, the scheme, and the port.
   - **Hosted Content:** If you select this option, choose an item from the list of content uploaded to the hosted content repository

   Note: *You must add all files that you have uploaded to the hosted content repository that apply to this particular hosted content resource.*

5. Configure the properties for the resource item.
   - To add headers, select **Advanced** next to New Resource Item.
   - To configure **Session Update**, **Session Timeout**, and **Home Tab**, select **Advanced** next to Resource Item Properties.
6. Click **Finished**.
   This creates the portal access resource item.

Portal access resource item properties

Use these properties to configure a resource item for a portal access resource.

Property	Value	Description
Item Type	Paths or Hosted Content	Specifies whether the resource item is a path to a web resource or an uploaded file from the hosted content repository.

Property	Value	Description
Destination	Host name, IP address, or network address and mask	Specifies whether the web application destination is a host or an IP address, and provides the host name or IP address. You can specify an IPv4 or IPv6 IP address, or a host name that resolves to either an IPv4 or IPv6 address. When a resource is configured using the host name, and the host name resolves to both IPv4 and IPv6 addresses, the IP address family preference setting in the client's DNS configuration is used to choose the IP address type from the DNS response.
Hosted Files	A local file	If the item type is Hosted Content, you can select a local file from this list to specify as the resource. ***Important:*** *If the portal access resource is a hosted content file, all related files must be defined separately as portal access resource items within that portal access resource.*
Port	A port number or **0**	Specifies the port for the web application. `0` means the web application matches port `80` for the **http** scheme option, and port `443` for the **https** scheme option.
Scheme	**http**, **https**, or **any**	Specifies whether the URI scheme for the web application is **http**, **https**, or any (either HTTP or HTTPS) scheme.
Paths	An application path or paths, separated by spaces	Specifies any paths for the web application. You can separate multiple paths with spaces. You can use wildcards, for example `/*`.
Headers	Name-value pairs	Specifies any custom headers required by the web application. To add a header, type the header name in the **Name** field, and the header content in the **Value** field, then click the **Add** button.
Compression	**No compression** or **GZIP compression**	**No Compression** specifies that application data sent to the client browser is not compressed. **GZIP Compression** specifies that application data sent to the client browser is compressed with GZIP compression. ***Important:*** *To use GZIP compression with a portal access resource, in the virtual server definition, you must specify the* ***HTTP Compression Profile*** *setting as* `httpcompression`*.*
Client Cache	**Default**, **Cache All**, or **No Cache**	Specifies settings for client caching of web applications. In the rewrite profile that you associate with the virtual server for the portal access resource, you can specify a client caching option: **CSS and JavaScript**, **CSS, Images and JavaScript**, **No Cache** or **Cache All**. If you configure a client cache setting other than **Default** in the portal access resource item, that resource setting overrides the cache setting in the rewrite profile. • **Default** uses the client cache settings from the rewrite profile. • **Cache All** uses cache headers as is from the back-end server, and allows caching of everything that can be cached, including CSS, images, JavaScript®, and XML. May provide better client performance and lower security depending on the server configuration. • **No Cache** caches nothing. This provides the slowest client performance and is the most secure.

Property	Value	Description
SSO Configuration	SSO configuration, selected from a list of available SSO configurations	Specifies an SSO configuration to use with the portal access resource item for Single Sign-On.
Session Update	Enable or disable	Some application web pages that start through portal access connections contain JavaScript code that regularly refreshes the page or sends HTTP requests, regardless of user activity or inactivity. A session that is abandoned at such a site does not time out, because it appears to be active. When disabled, the session update feature prevents these sessions from remaining active indefinitely.
Session Timeout	Enable or disable	Enables or disables session timeouts.
Home Tab	Enable or disable	This option inserts into HTML pages a small amount of HTML code that includes the JavaScript that displays the home tab, which contains links to the Home and Logout functions and a URL bar. To enable the home tab on a web application page, select the **Home Tab** check box. Web pages generated without the home tab JavaScript code contain no home or logout links. You can customize the appearance and configuration of the home tab on the webtop customization page. When you start a web application from the full webtop, the home tab is displayed on the webtop only, and not on web pages launched from the webtop, regardless of this setting.
Log	**None** or **Packet**	Specifies the log level that is logged when actions of this type occur.

Creating a portal access resource item for minimal patching

Create a portal access resource item to add an port, path and other portal access functionality to a portal access resource. You typically use resource items to refine the behavior for web application directories; for example, you might specify `No Compression` and a `Cache All` caching policy for the **/attachment** directory for a portal access resource.

1. On the Main tab, click **Access Policy** > **Portal Access**.
   The Portal Access List screen opens.
2. Click the name of a portal access resource that is configured for minimal patching.
   The Portal Access Resource Properties screen opens.
3. In the Resource Items area, click **Add**.
   The New Resource Item screen opens.
4. In the **Host Name** field, type an asterisk `*`.
5. From the **Scheme** list, select `any`.
   When you select `any`, the port changes correctly to `0`.
6. In the **Paths** field, type `/*` .
7. Click **Finished**.
   The portal access resource item is created.

This creates the portal access resource item required for a minimal patching configuration.

Creating a portal access configuration with the wizard

You can use the portal access wizard to quickly configure an access policy, resource, resource item, and a virtual server to allow portal access connections.

