BIG-IP® Access Policy Manager® Application Access Guide

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0360-02

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.

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

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

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

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

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

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

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

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

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

Chapter 1

Configuring App Tunnel Access

- *What are app tunnels?*

What are app tunnels?

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

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

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

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

Task summary for app tunnels

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

Task list

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

Configuring an app tunnel object

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

1. On the Main tab, click **Access Policy** > **Application Access** > **App Tunnels**.
   The App Tunnels screen opens.
2. Click **Create**.
   The New App Tunnel Resource screen opens.
3. Type a name and description for your app tunnel.
4. Although an ACL is automatically created for your application object, you can choose to determine the order of your ACL as it appears in the ACL list. Use the **ACL Order** list to select the placement you want.
5. Under Default Customization Settings, type a **Caption** for the app tunnel.
   This caption identifies the app tunnel and enables it to appear on a full webtop.
6. Click **Create**.

You have just created an app tunnel object.

Configuring an application resource item for an app tunnel

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

1. On the Main tab, click **Access Policy** > **Application Access** > **App Tunnels**.
   The list of app tunnels opens.
2. Click the name of the app tunnel you created.
   The Properties screen opens.
3. Under Resource Items, click **Add**.
   The New Resource Item screen opens.
4. For the **Destination** setting, specify whether the application destination **Type** is a host or an IP address.

   You cannot use the fully qualified domain name to connect to an application resource that is configured with an IP address destination type.

   If you specify a hostname, make sure that it is DNS-resolvable. After the application tunnel is assigned to a full webtop in an access policy, the application tunnel does not appear on the full webtop if the hostname is not DNS-resolvable.
5. Specify your port or port range for the application.
6. From the **Application Protocol** list, select the application protocol.

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

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

Configuring an access policy to include an app tunnel

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

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

3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile *profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. Click the **(+)** sign anywhere in the access policy to add a new action item.
   An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. On the Assignment tab, select the **Resource Assign** agent, and click **Add Item**.
   The Resource Assignment screen opens.
7. Next to the **App Tunnel** setting, click the **Add/Delete** link, and select the application tunnel to assign.
8. Click **Update**.
9. Click the **Save** button to save changes to the access policy item.

Your app tunnels are now assigned to the session.

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

Attaching an access policy to the virtual server for app tunnels

When creating a virtual server for an access policy, specify 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 opens.
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. If you are using a connectivity profile, from the **Connectivity Profile** list, select the connectivity profile.
7. If you are creating a virtual server to use with portal access resources in addition to app tunnels, from the **Rewrite Profile** list, select the default **rewrite** profile, or another rewrite profile you created.
8. If you want to provide connections to VDI desktop resources or Java RDP clients for Application Access, or allow Java rewriting for Portal Access, select the **VDI & 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.
9. If you want to provide native integration with an OAM server for authentication and authorization, select the **OAM Support** check box.

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

Your access policy is now associated with the virtual server.

Chapter 2

Configuring Remote Desktop Access

What are remote desktops?

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

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

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

What is Microsoft remote desktop?

With Access Policy Manager®, you can configure clients to access a server running Microsoft® Remote Desktop Services. Microsoft Remote Desktop servers run the Microsoft Remote Desktop Protocol (RDP) server. RDP is a protocol that provides a graphical interface to another computer on a network.

To provide Microsoft RDP connections to Windows®, Mac®, and Linux clients natively, you can select the Java Client option. This provides a simple Java Client interface to the Microsoft RDP server, with reduced visual display features, on any compatible platform. See the online help for feature differences between the Java client and the Windows client.

What is Citrix remote desktop?

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

Task summary for remote desktops

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

Task list

Configuring a resource for Citrix or Microsoft remote desktops
Configuring an access policy to include a remote desktop
Attaching an access policy to a virtual server for remote desktops

Configuring a resource for Citrix or Microsoft remote desktops

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

1. On the Main tab, navigate to **Access Policy** > **Application Access** > **Remote Desktops**.
   The Remote Desktops list opens.
2. Click **Create**.

The General Properties screen opens.

3. Configure the following settings:

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

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

4. Under the **Default Customization Settings** section, type a **Caption**.
   The caption identifies the remote desktop and enables it to appear on a full webtop.

Configuring an access policy to include a remote desktop

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

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. Click the **(+)** sign anywhere in the access policy to add a new action item.
   An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. On the Assignment tab, select the **Resource Assign** agent, and click **Add Item**.
   The Resource Assignment screen opens.
7. Next to each type of resource that you want assign (**Network Access**, **Portal Access**, **App Tunnel**, **Remote Desktop**, or **SAML**), click the **Add/Delete** link, and select from available resources.
8. Click **Update**.
9. Click **Save**.

Your remote desktop is assigned to the session.

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

Attaching an access policy to a virtual server for remote desktops

When creating a virtual server for an access policy, specify 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 opens.
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. For the **HTTP Profile** setting, verify that the default HTTP profile, **http**, is selected.
5. In the Access Policy area, from the **Access Profile** list, select the access profile.
6. If you are using a connectivity profile, from the **Connectivity Profile** list, select the connectivity profile.
7. If you are creating a virtual server to use with portal access resources in addition to remote desktops, from the **Rewrite Profile** list, select the default **rewrite** profile, or another rewrite profile you created.
8. If you want to provide connections to VDI desktop resources or Java RDP clients for Application Access, or allow Java rewriting for Portal Access, select the **VDI & 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.
9. If you want to provide native integration with an OAM server for authentication and authorization, select the **OAM Support** check box.

