BIG-IP® Access Policy Manager® Portal Access Guide

Version 11.2

IT agility. Your way.

Table of Contents

Legal Notices **5**
Acknowledgments **7**

Chapter 1: Overview of Portal Access **9**
Overview: What is portal access? 10
About portal access configuration elements 10
Understanding portal access patching 11

Chapter 2: Configuring Resources for Portal Access **13**
Creating a portal access configuration 14
Creating a portal access resource item 15
Creating a portal access resource item for minimal patching 17
Creating a portal access configuration with the wizard 17
Creating a portal access configuration with a template 18

Chapter 3: Configuring Webtops for Portal Access **21**
About webtops 22
Configuring a webtop for portal access only 22
Configuring a full webtop 23
Webtop properties 24

Chapter 4: Configuring Access Profiles for Portal Access **25**
Creating an access profile 26
Configuring an access policy 27
Access profile settings 31

Chapter 5: Configuring Rewrite Profiles for Portal Access **35**
About rewrite profiles 36
About split tunneling with rewrite profiles 36
Creating a rewrite profile 36

Chapter 6: Configuring Virtual Servers for Portal Access **39**
Defining a virtual server for portal access 40

Table of Contents

Legal Notices

Publication Date

This document was published on May 7, 2012.

Publication Number

MAN-0360-02

Copyright

Trademarks

Patents

This product may be protected by U.S. Patent 7,114,180. This list is believed to be current as of May 7, 2012.

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.

Chapter 1

Overview of Portal Access

Topics:

- *Overview: What is 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.

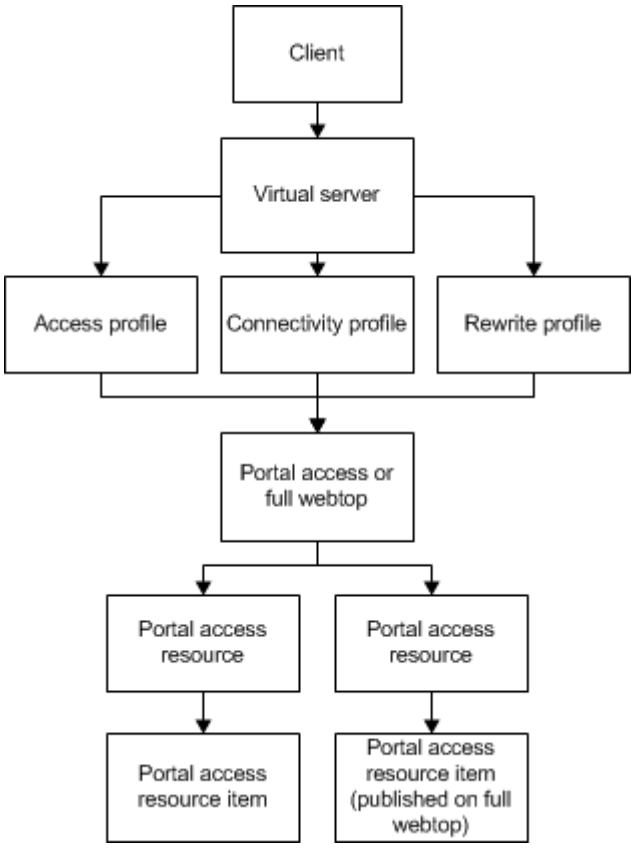

Figure 1: Portal access elements

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.

Patching content type	Description
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

Topics:

- *Creating a portal access configuration*

Creating a portal access configuration

You create a portal access resource, that you can then add to an access policy, in order to provide clients with web application connections.

1. On the Main tab, click **Access Policy** > **Portal Access** > **Portal Access List**.
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, 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**, type the 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.
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 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.
   The Portal Access Properties screen for that resource opens.
3. In the Resource Items area, click **Add**.
   A New Resource Item for that resource screen opens.
4. 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.
5. Click **Finished**.
   This creates the portal access resource item.

This creates the portal access resource, and configures the common resource items for the template.

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

Portal access resource item properties

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

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.
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.

Property	Value	Description
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.
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**

Property	Value	Description
		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.

Options	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.

Options	Description
Last	Select this option to place the new portal access resource last in the ACL list.

Options	Description
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

Topics:

- *About webtops*

About webtops

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

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

- A network access webtop provides a webtop for an access policy branch to which you assign only a network access resource.
- 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 a network access tunnel. The full webtop then provides your clients with a web page on which they can choose a network access connection to start.