1. ***Tip:*** *Follow the instructions in the wizard to create your access policy and virtual server.*

   On the Main tab, click **Wizards** > **Device Wizards**.
2. Select **Portal Access Setup Wizard** and click **Next**.
3. Type the **Policy Name**, select the default language, and specify whether to enable the simple antivirus check in the access policy.
4. Click **Next**.
5. On the Select Authentication wizard screen, configure authentication. You can select an existing authentication server configured on the Access Policy Manager®, or you can create a new authentication configuration.

   For a full discussion of Access Policy Manager authentication, see the *BIG-IP® Access Policy Manager® Authentication Configuration Guide*.
6. On the Portal Access screen, select a portal access application.

Option	Description
DWA	Configures a Domino Web Access configuration with common settings.
OWA2003	Configures an Outlook® Web Access 2003 configuration with common settings.
OWA2007	Configures an Outlook Web Access 2007 configuration with common settings.
OWA2010	Configures an Outlook Web Access 2010 configuration with common settings.
Custom	Allows you to configure custom settings for a portal access configuration.

7. In the **Portal Access Start URI** field, type the applicable URI.
8. To configure SSO with the portal access configuration, select the **Configure SSO** check box.

   If you enable this setting, you also select the SSO method from the **SSO Method** list.
9. Click **Next**.
10. In the **Virtual Server IP address** field, type the IP address for your virtual server.

    Select the **Create Redirect Virtual Server** check box to create a redirect for clients who attempt to connect over HTTP instead of HTTPS.
11. Click **Next**.
12. Review the configuration.

    You can click **Next** to accept the configuration and create the portal access configuration, **Back** to go back and change settings, or **Cancel** to discard the configuration.

Configuration is complete. You can test the portal access resource by browsing to the virtual server address.

Creating a portal access configuration with a template

You can create a portal access resource with a template for a common application, to add when you configure an access policy. When you create a portal access configuration with a template, you create the portal access resource, along with common resource items for the configuration.

1. On the Main tab, click **Access Policy** > **Portal Access**.
2. Click the **Create with Template** button.
3. Type a name for the portal access resource.
4. From the **Template** list, select a portal access application template.
   - **DWA** - Configures a Domino Web Access configuration with common settings.
   - **OWA2003** - Configures an Outlook Web Access 2003 configuration with common settings.
   - **OWA2007** - Configures an Outlook Web Access 2007 configuration with common settings.
   - **OWA2010** - Configures an Outlook Web Access 2010 configuration with common settings.
5. From the **Order** list, specify the sequence for the resource.

Option	Description
Last	Select this option to place the new portal access resource last in the ACL list.
After	Select this option to select, from the list of configured ACLs, the ACL that this portal access resource should follow in sequence.
Specify	Select this option to specify an order number, for example, `0` or `631` for the ACL.

6. For the **Destination** setting, select **Host Name** or **IP Address** for the resource address, then type the resource address in the corresponding field or fields.
7. Click the **Finished** button.

The Access Policy Manager® creates a portal access resource and the associated common resource items from the template.

You can add resource items to the portal access resource, to provide more functionality for your web applications.

Chapter 3

Configuring Webtops for Portal Access

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.*

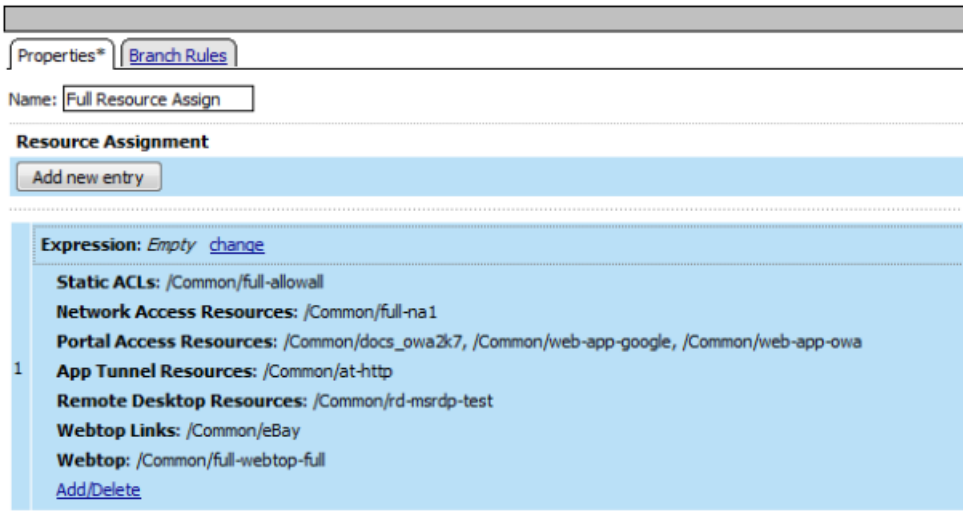

Figure 2: Resource assign action with resources and a webtop assigned

Configuring a webtop for portal access only

A webtop provides a screen for your users to connect and disconnect from the portal access connection.

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 **Portal Access**.

5. In the **Portal Access Start URI** field, specify the URI that the webtop starts.
6. 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.

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

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.

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.

