# BIG-IP® Access Policy Manager®: Implementations

Version 11.5

# Table of Contents

**Legal Notices.......................................................7**

**Acknowledgments.....................................................9**

**Chapter 1: Configuring Web Access Management.....................13**

Overview: Configuring APM for web access management....................14

About configuring timeout for a web access management session.........14

Creating a pool.......................................................14

Creating an access profile............................................15

Creating an access policy for web access management..................16

Creating a virtual server..............................................17

**Chapter 2: Configuring Dynamic ACLs..................................19**

Overview: Applying ACLs from external servers..........................20

About dynamic ACLs......................................................20

Configuring a dynamic ACL container.....................................20

Adding a dynamic ACL to an access policy.................................21

F5 ACL format...........................................................22

Cisco ACL format........................................................24

**Chapter 3: Configuring Routing for Access Policies.....................25**

Overview: Selecting a route domain for a session (example)...............26

Creating a route domain on the BIG-IP system.............................26

Creating an access profile...............................................27

Configuring policy routing...............................................27

**Chapter 4: Synchronizing Access Policies...............................31**

Overview: Syncing access policies with a Sync-Only device group..........32

About device groups and synchronization..................................32

Before you configure device trust.......................................32

Task summary............................................................33

Establishing device trust................................................33

Creating a Sync-Only device group for access policy sync.................34

Synchronizing an access policy across devices initially.................34

Configuring static resources with access policy sync....................35

Configuring dynamic resources with access policy sync...................36

Resolving access policy sync conflicts...................................36

About ignoring errors due to the Variable Assign agent...................37

Implementation result....................................................37

**Chapter 5: Maintaining OPSWAT Libraries with a Sync-Failover Device Group................39**
Overview: Updating antivirus and firewall libraries with a Sync-Failover device group....................40
About device groups and synchronization....................40
Before you configure device trust....................40
Task summary....................40
Establishing device trust....................41
Adding a device to the local trust domain....................42
Creating a Sync-Failover device group....................42
Manually synchronizing the BIG-IP configuration....................43
Uploading an OPSWAT update to Access Policy Manager....................44
Installing an OPSWAT update on one or more Access Policy Manager devices....................45
Viewing supported products in the installed OPSWAT EPSEC version....................45
Implementation result....................46

**Chapter 6: Maintaining OPSWAT Libraries with a Sync-Only Device Group......................47**
Overview: Updating antivirus and firewall libraries with a Sync-Only device group.........48
About device groups and synchronization....................48
Before you configure device trust....................48
Task summary....................48
Establishing device trust....................49
Adding a device to the local trust domain....................50
Creating a Sync-Only device group....................50
Uploading an OPSWAT update to Access Policy Manager....................51
Installing an OPSWAT update on one or more Access Policy Manager devices....................52
Viewing supported products in the installed OPSWAT EPSEC version....................52
Implementation result....................53

**Chapter 7: Adding Hosted Content to Access Policy Manager....................55**
About uploading custom files to Access Policy Manager....................56
Understanding hosted content....................56
About accessing hosted content....................56
Permissions for hosted content....................56
Task summary....................57
Uploading files to Access Policy Manager....................57
Associating hosted content with access profiles....................58
Implementation result....................58

**Chapter 8: Editing Hosted Content with Access Policy Manager....................59**
About editing hosted files on Access Policy Manager....................60

Task summary.....60
Renaming or moving hosted content files.....60
Editing hosted content file properties.....60
Replacing a hosted file.....61
Deleting a hosted file.....61
Implementation result.....62

**Chapter 9: Hosting a BIG-IP Edge Client Download with Access Policy Manager.....63**
About hosting a BIG-IP Edge Client file on Access Policy Manager.....64
Task summary.....64
Customizing a connectivity profile for Mac Edge Clients.....64
Downloading the Mac client package for the BIG-IP Edge Client.....66
Uploading BIG-IP Edge Client to hosted content on Access Policy Manager .....66
Associating hosted content with access profiles.....66
Creating a webtop link for the client installer.....67
Adding a webtop and webtop links to an access policy.....67
Implementation result.....68

**Chapter 10: Hosting Files with Portal Access on Access Policy Manager.....69**
About using hosted files with a Portal Access resource.....70
Task summary.....70
Uploading files to Access Policy Manager for Portal Access.....70
Associating hosted content with access profiles.....71
Creating a portal access configuration with hosted content.....71
Creating a portal access resource item for hosted content.....72
Implementation result.....73

# Legal Notices

## Publication Date

This document was published on January 27, 2014.

## Publication Number

MAN-0508-00

## Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

## Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, 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 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, 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 one or more patents indicated at: *http://www.f5.com/about/guidelines-policies/patents*

## Export Regulation Notice

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

## RF Interference Warning

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

## FCC Compliance

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

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

## Canadian Regulatory Compliance

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

## Standards Compliance

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

# Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

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

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

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

# Chapter 1

# Configuring Web Access Management

- *Overview: Configuring APM for web access management*

## Overview: Configuring APM for web access management

Access Policy Manager® (APM®) web access management provides the ability to access web applications through a web browser without the use of tunnels or specific resources. With this type of access, APM communicates with backend web servers, forwarding requests from the client to web servers within a local traffic pool.

In a typical web access management connection, access occurs through a rewriting engine that rewrites links and URLs to and from the client. APM web access management eliminates the need for content rewriting, allowing access to the configured local traffic pool after the user passes through the access policy checks.

### Task summary

To support APM web access management connections, you need a pool of web application servers, an access profile and access policy, and a virtual server.

*Creating a pool*

*Creating an access profile*

*Creating an access policy for web access management*

*Creating a virtual server*

## About configuring timeout for a web access management session

The web access management access type does not have a logout mechanism, so you must configure a timeout option from these choices.

**The Windows Cache and Session Control access policy item**

Terminates a user session when it detects that the browser screen has closed. You can also configure it to provide inactivity timeouts for the user session using the Terminate session on user inactivity setting.

**Maximum Session Timeout access profile setting**

Provides an absolute limit for the duration of the access policy connection, regardless of user activity. To ensure that a user session closes after a certain number of seconds, configure this setting.

**Inactivity Timeout access profile setting**

Terminates the session after there is no traffic flow for a specified number of seconds.

***Note:*** *Depending on the application, you might not want to set this to a very short duration, because many applications cache user typing and generate no traffic for an extended period. In this scenario, a session can time out while the application is still in use, but the content of the user input is not relayed back to the server.*

.

## Creating a pool

You can create a pool of servers for Access Policy Manager® (APM®) to perform access control for web application servers configured as local traffic pool members.

***Important:*** *When you implement a service with multiple hosts, access through the virtual server for new requests causes the load balancing algorithm for the associated member pool to select a new server. This can cause problems if persistence to a particular host is required.*

***Note:*** *When you add web servers as members of the pool, select the HTTPS service if the web server uses SSL, to maintain consistency between APM and the web servers.*

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, for the **New Members** setting, add to the pool the application servers that host the web application:
   a) Type an IP address in the **Address** field.
   b) In the **Service Port** field, type a port number (for example, type `80` for the HTTP service), or select a service name from the list.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

## Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session. In the access profile, you can also specify a timeout to use to terminate a web access management connection

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. From the **Profile Type** list, select **LTM-APM**.
   With this type selected, when you configure the access policy, only access policy items that are applicable for web access management are displayed.
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.

   The web access management connection type does not provide a logout mechanism. You should configure at least one timeout for the connection, either in this access profile, or by including the Windows Cache and Session Control item in the access policy and configuring a timeout in it.
6. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.

   Type `0` to set no timeout.
7. 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.
8. Click **Finished**.

This creates an access profile with a default access policy.

## Creating an access policy for web access management

You create an access policy to specify, at a minimum, logon and authentication. You can add other items to the policy to direct traffic and grant or deny access appropriately, increasing your security.