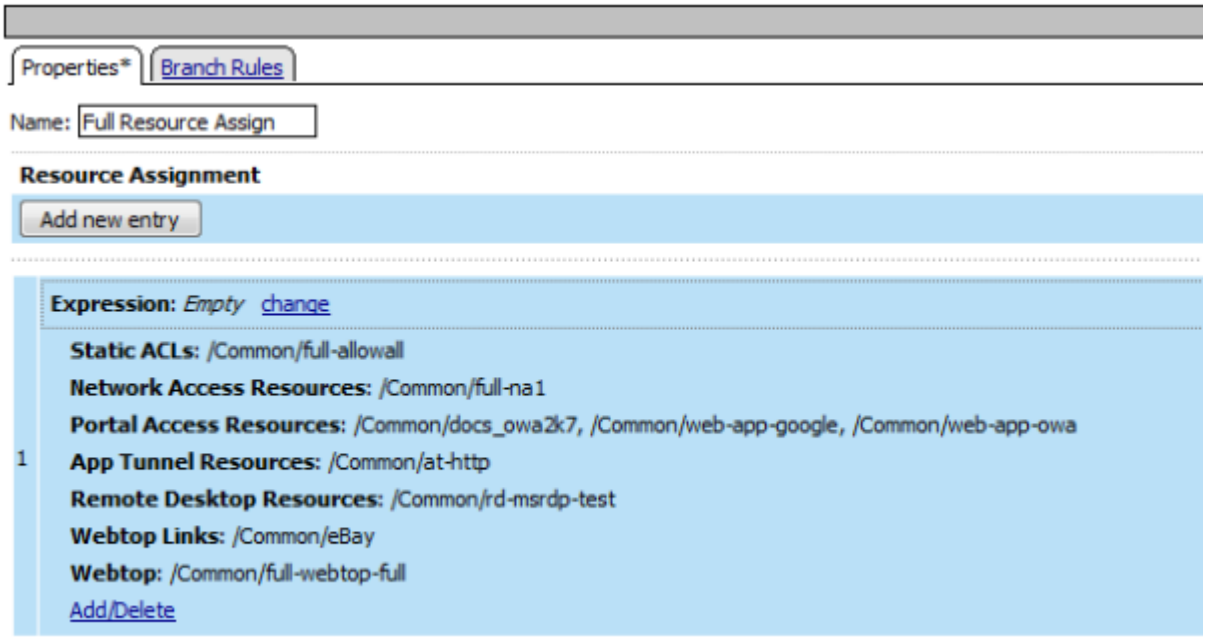

Figure 2: Resource assign action with resources and a webtop assigned

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 a full 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, 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 a full 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. In the **Application URI** field, type the application URI.
5. In the **Caption** field, type a descriptive caption.

   The **Caption** field is pre-populated with the text from the **Name** field.
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 a full resource assign action or a webtop and links assign action.

Webtop properties

Use these properties to configure a webtop.

Property	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 a single network access resource, 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	Enabled or disabled	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

Topics:

- *Creating an access profile*

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. Type a name for the access profile.
4. To configure timeout and session settings, select the **Custom** check box.
5. 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.
6. 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.

   You must select the associated **Custom** check box before you can configure this setting.
7. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.

   Type `0` to set no timeout.

   You must select the associated **Custom** check box before you can configure this setting.
8. 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.

   You must select the associated **Custom** check box before you can configure this setting.
9. 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.

   You must select the associated **Custom** check box before you can configure this setting.
10. 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.

    You must select the associated **Custom** check box before you can configure this setting.
11. 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.

    You must select the associated **Custom** check box before you can configure this setting.

    With this setting enabled, 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.
12. To configure logout URIs, in the Configurations area, type each logout URI in the **URI** field, and then click **Add**.

13. 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.
14. In the SSO across Authentication Domains area, use the **Domain Mode** setting to select whether users log in to a single domain or multiple domains.
15. If you selected **Multiple Domains**, then in the **Primary Authentication URI** field, type the primary URI for authentication.
16. If the policy requires a secure cookie, in the **Cookie Options** area select the **Secure** check box to add the **secure** keyword to the session cookie. If you are configuring an LTM access 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.
17. If the access policy requires a persistent cookie, in the **Cookie Options** area 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.
18. From the **SSO Configuration** list, select the SSO configuration.
19. In the **Domain Cookie** field, specify a domain cookie, if required.
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 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.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access policy 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 **[+]** sign anywhere in your access profile to add your new policy action item.
   An Add Item window opens, listing Predefined Actions that are grouped by General Purpose, Authentication, and so on.
6. From the General Purpose area, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent popup 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.

Adding full resources to an access policy

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

You can add the full 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. You can also assign ACLs, webtops, and webtop links with the full 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 Access Profile 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 window or tab.
5. On an access policy branch, click the plus symbol (+) to add an item to the access policy.
6. From the General Purpose list, select **Full Resource Assign** and click the **Add Item** button.
   The Full 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 box in 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 Resources	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.