Chapter 4

Configuring Access Profiles for Portal Access

Creating an access profile

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

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

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

4. From the **Profile Type** list, select **SSL-VPN**.
   Additional settings display.
5. To configure timeout and session settings, select the **Custom** check box.
6. In the **Inactivity Timeout** field, type the number of seconds that should pass before the access policy times out. Type `0` to set no timeout.

   If there is no activity (defined by the **Session Update Threshold** and **Session Update Window** settings in the Network Access configuration) between the client and server within the specified threshold time, the system closes the current session.
7. In the **Access Policy Timeout** field, type the number of seconds that should pass before the access profile times out because of inactivity.

   Type `0` to set no timeout.
8. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.

   Type `0` to set no timeout.
9. In the **Max Concurrent Users** field, type the maximum number of users that can use this access profile at the same time.

   Type `0` to set no maximum.
10. In the **Max Sessions Per User** field, type the maximum number of concurrent sessions that one user can start.

    Type `0` to set no maximum.
11. In the **Max In Progress Sessions Per Client IP** field, type the maximum number of concurrent sessions that one client IP address can support.

    Type `0` to set no maximum.
12. Select the **Restrict to Single Client IP** check box to restrict the current session to a single IP address.

    This setting associates the session ID with the IP address.

    Upon a request to the session, if the IP address has changed the request is redirected to a logout page, the session ID is deleted, and a log entry is written to indicate that a session hijacking attempt was detected. If such a redirect is not possible, the request is denied and the same events occur.
13. To configure logout URIs, in the Configurations area, type each logout URI in the **URI** field, and then click **Add**.
14. In the **Logout URI Timeout** field, type the delay in seconds before logout occurs for the customized logout URIs defined in the **Logout URI Include** list.
15. To configure SSO:

- For users to log in to multiple domains using one SSO configuration, skip the settings in the SSO Across Authentication Domains (Single Domain mode) area. You can configure SSO for multiple domains only after you finish the initial access profile configuration.
- For users to log in to a single domain using an SSO configuration, configure settings in the SSO Across Authentication Domains (Single Domain mode) area, or you can configure SSO settings after you finish the initial access profile configuration.

16. In the **Domain Cookie** field, specify a domain cookie, if the application access control connection uses a cookie.
17. In the **Cookie Options** setting, specify whether to use a secure cookie.
    - If the policy requires a secure cookie, select the **Secure** check box to add the **secure** keyword to the session cookie.
    - If you are configuring an LTM access scenario that uses an HTTPS virtual server to authenticate the user and then sends the user to an existing HTTP virtual server to use applications, clear this check box.
18. If the access policy requires a persistent cookie, in the **Cookie Options** setting, select the **Persistent** check box.

    This sets cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent; but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value will be used to set the persistent cookie expiration.
19. From the **SSO Configurations** list, select an SSO configuration.
20. 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.
21. Click **Finished**.

The access profile appears in the Access Profiles List.

To add an SSO configuration for multiple domains, click **SSO / Auth Domains** on the menu bar. To provide functionality with an access profile, you must configure the access policy. The default access policy for a profile denies all traffic and contains no actions. Click **Edit** in the **Access Policy** column to edit the access policy.

Configuring an access policy

You configure an access policy to provide authentication, endpoint checks, and resources for an access profile. This procedure configures a simple access policy that adds a logon page, gets user credentials, submits them to an authentication type of your choice, then allows authenticated users, and denies others.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile you want to edit.
3. On the menu bar, click **Access Policy**.
4. For the **Visual Policy Editor** setting, click the **Edit access policy for Profile** ***policy_name*** link.
   The visual policy editor opens the access policy in a separate window or tab.
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 Logon tab, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent properties screen opens.
7. Click **Save**.
   The Access Policy screen reopens.
8. On the rule branch, click the plus sign **(+)** between **Logon Page** and **Deny**.
9. Set up the appropriate authentication and client-side checks required for application access at your company, and click **Add Item**.
10. Change the Successful rule branch from **Deny** to **Allow** and click the **Save** button.
11. If needed, configure further actions on the successful and fallback rule branches of this access policy item, and save the changes.
12. At the top of the screen, click the **Apply Access Policy** link to apply and activate your changes to this access policy.
13. Click the **Close** button to close the visual policy editor.

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.

Adding connection resources to an access policy

Before you start this task, you must have an access profile created.

You add the resource assign action to an access policy to add a network access resource, portal access resources, application tunnel resources, and remote desktop resources to an access policy branch.

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 **Resource Assign** and click the **Add Item** button.
   This opens the Resource Assignment popup window.
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 Resource Assign screen, next to the type of resource you want to add, click the **Add/Delete** link.
   This expands the screen to display options for the resource you selected.
9. To assign resources, select the options you want.
10. Assign resources using the heading options on the screen.

Option	Description
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.

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. To assign a webtop and webtop links, add the Webtop and Links Assign action after this action.

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

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.

Access profile settings

You can configure the following settings in an access profile.