***Note:*** *In an access policy for web access management, you do not need to assign resources, such as, webtops, portal access or network access resources, application access tunnels, or remote desktops.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. On the Logon tab, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent properties screen opens.
5. Make any changes that you require to the logon page properties and click **Save**.
   The properties screen closes and the visual policy editor displays.
6. On an access policy branch, click the **(+)** icon to add an item to the access policy.

   Repeat this action from the visual policy editor whenever you want 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.
7. From the Authentication tab, select an authentication item.
8. Configure the properties for the authentication item and click **Save** when you are done.

   You can configure multiple authentication items in an access policy.

   You have now configured a basic access policy.
9. Add endpoint security checks or other items that you require to the access policy.

   Optionally, you can assign a pool of web servers in the access policy using the Pool Assign action; if you do, this pool takes precedence over the pool you assign to the virtual server configuration.

   ***Note:*** *You can add a* ***Windows Cache and Session Control*** *item to configure a way to terminate the session.*
10. To grant access at the end of any branch, change the ending from **Deny** to **Allow**:
    a) Click **Deny**.

       The default branch ending is **Deny**.

       A popup screen opens.

    b) Select **Allow** and click **Save**.
       The popup screen closes. The **Allow** ending displays on the branch.
11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

This creates an access policy that is appropriate for web access management connections. For an access policy to take effect, you must add it to a virtual server configuration.

## Creating a virtual server

This task creates a standard, host type of virtual server for application traffic. A host type of virtual server listens for traffic destined for the specified destination IP address and service. Using this virtual server, Access Policy Manager® (APM®) can provide access control for web applications on web servers in a local traffic pool without using tunnels or specific resources.

***Note:*** *By default, the health monitor is set to none and the load balancing method is set to Round Robin. You can add a health monitor or select an alternative load balancing method for this virtual server.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `80` (for HTTP) or `443` (for HTTPS), or select **HTTP** or **HTTPS** from the list.
6. For the **HTTP Profile** setting, verify that the default HTTP profile, **http**, is selected.
7. (Optional) For the **SSL Profile (Client)** setting, select a client SSL profile.

   If the web server uses SSL, the client should use SSL.
8. (Optional) For the **SSL Profile (Server)** setting, select an SSL server profile.

   If the web server uses SSL, the virtual server should use SSL.
9. In the Content Rewrite area, retain the default settings.

   The web access management access type eliminates the need for content rewriting. The default values for the **Rewrite Profile** and the **HTML Profile** settings are **None**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile you configured previously.

    Retain the default values for other settings in the Access Policy area.
11. (Optional) From the **HTTP Compression Profile** list, select **httpcompression**.

    You can use compression to provide a better end user experience, particularly where there is limited bandwidth or high latency between the virtual server and the client.
12. In the Resources area of the screen, from the **Default Pool** list, select a pool name.
13. Click **Finished**.

You have a virtual server that supports web access management connections.

# Chapter 2

## Configuring Dynamic ACLs

- *Overview: Applying ACLs from external servers*
- *F5 ACL format*
- *Cisco ACL format*

## Overview: Applying ACLs from external servers

You can apply ACLs from Active Directory, RADIUS, or LDAP servers using the Dynamic ACL action from an Access Policy Manager® access policy.

### Task summary

After you configure ACLs in a supported format on an Active Directory, LDAP, or RADIUS server, you can configure a dynamic ACL action to extract and use the ACLs.

### Task list

*Configuring a dynamic ACL container*

*Adding a dynamic ACL to an access policy*

## About dynamic ACLs

A *dynamic ACL* is an ACL that is created on and stored in an LDAP, RADIUS, or Active Directory server. A Dynamic ACL action dynamically creates ACLs based on attributes from the AAA server. Because a dynamic ACL is associated with a user directory, you can use it to assign ACLs specifically per the user session. Access Policy Manager® supports dynamic ACLs in an F5® ACL format, and in a subset of the Cisco ACL format.

You can configure a Dynamic ACL action with the following elements and options:

**Source**

Specifies an option and the attribute from which the Dynamic ACL action extracts ACLs: **Custom** indicates an F5 ACL from an Active Directory, RADIUS, or LDAP directory at the attribute you specify; **Cisco AV-Pair VSA** indicates a Cisco AV-Pair ACL from a RADIUS directory; the field is prepopulated with `session.radius.last.attr.vendor-specific.1.9.1.`

**ACL**

Specifies the dynamic ACL container configured on the BIG-IP® system.

**Format**

Specifies the format (F5 or Cisco) in which the ACL is specified.

***Note:*** *To succeed, the Dynamic ACL action must follow an authentication or query action to capture the authentication variables that contain the dynamic ACL specification.*

## Configuring a dynamic ACL container

A dynamic ACL container provides an unconfigured ACL that you select when you configure a dynamic ACL action in an access policy.

1. On the Main tab, click **Access Policy** > **ACLs**.
   The ACLs screen opens.
2. Click **Create**.
   The New ACL screen opens.
3. In the **Name** field, type a name for the access control list.

4. From the **Type** list, select **Dynamic**.
5. (Optional) In the **Description** field, add a description of the access control list.
6. (Optional) From the **ACL Order** list, specify the order in which to add the new ACL relative to other ACLs:
   - Select **After** to add the ACL after a specific ACL and select the ACL from the list.
   - Select **Specify** to type the specific number of the ACL in the field.
   - Select **Last** to add the ACL at the last position in the list.
7. From the **Match Case for Paths** list, select **Yes** to match case for paths, or **No** to ignore path case.

   This setting specifies whether alphabetic case is considered when matching paths in an access control entry.
8. Click the **Create** button.
   The ACL Properties screen opens; it displays the newly configured dynamic ACL container.

*Overview: Applying ACLs from external servers*
*Overview: Applying ACLs from external servers*
*Adding a dynamic ACL to an access policy*

## Adding a dynamic ACL to an access policy

Before you start this task, configure an access profile and a dynamic ACL container. Add an authentication action to the access policy before the dynamic ACL action so that APM can first capture authentication variables that contain the dynamic ACL specification.

Configure a dynamic ACL action to extract and apply an ACL from an AAA server (Active Directory, LDAP, or RADIUS).

***Note:*** *Because a dynamic ACL is associated with a user directory, you can use one to assign ACLs specifically per the user session.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. From the Assignment tab, select **Dynamic ACL**, and click **Add Item**.
   A properties screen opens.
5. To add an ACL, click the **Add new entry** button.
   A new row opens in the table.
6. Select one of these from the list:
   - **Custom** Select to use an F5 ACL from an AD, RADIUS, or LDAP directory.
   - **Cisco AV-Pair VSA** Select to use a Cisco AV-Pair ACL from a RADIUS directory.
7. In the **Source** field, type the attribute from which the Dynamic ACL action extracts ACLs.

   If you are using Cisco AV-Pair VSA from a RADIUS server, the field is prepopulated with `session.radius.last.attr.vendor-specific.1.9.1`.
8. From the **ACL** list, select the dynamic ACL container that you configured previously.

9. From the **Format** list, select the format in which the ACL is specified.
10. (Optional) To configure another ACL, click the **Add new entry** button and repeat the configuration steps.
11. Select **Save** to save any changes and return to the access policy.

The access policy is configured to extract an ACL from an AAA server and apply it when processing occurs on the access policy branch. You can now configure any additional actions you need in the access policy.

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

*Overview: Applying ACLs from external servers*

*Configuring a dynamic ACL container*

*Overview: Selecting a route domain for a session (example)*

## F5 ACL format

Specifies F5® ACL syntax and provides examples.

Specify an F5 ACL using this syntax.

```
{ action [logging_options] context }
```

### action

This is an action that the ACL takes on traffic that matches the ACL context.