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

The access policy is now associated with the virtual server.

Chapter 3

Configuring Webtops

About webtops

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

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

- A network access webtop provides a webtop for an access policy branch to which you assign only a network access resource.
- A portal access webtop provides a webtop for an access policy branch to which you assign only portal access resources.
- A full webtop provides an access policy ending for an access policy branch to which you can optionally assign portal access resources, app tunnels, remote desktops, and webtop links, in addition to network access tunnels. Then, the full webtop provides your clients with a web page on which they can choose a network access connection to start.

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

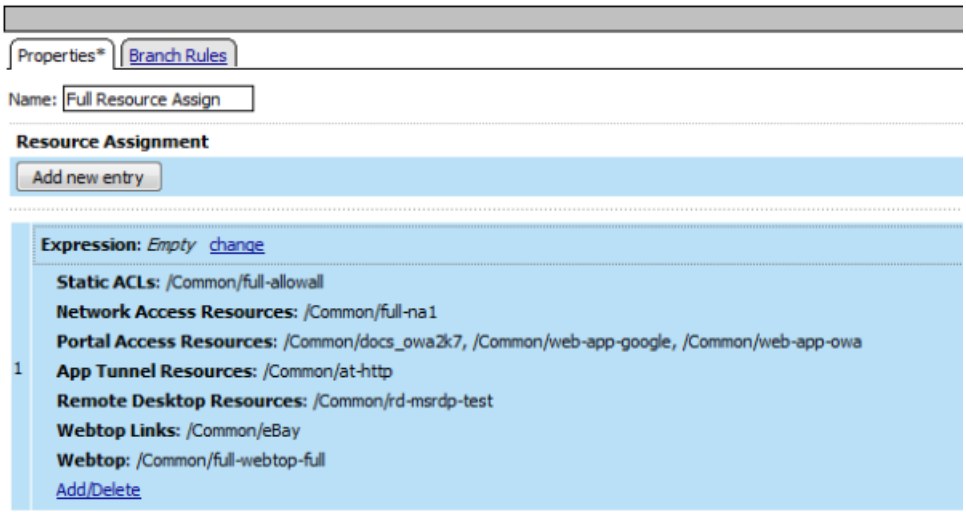

Figure 1: Resource assign action with resources and a webtop assigned

Configuring a full webtop

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

1. On the Main tab, click **Access Policy** > **Webtops**.
2. Click **Create** to create a new webtop.
3. Type a name for the webtop you are creating.

4. From the **Type** list, select **Full**.
5. Click **Finished**.

The webtop is now configured, and appears in the list. You can edit the webtop further, or assign it to an access policy.

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

Creating a webtop link

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

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

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

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

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

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

Customizing a webtop link

You can customize links that you assign to full webtops.

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

10. In the **Detailed Description** field, type a detailed description.
11. In the **Image** field, click **Browse** to select an image to show on the webtop to represent the webtop link. Click the **View/Hide** link to show the currently assigned image.

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

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

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

Webtop properties

Use these properties to configure a webtop.

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

Adding a webtop and webtop links to an access policy

Before you start this task, you must create an access profile.

Add the advanced 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 advanced resource assign action.

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

---

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

3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile *profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. On an access policy branch, click the 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. Next to the **Webtop** and **Webtop Links** links, click the **Add/Delete** link, and select the webtop and links to assign.
   You can only assign one webtop, though you can assign multiple webtop links.
9. Click the **Save** button to save changes to the access policy item.

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

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

Adding advanced resources to an access policy

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

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

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

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile *profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. On an access policy branch, click the 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 **Advanced Resource Assign** and click the **Add Item** button.
   The Advanced Resource Assign popup screen opens.
7. In the **Name** field, type a name for the access policy item.
   This name is displayed in the action field for the access policy.
8. Click the **Add new entry** button.
   A new resource line is added to the list.

9. To assign resources, in the Expression area, click the **Add/Delete** link.
   The Resource Assignment popup screen opens.
10. Assign resources to the access policy using the available tabs.

Tab	Description
Static ACLs	Allows you to select one or more ACLs defined on the system. Each ACL you select is assigned to the access policy branch on which this resource assign action operates.
Network Access	Allows you to select a single network access resource from the system. You can select only one network access resource. The network access resource you select is assigned to the access policy branch on which this resource assign action operates.
Portal Access	Allows you to select one or more portal access resources from the system. The portal access resources you select are assigned to the access policy branch on which this resource assign action operates.
App Tunnel	Allows you to select one or more application tunnel resources from the system. The application tunnel resources you select are assigned to the access policy branch on which this resource assign action operates.
Remote Desktop	Allows you to select one or more remote desktop (terminal server) resources from the system. The remote desktop resources you select are assigned to the access policy branch on which this resource assign action operates.
SAML	Allows you to select one or more SAML resources from the system. The SAML resources you select are assigned to the access policy branch on which this resource assign action operates. Select a full webtop to display SAML resources.
Webtop Links	Allows you to select links to pages and applications defined on the system to display on the full webtop. A full webtop must be assigned to display webtop links.
Webtop	Allows you to select a webtop from the system. The webtop resource you select is assigned to the access policy branch on which this resource assign action operates. You can select a webtop that matches the resource type, or a full webtop.
Static Pool	Allows you to dynamically assign a predefined LTM pool to a session. This value takes precedence over any existing assigned pool attached to the virtual server. The static pool you select is assigned to the access policy branch on which this resource assign action operates.

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

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

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

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

Index