Setting	Value	Description and defaults
Name	Text	Specifies the name of the access profile.
Inactivity Timeout	Number of seconds, or `0`	Specifies the inactivity timeout for the connection. If there is no activity between the client and server within the specified threshold time, the system closes the current session. By default, the threshold is `0`, which specifies that as long as a connection is established, the inactivity timeout is inactive. However, if an inactivity timeout value is set, when server traffic exceeds the specified threshold, the inactivity timeout is reset.
Access Policy Timeout	Number of seconds, or `0`	Designed to keep malicious users from creating a denial-of-service (DoS) attack on your server. The timeout requires that a user, who has followed through on a redirect, must reach the webtop before the timeout expires. The default value is `300` seconds.
Maximum Session Timeout	Number of seconds, or `0`	The maximum lifetime is from the time a session is created, to when the session terminates. By default, it is set to `0`, which

Setting	Value	Description and defaults
		means no limit. When you configure a maximum session timeout setting other than `0`, there is no way to extend the session lifetime, and the user must log out and then log back in to the server when the session expires.
Max Concurrent Users	Number of users, or `0`	The number of sessions allowed at one time for this access profile. The default value is `0` which specifies unlimited sessions.
Max Sessions Per User	Number between `1` and `1000`, or `0`	Specifies the number of sessions for one user that can be active concurrently. The default value is `0`, which specifies unlimited sessions. You can set a limit from `1`-`1000`. Values higher than `1000` cause the access profile to fail. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*
Max In Progress Sessions Per Client IP	Number `0` or greater	Specifies the maximum number of sessions that can be in progress for a client IP address. When setting this value, take into account whether users will come from a NAT-ed or proxied client address and, if so, consider increasing the value accordingly. The default value is **0** which represents unlimited sessions. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*
Restrict to Single Client IP	Selected or cleared	When selected, limits a session to a single IP address. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*
Logout URI Include	One or more URIs	Specifies a list of URIs to include in the access profile to initiate session logout.
Logout URI Timeout	Logout delay URI in seconds	Specifies the time delay before the logout occurs, using the logout URIs defined in the logout URI include list.
SSO Authentication Across Domains (Single Domain mode) or SSO / Auth Domains: **Domain Cookie**	A domain cookie	If you specify a domain cookie, then the line `domain=`*`specified_domain`* is added to the `MRHsession` cookie.
SSO / Auth Domains: **Domain Mode**	**Single Domain** or **Multiple Domains**	Select **Single Domain** to apply your SSO configuration to a single domain. Select **Multiple Domain** to apply your SSO configuration across multiple domains. This is useful in cases where you want to allow your users a single Access Policy Manager® (APM®) login session and apply it across multiple Local Traffic Manager™ or APM virtual servers, front-ending different domains. ***Important:*** *All virtual servers must be on one single BIG-IP® system in order to apply SSO configurations across multiple domains.*

Setting	Value	Description and defaults
SSO / Auth Domains: **Primary Authentication URI**	URI	The URI of your primary authentication server, for example `https://logon.siterequest.com`. This is required if you use SSO across multiple domains. You provide this URI so your users can access multiple back-end applications from multiple domains and hosts without requiring them to re-enter their credentials, because the user session is stored on the primary domain.
Cookie Options: **Secure**	Enable or disable check box	Enabled, this setting specifies to add the **secure** keyword to the session cookie. If you are configuring an application access control scenario where you are using an HTTPS virtual server to authenticate the user, and then sending the user to an existing HTTP virtual server to use applications, clear this check box.
Cookie Options: **Persistent**	Enable or disable check box	Enabled, this setting specifies to set cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent, but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. ***Note:*** *Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to the session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value is used to set the persistent cookie expiration.*
Cookie Options: **HTTP only**		HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Use the HttpOnly flag when generating a cookie to help mitigate the risk of a client-side script accessing the protected cookie, if the browser supports HttpOnly. When this option is enabled, only the web access management type of access (an LTM virtual server with an access policy) is supported.
SSO Authentication Across Domains (Single Domain mode) or SSO / Auth Domains **SSO Configuration**	Predefined SSO configuration	SSO configurations contain settings to configure single sign-on with an access profile. Select the SSO configuration from the list that you want applied to your domain.
SSO / Auth Domains: Authentication Domains	Multiple	If you specify multiple domains, populate this area with hosts or domains. Each host or domain can have a separate SSO config, and you can set persistent or secure cookies. Click **Add** to add each host you configure.
Accepted Languages	Language strings	Adds a built-in or customized language to the list of accepted languages. Accepted languages can be customized separately and can present customized messages and screens to users, if the user's default browser language is one of the accepted languages. Select a language from the **Factory Builtin Languages** list and click the Move button (**<<**) to add it to the **Accepted Languages** list. Select a language from the **Additional Languages** list and click **Add** to add it to the **Accepted Languages** list.

Setting	Value	Description and defaults
Factory Builtin Languages	Languages in a predefined list	Lists the predefined languages on the Access Policy Manager system, which can be added to the **Accepted Languages** list. Predefined languages include customized messages and fields for common appearance items, as opposed to **Additional Languages**, which must be separately customized.
Additional Languages	Languages in a predefined list	Lists additional languages that can be added to the **Accepted Languages** list, and customized on the Access Policy Manager system. These languages are populated with English messages and fields and must be individually customized using the Customization menu, as opposed to **Factory Builtin Languages**, which are already customized.