`allow` Allows the specified traffic.

`reject` Rejects the specified traffic and sends a TCP RST code to the initiator.

`discard` Silently drops the packets.

`continue` Skips checking against the remaining access control entries in this ACL, and continues evaluation at the next ACL.

### logging_options

Specifying a logging option is optional.

`log` Enables default logging for the ACL

`log-packet` Writes packet-level logs to the packet filter log file

`log-verbose` Writes verbose logs

`log-summary` Writes summary logs

`log-config` Writes configuration logs to the configuration log file

### context

Context specifies a protocol followed by addresses, networks, and ports for the ACL action.

`http` HTTP protocol traffic. Requires that you specify an HTTP or HTTPS URL in the ACL definition

`udp` UDP traffic only

`tcp` TCP traffic only

### Address, network, and port specification

Specify addresses in a pair separated by a space. The first address in the pair should match the host, and the second address in the pair should match the destination. This syntax:

```
any[/mask][:port]
```

matches any host or IP address with an optional subnet mask or a port. For example,

```
{ allow tcp any 1.2.3.4 }
```

allows TCP traffic between any host and the destination IP address 1.2.3.4.

This syntax:

```
IP address[/mask][:port]
```

matches a specific IP address with an optional subnet mask or a port. For example,

```
{ allow 1.1.1.1 1.2.3.4 }
```

allows TCP traffic between the host IP address 1.1.1.1 and the destination IP address 1.2.3.4.

### F5 ACL with the IP protocol

This example shows how to specify an IP protocol address in F5 ACL format. An IP protocol number, 51, and an address pair specification follow the context word `ip`.

```
{ allow ip 51 any 1.2.3.4 }
```

### F5 ACL with the TCP or UDP protocol

This example shows how to specify a TCP or UDP protocol address in F5 ACL format. An address pair specification follows the context word (`tcp` or `udp)`.

```
{ allow tcp any 1.2.3.4 }
{ allow udp any 1.2.3.4 }
```

### F5 ACL with the HTTP protocol

These examples show how to specify an HTTP protocol address in F5 ACL format. A host address, destination address, and URL follow the context word `http`. The URL specification supports wildcards with glob matching.

```
{ allow http any 1.2.3.4 https://www.siterequest.com/* }
{ allow http any 1.2.3.0/24 http://*.siterequest.com/* }
{ allow http any 1.2.3.0/24 http://*.siterequest.???/* }
```

# Cisco ACL format

Specifies the subset of Cisco ACL syntax that Access Policy Manager® supports and provides examples.

### Usage

On a RADIUS server, Access Policy Manager supports dynamic ACLs that use the subset of the Cisco ACL format described here.

### Prefix

You can specify this prefix `ip:inacl#X=` where *X* is an integer used as a rule identifier.

### Keywords

These keywords are mapped with the F5 log-packet format: `log` and `log-input`.

These keywords are not supported: `tos`, `established`, `time-range`, `dynamic`, and `precedence`.

### Supported specification for Cisco ACL for IP protocol

```
{deny|permit}
      ip source source-wildcard destination destination-wildcard
       [log|log-input]
```

For example:

```
ip:inacl#10=permit ip any any log
```

### Supported specification for Cisco ACL for TCP protocol

```
{deny|permit}
      tcp source source-wildcard [operator [port]] destination
destination-wildcard
     [operator [port]] [log|log-input]
```

For example:

```
ip:inacl#10=permit tcp any host 10.168.12.100 log
```

### Supported specification for Cisco ACL for UDP protocol

```
{deny|permit}
      udp source source-wildcard [operator [port]] destination
destination-wildcard
     [operator [port]] [log|log-input]
```

For example:

```
deny udp any any log
```

# Chapter 3

## Configuring Routing for Access Policies

- *Overview: Selecting a route domain for a session (example)*

## Overview: Selecting a route domain for a session (example)

A *route domain* is a BIG-IP® system object that represents a particular network configuration. Route domains provide the capability to segment network traffic, and define separate routing paths for different network objects and applications. You can create an access policy that assigns users to different route domains using the Route Domain and SNAT Selection action based on whatever criteria you determine appropriate.

You might use policy routing in a situation such as this: your company has switched from RADIUS authentication to Active Directory authentication, but has not yet completed the full transition. Because of the state of the authentication changeover, you would like your legacy RADIUS users to pass through to a portal access connection on a separate router, instead of allowing full access to your network.

This implementation provides configuration steps for this example.

**Task summary**

*Creating a route domain on the BIG-IP system*
*Creating an access profile*
*Configuring policy routing*

## Creating a route domain on the BIG-IP system

Before you create a route domain:

- Ensure that an external and an internal VLAN exist on the BIG-IP® system.
- Verify that you have set the current partition on the system to the partition in which you want the route domain to reside.

You can create a route domain on BIG-IP system to segment (isolate) traffic on your network. Route domains are useful for multi-tenant configurations.

1. On the Main tab, click **Network** > **Route Domains**.
   The Route Domain List screen opens.
2. Click **Create**.
   The New Route Domain screen opens.
3. In the **Name** field, type a name for the route domain.

   This name must be unique within the administrative partition in which the route domain resides.
4. In the **ID** field, type an ID number for the route domain.

   This ID must be unique on the BIG-IP system; that is, no other route domain on the system can have this ID.
5. For the **Parent Name** setting, retain the default value.
6. For the **VLANs** setting, from the **Available** list, select a VLAN name and move it to the **Members** list.

   Select the VLAN that processes the application traffic relevant to this route domain.

   Configuring this setting ensures that the BIG-IP system immediately associates any self IP addresses pertaining to the selected VLANs with this route domain.
7. Click **Finished**.
   The system displays a list of route domains on the BIG-IP system.

You now have another route domain on the BIG-IP system.

## 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. From the **Profile Type** list, select one:

   - **APM-LTM** - Select for a web access management configuration.
   - **SSO** - Select only when you do not need to configure an access policy.
   - **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
   - **SSL-VPN** - Select for other types of access, such as network access, portal access, application access. (Most access policy items are available for this type.)
   - **ALL** - Select for any type of access.

   Additional settings display.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

This creates an access profile with a default access policy.

## Configuring policy routing

To follow the steps in this example, you must have Access Policy Manager® AAA server objects created for Active Directory and RADIUS as well.

You configure an access policy similar to this one to route users depending on whether they pass Active Directory authentication or RADIUS authentication. This example illustrates one way to handle a company-wide transition between one type of authentication and another, and to ensure that users get access to the correct resources, however they authenticate.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile** ***`profile_name`***.
   The visual policy editor opens the access policy in a separate screen.
5. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
6. On the Logon tab, select **Logon Page** and click the **Add Item** button.

The Logon Page Agent properties screen opens.

7. Make any changes that you require to the logon page properties and click **Save**.
   The properties screen closes and the visual policy editor displays.
8. On the fallback branch after the previous action, click the **(+)** icon to add an item to the access policy.
   A popup screen opens.
9. On the Authentication tab, select **AD Auth**.
   A properties screen displays.
10. From the **Server** list, select a server.
11. Click **Save**.
    The properties screen closes and the visual policy editor displays.
12. On the Successful branch after the previous action, click the **(+)** icon.
    A popup screen opens.
13. Assign resources to the users that successfully authenticated with Active Directory.
    a) On the Assignment tab, select the **Advanced Resource Assign** agent, and click **Add Item**.
       The Resource Assignment window opens.
    b) Click **Add new entry**.
       An **Empty** entry displays.
    c) Click the **Add/Delete** link below the entry.
       The screen changes to display resources on multiple tabs.
    d) On the Network Access tab, select a network access resource.
    e) (Optional) Optionally, on the Webtop tab, select a network access webtop.
    f) Click **Update**.
       The popup screen closes.
    g) Click **Save**.
       The properties screen closes and the visual policy editor is displayed.
    h) Click the ending that follows the Advanced Resource Assign action and change it to an allow ending, by selecting **Allow** and clicking **Save**.