Tab	Description
Portal Access Resources	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 Resources	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 Resources	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.
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.

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 Access Profile 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 window or tab.
5. On an access policy branch, click the plus symbol (+) to add an item to the access policy.
6. From the General Purpose section, 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 box in 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.

Options	Description
Network Access Resources	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 Resources	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 Resources	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 Resources	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.

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

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

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 Access Profile 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 window or tab.
5. On an access policy branch, click the plus symbol (+) to add an item to the access policy.
6. From the General Purpose section, select **Webtop and Links Assign** and click the **Add Item** button.
   This adds the action to the access policy, and opens a popup assignment window.
7. In the **Name** field, type a name for the access policy item.

   This name is displayed in the action box in 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		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 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.
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.
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 APM login session and apply it across multiple Local Traffic Manager™ or Access Policy Manager® virtual servers, front-ending different domains.

Setting	Value	Description and defaults
		Important: *All virtual servers must be on one single BIG-IP system in order to apply SSO configurations across multiple 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.*
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.
Domain Cookie	A domain cookie	If you specify a domain cookie, then the line `domain=`*`specified_domain`* is added to the `MRHsession` cookie.
Configure 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.
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

Setting	Value	Description and defaults
		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

Topics:

- *About rewrite profiles*

About rewrite profiles

A rewrite profile defines client caching settings for a virtual server. 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 rewrite profile, `rewrite`.

A rewrite profile provides four options for client caching. When a portal access resource item's **Client Cache** setting is set to **Default**, the system uses the caching option configured in the rewrite profile. If the **Client Cache** option is configured for any other setting, the portal access resource item configuration overwrites the setting in the rewrite profile. These options are available 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.

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.

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**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the rewrite profile.
4. (Optional) From the **Parent Profile** list, select a parent profile.

The new rewrite profile inherits the **Client Caching Type** setting from the parent profile.

5. (Optional) Above the Settings area, select the **Custom** check box to change the **Client Caching Type** or **Split Tunneling** setting.
6. From the **Client Caching Type** list, select the caching option.
7. 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.

8. If **Java Patching** is enabled for the portal access resource, configure the Java Patcher options for verification and re-signing of signed applets.
9. To configure the **Trusted Certificate Authorities**, first select the check box to the right of this setting, and then from the list select a CA against which to verify signed applets signatures.
10. To configure a **Signer**, first select the check box to the right of this setting, and then from the list select a certificate to use for re-signing.
11. To configure a **Signing Key**, first select the check box to the right of this setting, and then from the list select a corresponding private key for re-signing.
12. To set a **Sign Key Pass Phrase**, first check the box to the right of this setting, and then type a passphrase for the private key to be encrypted with.
13. Click **Finished**.

The rewrite profile appears in the Rewrite Profiles list.

To use 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

Topics:

- *Defining a virtual server 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, specify that the virtual server is a host virtual server, and not a network virtual server.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen displays a list of existing virtual servers.
2. Click the name of the virtual server you want to modify.
3. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
4. From the **HTTP Profile** list, select **http**.
5. In the Access Policy area, from the **Access Profile** list, select the access profile.
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**.
11. If you want to provide connections to Citrix desktop resources or Java RDP clients for Application Access, or allow Java rewriting for Portal Access, select the **Citrix & Java Support** 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.

Index

A

access policy
    adding a webtop and webtop links 30
    configuring 27
access profile
    creating 26
access profile settings
    listed 31

C

configuration elements
    for portal access 10

F

full patching
    for portal access 11
full resource assign action
    adding to an access policy 28
full webtop
    configuring 23

I

IP addresses
    IPv4 and IPv6 addresses 15

M

minimal patching
    configuring a portal access resource item 17
    for portal access 12

P

portal access
    and configuration elements 10
    and full patching 11
    and minimal patching 12
    configuring webtops 22
    creating resource item 15
    creating resource item for minimal patching 17
    creating with a template 18
    creating with wizard 17
    overview 10
portal access configuration
    creating manually 14

R

resource assign action
    adding to an access policy 29
resource item
    and properties for portal access 15
    creating for minimal patching 17
    creating for portal access 15
rewrite profile
    and split tunneling 36
    creating 36
    for portal access 36

S

split tunneling
    and bypass 36
    and rewrite 36

T

template
    for portal access 18

V

virtual server
    associating with portal access 40
    defining for portal access 40

W

web application
    creating resource item 15, 17
webtop and links assign action
    adding to an access policy 30
webtop link
    creating 23
webtops
    about 22
    configuring for portal access 22
    configuring full 23
    properties 24
wizard
    for portal access 17