Chapter 5

Configuring Rewrite Profiles for Portal Access

About rewrite profiles for Portal Access

A Portal Access rewrite profile defines certificate settings for Java patching, client caching settings for a virtual server, split tunneling settings, and URI translation settings. You can configure a rewrite profile and select the rewrite profile when you configure the virtual server for a portal access policy. Alternatively, you can use the default Portal Access rewrite profile, `rewrite-portal`.

Portal access rewrite profile Portal Access settings

Use these properties to configure a resource item for a portal access resource.

In the rewrite profile Portal Access settings, you can configure settings for client caching and split tunneling.

These options are available for Portal Access in the rewrite profile.

Client Cache setting	Description
CSS and JavaScript	Caches CSS and JavaScript. This is the default rewrite caching configuration, and provides a balance between performance and security.
CSS, Images and JavaScript	Caches CSS, images, and JavaScript. This provides faster client performance but is slightly less secure because of cached images in the client browser cache.
No Cache	Caches nothing. This provides the slowest client performance and is the most secure.
Cache All	Uses the unmodified cache headers from the backend server.

Enable split tunneling: Set this option to **Yes** to enable split tunneling for portal access sessions that use this rewrite profile. Set this option to **No** to force all traffic through the tunnel for portal access sessions that use this rewrite profile.

About split tunneling with rewrite profiles

Consider these factors when split tunneling is enabled:

- Access Policy Manager matches the URI to the expressions specified on the **Bypass** list first. If an expression matches, then the URI is bypassed and links are not rewritten.
- If the URI does not match the **Bypass** list, then it is compared to the **Rewrite** list. If the URI matches the expressions specified on the **Rewrite** list, the URI links are rewritten. If there are no matches, links are not rewritten.
- If the URI does not match anything on the **Bypass** or **Rewrite** lists, and if the host name in the URI is a short name, not a fully qualified domain name, then links for that URI are rewritten.

Portal access rewrite profile JavaPatcher settings

Use these properties to configure a resource item for a portal access resource.

In a rewrite profile, you can configure settings for Java patching. These settings configure certificate authorities, signing rights, and certificate revocation that is required for to patch some Java apps.

These options are available for JavaPatcher in the rewrite profile.

Setting	Value	Description
Trusted Certificate Authorities	List selection	Select the certificate authority to use for Java app link rewriting from the list of predefined Certificate authorities on the system, to use with Java app rewriting.
Signer	List selection	Select the Java app signer to use for app re-signing, from a list of existing signers on the system. Select None if the app is unsigned.
Signing Key	List selection	Select the private key from a list of existing keys on the system for Java app re-signing. Select None if the app is unsigned or does not require a signing key.
Signing Key Pass Phrase	Text (obscured)	To encrypt the private signing key with a passphrase, type the private key pass phrase.
Certificate Revocation List (CRL)	List selection	Select the CRL from the list, if one is defined on the system.

Portal access rewrite profile URI translation settings

Use these properties to configure URI translation for a rewrite profile with Portal Access.

In a rewrite profile, you can configure settings for rewriting headers in the request and the response.

These options are available for URI translation in Request Settings.

Property	Description
Rewrite Headers	Select this option to rewrite headers in Request Settings.
Insert X-Forwarded For Header	Select this option to add the X-Forwarded For (XFF) header, to specify the originating IP address of the client.
Insert X-Forwarded Proto Header	Select this option to add the X-Forwarded Proto header, to specify the originating protocol of the client.
Insert X-Forwarded Host Header	Select this option to add the X-Forwarded Host header, to specify the originating host of the client.

These options are available for URI translation in Response Settings.

Property	Description
Rewrite Headers	Select this option to rewrite headers in the response.
Rewrite Content	Select this option to rewrite links in content in the response.

Creating a rewrite profile

You can create a rewrite profile to specify the rewriting and bypass lists, and define client caching in the virtual server definition.

1. Click **Access Policy** > **Portal Access** > **Rewrite Profiles**.
   The Rewrite Profile List screen opens.
2. Click **Create New Profile**.
   The Create New Profile Rewrite screen opens.
3. In the **Name** field, type a name for the rewrite profile.
4. From the **Parent Profile** list, select a parent profile.

   For Portal Access, you should select the `/Common/rewrite` or `/Common/rewrite-portal` profile as the parent. The new rewrite profile inherits the **Client Caching Type** setting from the parent profile.
5. From the **Rewrite Mode** list, select **Portal (Access)**.
6. On the left side, click the Portal (Access) link.
7. From the **Client Caching Type** list, select the caching option.
8. To enable split tunneling for portal access connections, select **Split Tunneling** from the list.

   Split tunneling provides two options to access your web page: **Rewrite** and **Bypass**. If you enable split tunneling, Access Policy Manager® presents only web pages that satisfy one of these filters. Others are blocked (although a blocked public site may still be available outside the webtop). If you do not use split tunneling, Access Policy Manager processes all portal access URLs through the rewriting engine. You can specify a URL pattern using the following syntax: `scheme: //host[:port]/path`. You can also use wildcards such as the asterisk (*) to denote any sequence of characters and the question mark (?) for any single character. Access Policy Manager rewrites links in all pages specified for **Rewrite**.