14. On the fallback branch after the Active Directory action, click the **(+)** icon to add an item to the access policy.

    In this case, fallback indicates failure. For users that did not pass Active Directory authentication, you can configure RADIUS authentication and select a route domain for them so that they go to a different gateway.

    A popup screen opens.
15. Type `radi` in the search box, select **RADIUS Auth** from the results, and click **Add Item**.
    A popup screen opens.
16. From the **AAA Server** list, select a RADIUS server and click **Save**.
    The popup screen closes and the visual policy editor displays.
17. On the Successful branch after the previous action, click the **(+)** icon.
    A popup screen opens.
18. On the Assignment tab, select **Route Domain and SNAT Selection** and click the **Add Item** button.
    This opens the popup screen for the action.
19. From the Route Domain list, select a route domain and click **Save**.
    The popup screen closes and the visual policy editor displays.
20. On the successful branch after the route domain selection action, click the **(+)** icon.
    A popup screen opens.
21. Assign resources to the users that successfully authenticated with RADIUS.
    a) On the Assignment tab, select the **Advanced Resource Assign** agent, and click **Add Item**.
       The Resource Assignment window opens.

b) Click **Add new entry**.
An **Empty** entry displays.

c) Click the **Add/Delete** link below the entry.
The screen changes to display resources on multiple tabs.

d) On the Network Access tab, select a network access resource.

Note that you can assign the same network access resource to clients whether they authenticate with Active Directory or RADIUS. You assigned a different route domain to the clients that successfully authenticated with RADIUS. As a result, both types of clients will reach separate routers.

e) (Optional) Optionally, on the Webtop tab, select a network access webtop.

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

g) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

h) Click the ending that follows the Advanced Resource Assign action and change it to an allow ending, by selecting **Allow** and clicking **Save**.

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

# Chapter 4

## Synchronizing Access Policies

- *Overview: Syncing access policies with a Sync-Only device group*
- *Task summary*

## Overview: Syncing access policies with a Sync-Only device group

This implementation describes how to sync access policies from one BIG-IP® Access Policy Manager® device to another Access Policy Manager device, or to multiple devices in a device group. This allows you to maintain up-to-date access policies on multiple Access Policy Manager devices, while adjusting appropriate settings for objects that are specific to device locations.

To synchronize access policies between multiple devices, you configure a Sync-Only device group, which includes the devices between which you want to synchronize access policies. Device group setup requires establishing trust relationships between devices and creating a device group. You set the devices in each group to use **Automatic Sync** and **Full Sync**, and then synchronize access policies one at a time, resolving conflicts as you go.

***Important:*** *Sync-Only groups must be configured before you pair Active-Standby devices. To add an Active-Standby device pair to a Sync-Only device group, first you must reset the trust between the devices. Next, you must remove the devices from the Sync-Failover device group. Next, you must add both devices to a Sync-Only device group. Finally, add the devices as an Active-Standby pair to the Sync-Failover group.*

### About device groups and synchronization

When you have more than one BIG-IP® device in a local trust domain, you can synchronize BIG-IP configuration data among those devices by creating a device group. A *device group* is a collection of BIG-IP devices that trust each other and synchronize their BIG-IP configuration data. If you want to exclude certain devices from ConfigSync, you can simply exclude them from membership in that particular device group.

You can synchronize some types of data on a global level across all BIG-IP devices, while synchronizing other data in a more granular way, on an individual application level to a subset of devices.

***Important:*** *To configure redundancy on a device, you do not need to explicitly specify that you want the BIG-IP device to be part of a redundant configuration. Instead, this occurs automatically when you add the device to an existing device group.*

### Before you configure device trust

Before you configure device trust, you should consider the following:

- Only version 11.x or later systems can join the local trust domain.
- You can manage device trust when logged in to a certificate signing authority only. You cannot manage device trust when logged in to a subordinate non-authority device.
- If you reset trust authority on a certificate signing authority by retaining the authority of the device, you must subsequently recreate the local trust domain and the device group.
- As a best practice, you should configure the ConfigSync and mirroring addresses on a device before you add that device to the trust domain.
- You must configure DNS on all systems.
- You must configure NTP on all systems, preferably to the same NTP server.

# Task summary

The configuration process for a BIG-IP® system entails configuring a Sync-Only device group, syncing access policies to a device group, and resolving conflicts caused by location-specific and dynamic resources. You must pre-configure a device group to sync access policies to multiple systems.

*Establishing device trust*
*Creating a Sync-Only device group for access policy sync*
*Synchronizing an access policy across devices initially*
*Configuring static resources with access policy sync*
*Configuring dynamic resources with access policy sync*
*Resolving access policy sync conflicts*

## Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices `A`, `B`, and `C` each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device `A` and add devices `B` and `C` to the local trust domain. Note that there is no need to repeat this process on devices `B` and `C`.

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
   - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
   - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
   - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
   - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Creating a Sync-Only device group for access policy sync

You perform this task to create a Sync-Only type of device group. When you create a Sync-Only device group, the BIG-IP® system can then automatically synchronize certain types of data such as security policies to the other devices in the group, even when some of those devices reside in another network. You can perform this task on any BIG-IP device within the local trust domain.

***Important:*** *When you sync access policies from one device to another, you can only select a device group to which to sync an access policy, if the device group is configured with the settings specified in this task.*

1. On the Main tab, click **Device Management** > **Device Groups**.
2. On the Device Groups list screen, click **Create**.
   The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Only**, and type a description for the device group.
4. For the **Members** setting, select an IP address and host name from the **Available** list for each BIG-IP device that you want to include in the device group. Use the Move button to move the host name to the **Includes** list.

   The list shows any devices that are members of the device's local trust domain.
5. Select the **Automatic Sync** check box.
6. Select the **Full Sync** check box.
7. Click **Finished**.

You now have a Sync-Only type of device group containing BIG-IP devices as members.

***Important:*** *Sync-Only groups must be configured before you pair Active-Standby devices. To add an Active-Standby device pair to a Sync-Only device group, first reset the trust between the devices. Next, remove the devices from the Sync-Failover device group. Then add both devices to a Sync-Only device group. Finally, add the devices as an Active-Standby pair to the Sync-Failover group.*

## Synchronizing an access policy across devices initially

After you set up a sync-only device group for your Access Policy Manager devices, you can sync an access policy from one device to other devices in the group. You can perform an access policy sync from any device in the group.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **Policy Sync**.
   A list of access policies and related sync status information opens. The sync status is either:

   ### Policies with no sync pending
   No synchronization is currently in progress for access policies on this list.

   ### Policies with sync pending
   A synchronization is in progress for these access policies. Select an access policy from this list to view the Sync Details or Resolve Conflicts panel for it.
2. Select an access policy and click the **Sync Access Policy** button.

The **Policy Sync** screen opens.

3. From the **Device Group** list, select the device group to which to sync the access policy.

   This list displays only Sync-Only device groups with automatic sync and full sync enabled.
4. In the **Description** field, type a description of the reason for the access policy sync operation.
5. From the **Ignore errors due to Variable Assign Agent during sync** list, select whether to ignore errors caused by syncing the variable assign agent.

   ***Note:*** *If the access policy includes a Variable Assign action, errors occur when resources are missing from the target device. If you select* ***Yes****, you might need to manually configure the resources on the target device.*
6. Click **Sync**.
   The sync process begins.

The access policy is synced between devices in the device group.

