BIG-IP® Access Policy Manager®: Hosted Content Implementations

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0463-00

Copyright

Trademarks

Access Policy Manager, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Manager, MSM, OneConnect, OpenBloX, OpenBloX [DESIGN], Packet Velocity, Policy Enforcement Manager, PEM, Protocol Security Manager, PSM, Real Traffic Policy Builder, Rosetta Diameter Gateway, Scale^{N}, Signaling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Diameter Load Balancer, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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

Patents

This product may be protected by U.S. Patent 7,114,180; 8,301,837. This list is believed to be current as of May 15, 2013.

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

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

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

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

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

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

Chapter 1

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 this to display an HTML file that only a verified user can see.

Permission level	Description
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 2

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.

Chapter 3

Hosting a BIG-IP Edge Client Download with Access Policy Manager

About hosting a BIG-IP Edge Client file on Access Policy Manager

You can host files on BIG-IP® Access Policy Manager® (APM®) so clients can download them.

When you host a file on Access Policy Manager, you can provide the link to the file in a number of ways. In this example, the BIG-IP Edge Client® for Mac link is provided as a link on the user's webtop. The user connects through the web client, then clicks a link on the webtop to download the client file. To provide the BIG-IP Edge Client for Mac, first you must create a connectivity profile. Then, you can download the Mac client file as a ZIP file.

Task summary

To add the BIG-IP® Edge Client® for Mac file to the hosted content repository on Access Policy Manager®, so clients can download it, complete these tasks.

Task Summary

Customizing a connectivity profile for Mac Edge Clients
Downloading the Mac client package for the BIG-IP Edge Client
Uploading BIG-IP Edge Client to hosted content on Access Policy Manager
Associating hosted content with access profiles
Creating a webtop link for the client installer
Adding a webtop and webtop links to an access policy

Customizing a connectivity profile for Mac Edge Clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Macintosh. You update the settings to specify how to handle password caching and component updates, to specify the servers to display on the clients, and to supply DNS names to support location awareness.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane, select **Win/Mac Edge Client**.
   Edge Client action and password caching settings display in the right pane.
4. Set Edge Client action settings:
   a) (Optional) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      The setting specifies whether the BIG-IP Edge Client maintains a list of recently used Access Policy Manager servers. The BIG-IP Edge Client always lists the servers defined in the connectivity profile, and sorts the list of servers by most recent access, whether this option is selected or not. However, the BIG-IP Edge Client lists user-entered servers only if this option is selected.

5. Set password caching settings for enhanced security:

a) (Optional) Select the **Allow Password Caching** check box.

This check box is cleared by default.

The remaining settings on the screen become available.

b) (Optional) Select **disk** or **memory** from the **Save Password Method** list.

If you select **disk**, an encrypted password is saved on disk and cached when the system reboots or when the BIG-IP Edge Client is restarted.

If you select **memory**, the BIG-IP Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

c) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

d) From the **Component Update** list, select **yes** (default) or **no**.

If you select **yes**, APM updates the BIG-IP Edge Client software automatically on the Mac client when newer versions are available.

6. From the left pane, select **Server List**.
A table displays in the right pane.

7. Specify the servers that you want defined in the client downloads.

The servers you add here appear as connection options in the BIG-IP Edge Client.

a) Click **Add**.
A table row becomes available for update.

b) You must type a host name in the **Host Name column**.

Typing an alias in the **Alias** column is optional.

c) Click **Update**.
The new row is added at the top of the table.

d) Continue to add servers and when you are done, click **OK**.

8. From the left pane, select **Location DNS List**.
A table is displayed in the right pane.

9. Specify DNS suffixes that are considered to be in the local network.

DNS suffixes specified here conform to the rules specified for the local network. When the BIG-IP Edge Client is configured to use the option Auto-Connect , the client connects when the systems DNS suffix is not one defined on this list. When the client DNS suffix does appear on this list, the client automatically disconnects. If you do not specify any DNS suffixes, the option Auto-Connect does not appear in the downloaded client.

a) Click **Add**.
An update row becomes available.

b) Type a name and click **Update**.
The new row displays at the top of the table.

c) Continue to add DNS names and, when you are done, click **OK**.

10. 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 and an access profile to a virtual server.

Downloading the Mac client package for the BIG-IP Edge Client

You can download a Mac Client package and distribute it to clients whose configuration does not allow an automatic download.

Note: *If you already customized a Mac Client package for a connectivity profile, a customized package file,* `BIGIPMacEdgeClient.exe`*, was downloaded to your system. If you cannot find the package, use this procedure.*

---

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.
   The Customize Mac Client Package screen displays.
4. Click **Download**.

   The screen closes and the package, `BIGIPMacEdgeClient.zip`, downloads.

The customized package, `BIGIPMacEdgeClient.zip`, is downloaded to your client. It is available for you to distribute, if needed. The customized package is downloaded to clients automatically only when the Windows/Mac Edge Client settings in the related connectivity profile allow password caching and component updates.

Uploading BIG-IP Edge Client to hosted content on Access Policy Manager

Upload the client file to the Access Policy Manager® hosted content repository so you can provide it to clients through a download link.

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. Browse and select the `BIGIPMacEdgeClient.zip` file that you previously downloaded.
   The **Select File** and **File Name** fields are populated with the file name.
4. From the **File Action** list, select **Upload Only**.
5. In the **File Destination Folder** field, specify the folder path in which to place the file. For purposes of this example, the folder `/client` is specified.
6. 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.

Creating a webtop link for the client installer

You can create and customize links that you can assign to full webtops. In this context, *links* are defined applications and web sites 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 **Hosted Content**.
5. From the **Hosted File** link, select `public/share/client/BIGIPMacEdgeClient.zip`.
6. 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.
7. If you want to add a detailed description, type it in the **Detailed Description** field.
8. 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.
9. 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.

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 plus symbol (+) 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.

Implementation result

As a result of these implementation tasks, you have added the client file to a webtop link.

Chapter 4

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.

Index