   - **Rewrite** - Rewrites URLs. When you use this option, Access Policy Manager controls the redirection of the URL. Use this option to access URLs inside the network. Type a URL match pattern for the sites where you need to create the reverse-proxy and click the **Add to Rewrite List** button.
   - **Bypass** - Directly accesses the URL and leaves the URL unmodified. Use this option to speed up serving public sites. Type a URL match pattern for URLs to be accessed directly, bypassing the rewrite engine, and click the **Add to Bypass List** button.
9. To configure Java patching, click **JavaPatcher Settings**. Configure the Java Patcher options for verification and re-signing of signed applets.
10. To configure the **Trusted Certificate Authorities**, from the list select a CA against which to verify signed applets signatures.
11. To configure a **Signer**,from the list select a certificate to use for re-signing.
12. To configure a **Signing Key**, from the list select a corresponding private key for re-signing.
13. To set a **Signing Key Pass Phrase**, type a passphrase with which to encrypt the private key.
14. To select a **Certificate Revocation List (CRL)**, from the list select a CRL with which to check certificate validity.
15. To configure URI Translation request and response settings, under **URI Translation** select **Settings**.
16. Configure translation settings.
17. Click **OK** to complete the rewrite profile.

The rewrite profile appears in the Rewrite Profiles list.

To use this profile for portal access rewriting, you must next assign the rewrite profile to the virtual server that is also assigned the access profile for portal access.

Chapter 6

Configuring Virtual Servers for Portal Access

Defining a virtual server for portal access

You associate an access policy and a rewrite profile with the virtual server, to allow portal access in an access policy.

Important: *For portal access, 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. To use GZIP compression with a portal access resource, from the **HTTP Compression Profile** list, select **httpcompression**.
7. If you are using a connectivity profile, from the **Connectivity Profile** list, select the connectivity profile.
8. 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.
9. If you use client SSL for this profile, from the **SSL Profile (Client)** list, select a client SSL profile.
10. If you are using HTTPS with any portal access pages, from the **SSL Profile (Server)** list, select **serverssl-apm**.
11. 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.
12. 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.
13. Click **Update**.

Your access policy is now associated with the virtual server.

Chapter 7

Integrating Portal 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.*

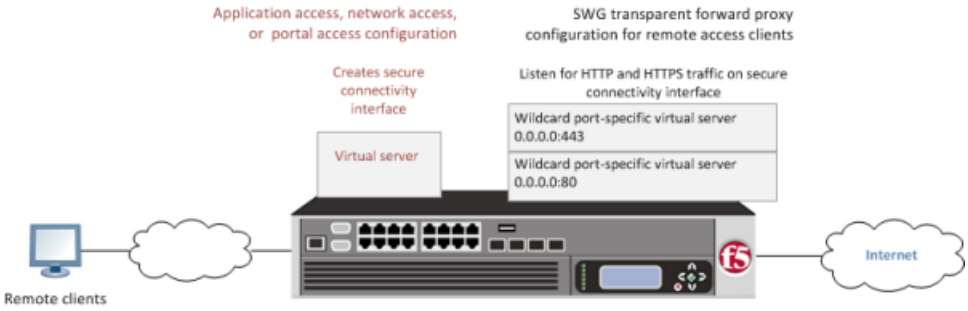

Figure 3: SWG transparent forward proxy for remote access

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 8

Hosting Files with Portal Access on Access Policy Manager

About using hosted files with a Portal Access resource

You can use hosted content that you have uploaded to the BIG-IP® Access Policy Manager™ to provide the resource and resource items for a Portal Access resource.

When you use hosted content for a Portal Access resource, the link on the webtop for the portal access resource opens a file hosted on the system, instead of a URI. You configure the main Portal Access resource as this linked file. You then configure this file, and all related and required files, as resource items of this file.

In this example, a simple web page consisting of an HTML file, a CSS file, a JavaScript file, and an image are uploaded to a directory in the hosted content repository. The files are then specified as a Portal Access resource and resource items.

File	Location	Description
index.html	`/index.html`	The main web page that displays when the link is clicked. This is the Portal Access Resource.
styles.css	`/styles.css`	The CSS file for the page index.html.
test_image.jpg	`/test_image.jpg`	An image that is referenced on the page index.html.
script.js	`/js/script.js`	A JavaScript file that is referenced from the page index.html.

In this example, hosted content is uploaded as a single **ZIP** file, `test.zip`, then extracted to the location `/test` on the server.

Task summary

To add hosted content to a Portal Access link on Access Policy Manager®, complete these tasks.

Task summary

Uploading files to Access Policy Manager for Portal Access
Associating hosted content with access profiles
Creating a portal access configuration with hosted content
Creating a portal access resource item for hosted content

Uploading files to Access Policy Manager for Portal Access

You upload files to Access Policy Manager® to provide content for a Portal Access webtop link.

Tip: *Before you upload multiple files to Access Policy Manager, you can combine the files in a ZIP archive format. Then, you can upload and extract the files in one step. In this example, four files are uploaded as a single ZIP archive, called* `test.zip`*.*

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.

2. Click the **Upload** button.
   The Create New File popup screen opens.
3. Under **Select File**, click the **Browse** button. Browse and select **test.zip**.
   The **Select File** and **File Name** fields are populated with the file name.
4. In the **File Destination Folder** field, specify the folder path `/test` in which to place the file.
5. From the **File Action** list, select **Upload and Extract**.
6. Click the **OK** button.
   The files appears in the hosted content list, in the folder specified. Any files in subfolders in the archive file also appear in subfolders in the hosted content list.