***Important:*** *An access policy sync operation takes 25-30 seconds, depending on the number of devices.*

## Configuring static resources with access policy sync

A BIG-IP® Access Policy Manager® might exist in a different physical location from another BIG-IP in the same device group, and might use different resources that are specific to that location or local network. For example, different authentication servers might exist in each location. Configure static resources to set these static resources for devices in different locations.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **Policy Sync**.
   If policies are present and configured for sync, a list of access policies and related sync status information opens.
2. Select an access policy and click the **Sync Access Policy** button.
   The **Policy Sync** screen opens.
3. Click the **Advanced Settings** button, then click **Static Resources**.
   The list displays a name, type, and **Location Specific** check box for each resource. You might need to configure a location-specific resource differently on a remote system. With the Location Specific check box selected, the first time a resource is synced as part of a policy, you must resolve its configuration on the remote system. Subsequent access policy sync operations do not modify a previously synced location-specific resource.

   ***Important:*** *Many resource types are marked as location-specific by default. If a resource is not location-specific in this configuration, clear the* ***Location Specific*** *check box.*
4. Click the **OK** button.
   The APM Policy Sync screen is displayed.
5. Click the **Sync** button.

The access policy is synced between devices in the device group.

If this is the first time you sync a policy with location-specific resources, or you have added location-specific resources to the policy sync operation, you must resolve the location-specific issues on each affected target system.

## Configuring dynamic resources with access policy sync

When access policies are configured with the Variable Assign action, some dynamically assigned resources might not be available on sync target machines. You can specify that such resources are included in a policy sync operation and will be created on the target devices.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **Policy Sync**.
   A list of access policies and related sync status information opens.
2. Select an access policy and click the **Sync Access Policy** button.
   The **Policy Sync** screen opens.
3. Click the **Advanced Settings** button, then click **Dynamic Resources**.
   The list displays a name, type, **Dynamic Resource**, and **Location Specific** check box for each resource.
4. Select the dynamic resources by clicking the check boxes.
5. Click the **OK** button.
   The APM Policy Sync screen is displayed.
6. Click the **Sync** button.

The access policy is synced between devices in the device group.

Resolve the location-specific issues on each affected target system.

## Resolving access policy sync conflicts

After you sync an access policy, you might need to resolve conflicts on the target devices. Conflicts occur when an access policy contains new location-specific resources.

1. On a target system that requires conflicts to be resolved, on the Main tab, click **Access Policy** > **Access Profiles** > **Policy Sync**.
   A list of access policies and related sync status information opens.
2. From the **Policies with Sync Pending** list, select an access policy for which you want to resolve conflicts.
   If conflicts exist, the Resolve Conflicts panel displays one entry and an Unresolved link for each location-specific or dynamic resource that is in conflict.
3. Click an **Unresolved** link.
   A popup window opens displaying two panes.
   - A navigation pane with one or more groups of settings. In the navigation pane, an icon indicates that data is required.
   - A data entry pane in which you can type or select values. The data entry pane displays the values from the source device, with labels for required fields asterisked (*) and filled with yellow.
4. Select a group of settings from the left pane, and type or select the required information in the right pane until you have added the required information.

   You can fill in the required information only, or any other information and settings you wish to configure.

   In the navigation pane, an icon indicates that required information for a group of settings is complete.
5. Click the **OK** button.
   The popup window closes. If no more **Unresolved** links remain, the **Finish** button is active.
6. After you resolve all conflicts, click the **Finish** button.

Access Policy Manager creates the resolved access policy on the device. After sync is completed on all target devices, sync status on the source device will be updated to **Sync completed**.

## About ignoring errors due to the Variable Assign agent

The **Ignore errors due to Variable Assign Agent during sync** setting affects system behavior only when a Variable Assign agent is included in an access policy, and the Variable Assign agent uses resources.

***Important:*** *The user name and password fields are not considered to be resources.*

If you set **Ignore errors due to Variable Assign Agent during sync** to **Yes**:

- If you do not select any dynamic resources, after the policy sync completes you must create all needed resources on each target system.
- If you select the appropriate dynamic resources, after the policy sync completes, you must resolve any conflicts that exist on the target systems. If you do not select all the dynamic resources that are required, you must create them on each target system.

If you set **Ignore errors due to Variable Assign Agent during sync** to **No**:

- If you do not select any dynamic resources, an error is displayed and the policy sync does not start.
- If you select the appropriate dynamic resources, after the policy sync completes, you must resolve any conflicts that exist on the target systems.

## Implementation result

To summarize, you now have synchronized access policies between devices in a sync-only device group.

### Understanding sync details

On the **Sync Details** tab, you can see sync status for an access policy.

| Column | Description |
|---|---|
| Device | The specific device to which the access policy was synced. |
| Sync Status | One of the following:<br>• `Sync initiated` - This status indicates that the sync is in progress, initiated from this device.<br>• `Sync Completed` - This status indicates that the sync completed successfully to the specified device.<br>• `Not available` - This status indicates that the device to which the sync was initiated was not available, or not available yet.<br>• `Sync cancelled` - This status indicates that the sync was cancelled before it could complete to the specified device.<br>• `User Changes Failed` - This status indicates that policy creation failed after the administrator resolved the conflicts. Sync success is set to Standby.<br>• `Pending location specific updates` - This status indicates that the access policy on the specified device requires updates because of conflicts due to location-specific information. |

| Column | Description |
|---|---|
|  | Resolve the conflicts to complete the sync successfully. |
| Status End Time | The time at which the last status entry completed on the specific device. |
| Sync Status Details | More information about the Sync Status for a specific device. |

### Understanding sync history

On the **Sync History** tab, you can see the sync history for an access policy.

| Column | Description |
|---|---|
| Last sync | The last time a sync was initiated for this access policy. |
| Last Sync Status | The outcome of the last sync for this access policy. |
| Device Group | The device group to which the access policy was synced. |
| Description | A clickable icon that presents information about the sync operation for the device group. |
| Non Location Specific Objects | An access policy was created with certain resources which the sync process indicates are not location-specific, but that might in fact be location-specific on the target device. This column lists such objects, which you can then verify by checking the objects on the remote systems, and modifying if necessary. |

# Chapter 5

# Maintaining OPSWAT Libraries with a Sync-Failover Device Group

- *Overview: Updating antivirus and firewall libraries with a Sync-Failover device group*
- *Task summary*
- *Implementation result*

# Overview: Updating antivirus and firewall libraries with a Sync-Failover device group

This implementation describes how to upload antivirus and firewall libraries from OPSWAT to one BIG-IP® Access Policy Manager® device, and to install an antivirus and firewall library to that device, or to multiple devices in a device group.

To download OPSWAT OESIS library updates, you must have an account with OPSWAT, and be able to download software updates.

To synchronize installation between multiple devices, you configure a Sync-Failover device group, which includes the devices between which you want to synchronize installation of updates. Device group setup requires establishing trust relationships between devices, creating a device group, and synchronization of settings.

## About device groups and synchronization

When you have more than one BIG-IP® device in a local trust domain, you can synchronize BIG-IP configuration data among those devices by creating a device group. A *device group* is a collection of BIG-IP devices that trust each other and synchronize their BIG-IP configuration data. If you want to exclude certain devices from ConfigSync, you can simply exclude them from membership in that particular device group.

You can synchronize some types of data on a global level across all BIG-IP devices, while synchronizing other data in a more granular way, on an individual application level to a subset of devices.

***Important:*** *To configure redundancy on a device, you do not need to explicitly specify that you want the BIG-IP device to be part of a redundant configuration. Instead, this occurs automatically when you add the device to an existing device group.*

## Before you configure device trust

Before you configure device trust, you should consider the following:

- Only version 11.x or later systems can join the local trust domain.
- You can manage device trust when logged in to a certificate signing authority only. You cannot manage device trust when logged in to a subordinate non-authority device.
- If you reset trust authority on a certificate signing authority by retaining the authority of the device, you must subsequently recreate the local trust domain and the device group.
- As a best practice, you should configure the ConfigSync and mirroring addresses on a device before you add that device to the trust domain.

# Task summary

The configuration process for a BIG-IP® system entails adding the OPSWAT library update to one system, then installing it to that same system, or to a device group. You must pre-configure a device group to install the update to multiple systems.

*Establishing device trust*

*Adding a device to the local trust domain*
*Creating a Sync-Failover device group*
*Manually synchronizing the BIG-IP configuration*
*Uploading an OPSWAT update to Access Policy Manager*
*Installing an OPSWAT update on one or more Access Policy Manager devices*
*Viewing supported products in the installed OPSWAT EPSEC version*
*Establishing device trust*
*Adding a device to the local trust domain*
*Creating a Sync-Only device group*
*Uploading an OPSWAT update to Access Policy Manager*
*Installing an OPSWAT update on one or more Access Policy Manager devices*
*Viewing supported products in the installed OPSWAT EPSEC version*

## Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices `A`, `B`, and `C` each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device `A` and add devices `B` and `C` to the local trust domain. Note that there is no need to repeat this process on devices `B` and `C`.

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
   - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
   - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
   - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
   - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Adding a device to the local trust domain

Verify that each BIG-IP® device that is to be part of a local trust domain has a device certificate installed on it.

Follow these steps to log in to any BIG-IP® device on the network and add one or more devices to the local system's local trust domain.

***Note:*** *Any BIG-IP devices that you intend to add to a device group at a later point must be members of the same local trust domain.*

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. In the Peer Authority Devices or the Subordinate Non-Authority Devices area of the screen, click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
    - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
    - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
    - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
    - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the displayed information is correct.
6. Click **Finished**.

After you perform this task, the local device and the device that you specified in this procedure have a trust relationship and, therefore, are qualified to join a device group.

## Creating a Sync-Failover device group

This task establishes failover capability between two or more BIG-IP® devices. If an active device in a Sync-Failover device group becomes unavailable, the configuration objects fail over to another member of the device group and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

Repeat this task for each Sync-Failover device group that you want to create for your network configuration.

1. On the Main tab, click **Device Management** > **Device Groups**.
2. On the Device Groups list screen, click **Create**.
   The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Failover**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.

5. In the Configuration area of the screen, select a host name from the **Available** list for each BIG-IP device that you want to include in the device group, including the local device. Use the Move button to move the host name to the **Includes** list.

   The **Available** list shows any devices that are members of the device's local trust domain but not currently members of a Sync-Failover device group. A device can be a member of one Sync-Failover group only.

6. For the **Network Failover** setting, select or clear the check box:

   - Select the check box if you want device group members to handle failover communications by way of network connectivity. This choice is required for active-active configurations.
   - Clear the check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

   For active-active configurations, you must select network failover, as opposed to serial-cable (hard-wired) connectivity.

7. For the **Automatic Sync** setting, select or clear the check box:

   - Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
   - Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.

8. For the **Full Sync** setting, select or clear the check box:

   - Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
   - Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

   If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

9. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of `1024`, or type a different value.

   This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

10. Click **Finished**.

You now have a Sync-Failover type of device group containing BIG-IP devices as members.

## Manually synchronizing the BIG-IP configuration

Before you perform this task, verify that device trust has been established and that all devices that you want to synchronize are members of a device group.

You perform this task when the automatic sync feature is disabled and you want to manually synchronize BIG-IP® configuration data among the devices in the device group. This synchronization ensures that any device in the device group can process application traffic successfully. You can determine the need to perform this task by viewing sync status in the upper left corner of any BIG-IP Configuration utility screen. A status of `Changes Pending` indicates that you need to perform a config sync within the device group.

***Important:*** *You can log into any device in the device group to perform this task.*

1. On the Main tab, click **Device Management** > **Overview**.
2. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.
   The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, in the Sync Status column, select a device.
4. From the **Sync** options list, select an option:

| Option | Description |
|---|---|
| **Sync Device to Group** | Select this option when you want to sync the configuration of the selected device to the other device group members. |
| **Sync Group to Device** | Select this option when you want to sync the most recent configurations of one or more device group members to the selected device. |

5. Click **Sync**.

The BIG-IP system compares the configuration data on the local device with the data on each device in the device group, and synchronizes the most recently-changed configuration data from one or more source devices to one or more target devices. Note that the system does not synchronize non-floating self IP addresses.

## Uploading an OPSWAT update to Access Policy Manager

When new updates to OPSWAT antivirus and firewall libraries are made available, you can add these updates to the BIG-IP® system. To upload an update to the BIG-IP system, you must first download an update, using a registered account, from the OPSWAT web site.

1. On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
   The Antivirus Check Updates screen displays a list of OPSWAT packages available on the device.
2. Click the **Upload** button to add an OPSWAT update.
   The **Upload Package** screen appears.
3. Click **Browse** and select an OPSWAT package ZIP file to upload.
4. Select an install option from the list.
   - Select **Do Not Install** to upload the package to the local device, but without installing the OPSWAT package on the system.
   - Select **Install on this device** to upload the package to the local device, and then install the OPSWAT package to this device.
   - Select **Install on device group** to upload the package to the local device, and then install the OPSWAT package on the device group. A list of available device groups appears, and you can select the device group on which to install.
5. Click **Ok**.

The OPSWAT package file is added to the list on the **System** > **Software Management** > **Antivirus Check Updates** page. You can install or delete OPSWAT packages from this page.

## Installing an OPSWAT update on one or more Access Policy Manager devices

After you have uploaded an OPSWAT antivirus and firewall library update to the BIG-IP® system, you can install the update to one or more BIG-IP systems in a device group.

1. On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
   The Antivirus Check Updates screen displays a list of OPSWAT packages available on the device.
2. Double-click an OPSWAT package to view details about the update and included firewall or antivirus libraries.
3. Select an OPSWAT package and click **Install**.
   The Install Package screen opens.
4. Select **Install on device group** to upload the package to the local device, and then install the OPSWAT package on the device group. A list of available device groups appears, and you can select the device group on which to install.
5. Click **Ok**.

The OPSWAT update is installed on the selected systems. You can view the installed and available OPSWAT versions on the **Software Management** > **Antivirus Check Updates** screen.

## Viewing supported products in the installed OPSWAT EPSEC version

You can always view details about any installed OPSWAT version, including supported antivirus, firewall, anti-spyware, hard disk encryption, peer-to-peer software, patch management software, and Windows Health Agent features for supported platforms.

1. To view the details for the current device group:
   a) Click the F5® logo to go to the start (Welcome) page.
   b) In the Support area, click the **OSWAT application integration support charts** link.
      The OPSWAT Integration web page opens in a new browser tab or window. By default, this page shows Antivirus Integration for Windows.
   c) From the lists at the top of the screen, select the page to view. You can select the supported EPSEC feature, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.
   d) Click the **Show** button to view the list of supported products for the type and platform you selected.

2. To view the details for another device group or another OESIS version:
   a) On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
      The Package Status screen displays a list of OPSWAT packages available on the device.
   b) Click the **Device EPSEC Status** button.
      The **Device EPSEC Status** screen appears and shows the installed OPSWAT version.
   c) To select a different device group on which to view the installed OPSWAT version, select the device group from the **Local Device/Device Group** list.
   d) Under **Installed OESIS version**, click the version number for which you want to view the OPSWAT features chart.
      The OPSWAT Integration web page opens in a new browser tab or window. By default, this page shows Antivirus Integration for Windows.
   e) From the lists at the top of the screen, select the page to view. You can select the supported EPSEC feature, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.
   f) Click the **Show** button to view the list of supported products for the type and platform you selected.