You must associate any access profiles that will access hosted content with the hosted content repository.

Associating hosted content with access profiles

A user can access hosted content that is associated with that user's access profile. Each access profile that requires hosted content access must be associated with the entire hosted content repository.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. On the **Upload** button, click the right-side arrow to select **Manage Access** from the list.
   The Access Settings popup screen opens.
3. Select the access profiles to associate with hosted content, then click **OK**.
   A user must belong to an associated access profile to access hosted content.

View the hosted content list, and verify that the access policy association was successful.

Creating a portal access configuration with hosted content

1. On the Main tab, click **Access Policy** > **Portal Access** > **Portal Access List**.
   The Portal Access List screen opens.
2. Click the **Create** button.
   The New Resource screen opens.
3. Type the name and an optional description.
4. From the **ACL Order** list, specify the placement for the resource.

Option	Description
Last	Select this option to place the new portal access resource last in the ACL list.
After	Select this option to select, from the list of configured ACLs, the ACL that this portal access resource should follow in sequence.
Specify	Select this option to specify an order number, for example, `0` or `631`for the ACL.

5. From **Configuration**, select **Basic** or **Advanced**.
   The **Advanced** option provides additional settings so you can configure a proxy host and port.
6. For the **Match Case for Paths** setting, select **Yes** to specify that portal access matches alphabetic case when matching paths in the portal access resource.
7. From the **Patching Type** list, select the patching type for the web application.

For both full and minimal patching types, you can select or clear patching methods specific to your selection.

8. If you selected **Minimal Patching** and the **Host Patching** option, type a host search string, or multiple host search strings separated with spaces, and the host replace string, which must be the Access Policy Manager® virtual server IP address or fully qualified domain name.
9. Select the **Publish on Webtop** check box.
10. From the **Link Type** list, select **Hosted Content**.
11. From the **Hosted File** list, select `public/share/test/index.html`.

    This is the filename for this example scenario only. Please select the correct file for your own configuration.
12. In the Customization Settings for English area, in the **Caption** field, type a caption.

    The caption appears on the full webtop, and is required. This field is required even if you do not select the **Publish on webtop** option.
13. Optionally, in the **Detailed Description** field type a description for the web application.
14. In the **Image** field, specify an icon for the web application link. Click the **View/Hide** link to show the current icon.
15. If your application is behind a proxy server, to specify a proxy host and port, you must select **Advanced** for the configuration to display additional fields, and type the proxy host and proxy port.
16. Click the **Create** button.
    The Portal Access resource is saved, and the Portal Access Resource screen now shows a **Resource Items** area.

This completes the portal access resource configuration.

Specify all hosted content files used by this example (all files in the `/test` folder) as resource items.

Creating a portal access resource item for hosted content

You create a portal access resource item in order for hosted content to add a file that is part of a portal access hosted content resource. For example, you might add image files, CSS files, or scripts that are required by the web page or application. You typically use resource items to refine the behavior for web application directories; for example, you might specify `No Compression` and a `Cache All` caching policy for the images for a portal access resource.

Note: *You must add (separately) each hosted file used by the portal access resource, and the resource file itself, as resource items.*

---

1. On the Main tab, click **Access Policy** > **Portal Access** > **Portal Access List**.
   The Portal Access List screen opens.
2. Click the name of a portal access resource.
   The Portal Access Properties screen for that resource opens.
3. In the Resource Items area, click the **Add** button.
   A New Resource Item screen for that resource opens.
4. Select that the resource item type is **Hosted Content**.
5. From the **Hosted File** list, select the file to specify as a resource item.

   For purposes of this example, specify `public/share/test/index.html`, `public/share/test/test_image.jpg`, `public/share/test/style.css`, and `public/share/test/js/script.js`.
6. Configure the properties for the resource item.

- To add headers, select **Advanced** next to New Resource Item.
- To configure **Session Update**, **Session Timeout**, and **Home Tab**, select **Advanced** next to Resource Item Properties.

7. Click **Finished**.
   This creates the portal access resource item.

Implementation result

You have now added a portal access resource and portal access resource items that are based on uploaded hosted content.

Chapter 9

Adding Hosted Content to Access Policy Manager

About uploading custom files to Access Policy Manager

You can upload custom files to BIG-IP® Access Policy Manager®(APM®) to provide resources directly to users.

For example, you can upload BIG-IP Edge Client® installers, antivirus or firewall update packages, or Citrix receiver files for your users to download. You can upload custom images, web pages, Java archives, JavaScript files, CSS files, archive files, and many other types of files as well.

Optionally, you can compress and upload multiple files as a single ZIP archive file. When you upload an archive file, you can choose to either upload the compressed file, or upload and extract the compressed file.

Upload Only
Select this option to upload an archived file that must remain in archive format. For example, you can upload a ZIP file for a user to download, containing a package of documents, or an application and related files. Some applications also use archived files; for example, you will upload a JAR file without extracting it.

Upload and Extract
Select this option to upload an archived file and extract it to the specified location. The folder hierarchy of the extracted file is preserved when you use this action. Select this option when you are uploading a collection of files that must be separated on the server for use by the end user; for example, to upload a web application that includes top-level HTML files, and subdirectories containing scripts, images, CSS, and other files.