## Implementation result

To summarize, you now have uploaded an OPSWAT update to one BIG-IP® system, and installed it to one system, or to multiple systems in a device group.

You can view the installed and available OPSWAT versions on the **Software Management** > **Antivirus Check Updates** screen.

Chapter

6

# Maintaining OPSWAT Libraries with a Sync-Only Device Group

- *Overview: Updating antivirus and firewall libraries with a Sync-Only device group*
- *Task summary*
- *Implementation result*

# Overview: Updating antivirus and firewall libraries with a Sync-Only device group

This implementation describes how to upload antivirus and firewall libraries from OPSWAT to one BIG-IP® Access Policy Manager® device, and to install an antivirus and firewall library to that device, or to multiple devices in a device group.

To download OPSWAT OESIS library updates, you must have an account with OPSWAT, and be able to download software updates.

To synchronize installation between multiple devices, you configure a Sync-Only device group, which includes the devices between which you want to synchronize installation of updates. Device group setup requires establishing trust relationships between devices, creating a device group, and synchronization of settings.

## About device groups and synchronization

When you have more than one BIG-IP® device in a local trust domain, you can synchronize BIG-IP configuration data among those devices by creating a device group. A *device group* is a collection of BIG-IP devices that trust each other and synchronize their BIG-IP configuration data. If you want to exclude certain devices from ConfigSync, you can simply exclude them from membership in that particular device group.

You can synchronize some types of data on a global level across all BIG-IP devices, while synchronizing other data in a more granular way, on an individual application level to a subset of devices.

***Important:*** *To configure redundancy on a device, you do not need to explicitly specify that you want the BIG-IP device to be part of a redundant configuration. Instead, this occurs automatically when you add the device to an existing device group.*

## Before you configure device trust

Before you configure device trust, you should consider the following:

- Only version 11.x or later systems can join the local trust domain.
- You can manage device trust when logged in to a certificate signing authority only. You cannot manage device trust when logged in to a subordinate non-authority device.
- If you reset trust authority on a certificate signing authority by retaining the authority of the device, you must subsequently recreate the local trust domain and the device group.
- As a best practice, you should configure the ConfigSync and mirroring addresses on a device before you add that device to the trust domain.

# Task summary

The configuration process for a BIG-IP® system entails adding the OPSWAT library update to one system, then installing it to that same system, or to a device group. You must pre-configure a device group to install the update to multiple systems.

*Establishing device trust*

*Adding a device to the local trust domain*
*Creating a Sync-Failover device group*
*Manually synchronizing the BIG-IP configuration*
*Uploading an OPSWAT update to Access Policy Manager*
*Installing an OPSWAT update on one or more Access Policy Manager devices*
*Viewing supported products in the installed OPSWAT EPSEC version*
*Establishing device trust*
*Adding a device to the local trust domain*
*Creating a Sync-Only device group*
*Uploading an OPSWAT update to Access Policy Manager*
*Installing an OPSWAT update on one or more Access Policy Manager devices*
*Viewing supported products in the installed OPSWAT EPSEC version*

## Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices `A`, `B`, and `C` each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device `A` and add devices `B` and `C` to the local trust domain. Note that there is no need to repeat this process on devices `B` and `C`.

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
   - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
   - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
   - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
   - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Adding a device to the local trust domain

Verify that each BIG-IP® device that is to be part of a local trust domain has a device certificate installed on it.

Follow these steps to log in to any BIG-IP® device on the network and add one or more devices to the local system's local trust domain.

***Note:*** *Any BIG-IP devices that you intend to add to a device group at a later point must be members of the same local trust domain.*

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. In the Peer Authority Devices or the Subordinate Non-Authority Devices area of the screen, click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
   - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
   - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
   - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
   - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the displayed information is correct.
6. Click **Finished**.

After you perform this task, the local device and the device that you specified in this procedure have a trust relationship and, therefore, are qualified to join a device group.

## Creating a Sync-Only device group

You perform this task to create a Sync-Only type of device group. When you create a Sync-Only device group, the BIG-IP® system can then automatically synchronize certain types of data such as security policies and acceleration applications and policies to the other devices in the group, even when some of those devices reside in another network. You can perform this task on any BIG-IP device within the local trust domain.

1. On the Main tab, click **Device Management** > **Device Groups**.
2. On the Device Groups list screen, click **Create**.
   The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Only**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. For the **Members** setting, select an IP address and host name from the **Available** list for each BIG-IP device that you want to include in the device group. Use the Move button to move the host name to the **Includes** list.

The list shows any devices that are members of the device's local trust domain.

6. For the **Automatic Sync** setting, select or clear the check box:

   - Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
   - Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.

7. For the **Full Sync** setting, select or clear the check box:

   - Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
   - Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

   If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

8. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of `1024`, or type a different value.

   This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

9. Click **Finished**.

You now have a Sync-Only type of device group containing BIG-IP devices as members.

## Uploading an OPSWAT update to Access Policy Manager

When new updates to OPSWAT antivirus and firewall libraries are made available, you can add these updates to the BIG-IP® system. To upload an update to the BIG-IP system, you must first download an update, using a registered account, from the OPSWAT web site.

1. On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
   The Antivirus Check Updates screen displays a list of OPSWAT packages available on the device.
2. Click the **Upload** button to add an OPSWAT update.
   The **Upload Package** screen appears.
3. Click **Browse** and select an OPSWAT package ZIP file to upload.
4. Select an install option from the list.

   - Select **Do Not Install** to upload the package to the local device, but without installing the OPSWAT package on the system.
   - Select **Install on this device** to upload the package to the local device, and then install the OPSWAT package to this device.
   - Select **Install on device group** to upload the package to the local device, and then install the OPSWAT package on the device group. A list of available device groups appears, and you can select the device group on which to install.

5. Click **Ok**.

The OPSWAT package file is added to the list on the **System** > **Software Management** > **Antivirus Check Updates** page. You can install or delete OPSWAT packages from this page.

## Installing an OPSWAT update on one or more Access Policy Manager devices

After you have uploaded an OPSWAT antivirus and firewall library update to the BIG-IP® system, you can install the update to one or more BIG-IP systems in a device group.

1. On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
   The Antivirus Check Updates screen displays a list of OPSWAT packages available on the device.
2. Double-click an OPSWAT package to view details about the update and included firewall or antivirus libraries.
3. Select an OPSWAT package and click **Install**.
   The Install Package screen opens.
4. Select **Install on device group** to upload the package to the local device, and then install the OPSWAT package on the device group. A list of available device groups appears, and you can select the device group on which to install.
5. Click **Ok**.

The OPSWAT update is installed on the selected systems. You can view the installed and available OPSWAT versions on the **Software Management** > **Antivirus Check Updates** screen.

## Viewing supported products in the installed OPSWAT EPSEC version

You can always view details about any installed OPSWAT version, including supported antivirus, firewall, anti-spyware, hard disk encryption, peer-to-peer software, patch management software, and Windows Health Agent features for supported platforms.

1. To view the details for the current device group:
   a) Click the F5® logo to go to the start (Welcome) page.
   b) In the Support area, click the **OSWAT application integration support charts** link.
   The OPSWAT Integration web page opens in a new browser tab or window. By default, this page shows Antivirus Integration for Windows.
   c) From the lists at the top of the screen, select the page to view. You can select the supported EPSEC feature, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.
   d) Click the **Show** button to view the list of supported products for the type and platform you selected.

2. To view the details for another device group or another OESIS version:
   a) On the Main tab, click **System** > **Software Management** > **Antivirus Check Updates**.
   The Package Status screen displays a list of OPSWAT packages available on the device.
   b) Click the **Device EPSEC Status** button.
   The **Device EPSEC Status** screen appears and shows the installed OPSWAT version.
   c) To select a different device group on which to view the installed OPSWAT version, select the device group from the **Local Device/Device Group** list.
   d) Under **Installed OESIS version**, click the version number for which you want to view the OPSWAT features chart.
   The OPSWAT Integration web page opens in a new browser tab or window. By default, this page shows Antivirus Integration for Windows.
   e) From the lists at the top of the screen, select the page to view. You can select the supported EPSEC feature, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.

f) Click the **Show** button to view the list of supported products for the type and platform you selected.