Understanding hosted content

Hosted content is any type of file you would like to serve from Access Policy Manager® (APM®) to access policy users. Hosted content can include executable files, scripts, text, HTML, CSS files, and image files. You can serve hosted content from a webtop link, or from a portal access link.

About accessing hosted content

To access hosted content, a user must belong to an access profile that is associated with the hosted content. After content is uploaded to Access Policy Manager® (APM®), the entire hosted content library must be associated with one or more access profiles. These access profiles alone can view the content.

In addition, each file uploaded to the hosted content repository is assigned a permission level that determines the users who can access that content.

Permissions for hosted content

A permission level is assigned to each file in the hosted content repository, as described here.

Permission level	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result, and an access profile associated with the hosted content repository. You can assign

Permission level	Description
	this to display an HTML file that only a verified user can see.
public	The file is available to anyone with an access profile associated with the hosted content repository. You can assign this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session and an access profile associated with the hosted content repository. You can assign this to allow a user with an active session access to a required logon component.

Task summary

To add hosted content to Access Policy Manager®, complete these tasks.

Task summary

Uploading files to Access Policy Manager

Associating hosted content with access profiles

Uploading files to Access Policy Manager

Before you upload multiple files to Access Policy Manager®, you can compress and combine the files into a ZIP archive file. Then, you can upload and extract the files in one step.

You can upload files to Access Policy Manager to provide content for public viewing, to provide pages and content to Portal Access connections, or to provide customized webtop links.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Click the **Upload** button.
   The Create New File popup screen opens.
3. For the **Select File** setting, click the **Browse** button and select the file to upload.
   - To upload each file separately, select the first file, then repeat this step for all remaining files.
   - To upload all files at once from a compressed file, select the compressed file.

   The **Select File** and **File Name** fields are populated with the file name.
4. If you are uploading a compressed file that you want to extract, from the **File Action** list, select **Upload and Extract**.
5. Click **OK**.
   The file appears in the hosted content list.

You must associate any access profiles that will access hosted content with the hosted content repository.

Associating hosted content with access profiles

A user can access hosted content that is associated with that user's access profile. Each access profile that requires hosted content access must be associated with the entire hosted content repository.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. On the **Upload** button, click the right-side arrow to select **Manage Access** from the list.
   The Access Settings popup screen opens.
3. Select the access profiles to associate with hosted content, then click **OK**.

   A user must belong to an associated access profile to access hosted content.

View the hosted content list, and verify that the access policy association was successful.

Implementation result

As a result of these implementation tasks, you have edited files and deleted hosted files on Access Policy Manager® as necessary.

Chapter 10

Editing Hosted Content with Access Policy Manager

About editing hosted files on Access Policy Manager

You can upload custom files to BIG-IP® Access Policy Manager® to provide resources directly to users.

You might need to edit files after you upload them to Access Policy Manager, such as to rename a file or change the file MIME type. You can make these changes using the hosted content settings.

Task summary

To edit hosted content on Access Policy Manager®, complete these tasks.

Task summary

Renaming or moving hosted content files
Editing hosted content file properties
Replacing a hosted file
Deleting a hosted file

Renaming or moving hosted content files

You can rename or move a hosted content file on Access Policy Manager®.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Rename/Move File** from the list.
   The **Rename/Move File Properties** popup screen opens.
3. In the **New File Name** field, type a new name for the file.
4. In the **New File Destination Folder**, specify a new destination folder for the file.
5. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

Editing hosted content file properties

You can edit the permissions and MIME type for hosted content files on Access Policy Manager®.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Edit File Properties** from the list.
   The **Edit File Properties** popup screen opens.
3. If the MIME type for the file is incorrect or must be changed, from the **Mime Type** list, select the MIME type for the file.
4. From the **Secure Level** menu, select the access level for the file.

Option	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result. You might use this to display an HTML file that only a verified user can see.
public	The file is available to anyone. You might use this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session. You might use this to allow a user with an active session access to a required logon component.

5. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

The settings for the file are displayed in the Hosted Content list.

Replacing a hosted file

You can upload a new version of a file to hosted content, to replace the current file on Access Policy Manager®.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Upload New Version** from the list.
   The **Upload New File Version** popup screen opens.
3. For the **Select File** setting, click the **Browse** button and select the file to upload.
   The **Select File** and **File Name** fields are populated with the file name.
4. If the MIME type for the file is incorrect or must be changed, from the **Mime Type** list, select the MIME type for the file.
5. From the **Secure Level** menu, select the access level for the file.

Option	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result. You might use this to display an HTML file that only a verified user can see.
public	The file is available to anyone. You might use this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session. You might use this to allow a user with an active session access to a required logon component.

6. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

View the hosted content list to verify your changes to the file.

Deleting a hosted file

You can delete one or more files from the hosted content on Access Policy Manager®.

1. On the Main tab, click **Access Policy** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Select one or more files to delete. To select all files, select the check box at the top of the list, next to the Name column.
3. Click **Delete**, and in the **Delete File** popup screen that opens, click **Yes**.

The files are removed from the list.

Implementation result

As a result of these implementation tasks, you have edited files and deleted hosted files on Access Policy Manager® as necessary.

Index

R

S

T

U

V

W