## Implementation result

To summarize, you now have uploaded an OPSWAT update to one BIG-IP® system, and installed it to one system, or to multiple systems in a device group.

You can view the installed and available OPSWAT versions on the **Software Management** > **Antivirus Check Updates** screen.

# Chapter 7

## Adding Hosted Content to Access Policy Manager

- *About uploading custom files to Access Policy Manager*
- *Task summary*
- *Implementation result*

## About uploading custom files to Access Policy Manager

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

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

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

**Upload Only**

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

**Upload and Extract**

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

## Understanding hosted content

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

## About accessing hosted content

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

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

## Permissions for hosted content

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

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

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

# Task summary

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

### Task summary

*Uploading files to Access Policy Manager*
*Associating hosted content with access profiles*

## Uploading files to Access Policy Manager

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

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

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

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

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

## Associating hosted content with access profiles

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

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

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

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

# Implementation result

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

# Chapter 8

# Editing Hosted Content with Access Policy Manager

- *About editing hosted files on Access Policy Manager*
- *Task summary*
- *Implementation result*

# 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 9

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

- *About hosting a BIG-IP Edge Client file on Access Policy Manager*
- *Task summary*
- *Implementation result*

## 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 **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
6. On the Assignment tab, select the **Webtop and Links Assign** agent and click **Add Item**.
   The Webtop and Links Assignment screen opens.
7. In the **Name** field, type a name for the access policy item.

   This name is displayed in the action field for the access policy.
8. On the Webtop & Webtop Links Assignment screen, next to the type of resource you want to add, click the **Add/Delete** link.

   Available resources are listed.
9. To assign resources, select the options you want.
10. Click the **Save** button to save changes to the access policy item.

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

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

## Implementation result

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

# Chapter 10

## Hosting Files with Portal Access on Access Policy Manager

- *About using hosted files with a Portal Access resource*
- *Task summary*
- *Implementation result*

# 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

## A

access policies
  *32*
  resolving conflicts *36*
access policy
  adding a dynamic ACL *21*
  adding a webtop and webtop links *67*
  configuring dynamic resources for sync *36*
  configuring static resources for sync *35*
  configuring timeout for *14*
  configuring timeout in *14*
  creating *16*
  Dynamic ACL action *20*
  initial sync *34*
  routing *26*
access policy sync
  configuring *33*
  described *32*
  result of *37*
access profile
  creating *15*, *27*
  timeout properties *15*
access profiles
  associating with hosted content *58*, *66*, *71*
ACL
  adding dynamically *21*
  dynamic, about *20*
  dynamic configuration *20*
  formats supported *20*
adding an OPSWAT update *44*, *51*
anti-spyware
  viewing supported products *45*, *52*
antivirus
  adding updates to the system *44*, *51*
  installing updates to the system *45*, *52*
  updating *40*, *48*
  viewing supported products *45*, *52*
antivirus and firewall libraries *40*, *48*
antivirus updates
  described *40*, *48*
authority devices
  and device trust *32*, *40*, *48*
automatic synchronization
  enabling *34*
  enabling and disabling *50*

## B

BIG-IP Edge Client file
  uploading to Access Policy Manager *66*
BIG-IP versions
  and device trust *32*, *40*, *48*

## C

certificates
  for device trust *42*, *50*
Cisco ACL format
  specifying *24*
client file
  adding to webtop link *68*
configuration data, synchronizing *32*, *40*, *48*
configuration synchronization
  syncing to group *43*
conflicts
  resolving between devices *36*
connectivity profile
  customizing *64*
  for Mac Edge Clients *64*

## D

default traffic groups *40*, *48*
deleting a file *61*
device discovery
  for device trust *33*, *41–42*, *49–50*
device groups
  and synchronizing configuration data *32*, *40*, *48*
  creating *34*, *42*, *50*
device trust
  adding domain members *42*, *50*
  establishing *33*, *41*, *49*
  managing *32*, *40*, *48*
  resetting *32*, *40*, *48*
DNS
  configuring *32*
dynamic ACL
  access policy action *20*
dynamic ACL action
  adding to an access policy *21*
dynamic resources
  ignoring errors *37*

## E

editing files
  properties *60*
  renaming *60*
editing hosted files
  results *58*, *62*
EPSEC
  viewing product support *45*, *52*
errors, ignoring
  due to Variable Assign agent *37*
example files
  uploading to Access Policy Manager *57*, *70*

## F

F5 ACL format
  specifying *22*
files
  about files *56*
  associating with access profiles *58*, *66*, *71*

files *(continued)*
- deleting *61*
- editing *60*
- editing properties *60*
- hosting a client file *64*
- moving *60*
- permissions *56*
- replacing *61*
- uploading new *61*
- using to define Portal Access resource *70*

firewall
- adding updates to the system *44*, *51*
- installing updates to the system *45*, *52*
- updating *40*, *48*
- viewing supported products *45*, *52*

firewall updates
- described *40*, *48*

## H

hard disk encryption
- viewing supported products *45*, *52*

health agent software
- viewing supported products *45*, *52*

hosted content
- about *56*
- about editing on Access Policy Manager *60*
- about uploading to Access Policy Manager *56*
- about using with Portal Access *70*
- hosting a BIG-IP Edge client file *64*
- permissions *56*
- specifying for portal access *72*

## I

installing an OPSWAT update *45*, *52*

## L

local trust domain
- and device groups *34*, *42*, *50*
- defined *33*, *41–42*, *49–50*
- joining *32*, *40*, *48*

location-specific resources
- resolving conflicts *36*

## M

Mac client package
- downloading *66*
- for BIG-IP Edge Clients *66*

MIME type
- editing *60*

moving a file *60*

## N

network failover
- configuring *42*

NTP
- configuring *32*

## O

OPSWAT
- installing updates *45*, *52*
- OESIS library updates *40*, *48*
- uploading updates *44*, *51*
- viewing product support *45*, *52*

OPSWAT update
- adding *40*, *48*
- result of *46*, *53*

## P

patch management
- viewing supported products *45*, *52*

peer-to-peer software
- viewing supported products *45*, *52*

permissions
- editing *60*
- for hosted content *56*

policy routing
- configuring in an access policy *27*

pools
- creating *14*

portal access
- creating resource item for hosted content *72*

portal access configuration
- creating for hosted content *71*
- creating manually *71*

portal access with hosted files
- results *73*

## R

renaming a file *60*

replacing a file *61*

resolving conflicts between devices *36*

route domain
- selecting from an access policy *27*
- selecting in an access policy *26*

route domains
- creating *26*

## S

Sync-Failover device groups
- creating *42*

synchronizing
- access policies *34*
- access policies with dynamic resources *36*
- access policies with static resources *35*

syncing
- access policies *33*

syncing an access policy
- *34*
- configuring dynamic resources *36*
- configuring static resources *35*

sync-only
- syncing access policies *32*

Sync-Only device groups
- creating *50*
- creating for access policy sync *34*

T

timeout options
for web access management 14
traffic groups
default name of 40, 48
trust domains
and local trust domain 33, 41–42, 49–50
trust relationships
establishing 32, 40, 48

U

uploading client file
example 66
uploading files
example 57, 70

V

variable assign action
syncing acess policies 36
viewing supported anti-spyware products 45, 52
viewing supported antivirus products 45, 52
viewing supported firewall products 45, 52
viewing supported hard disk encryption products 45, 52
viewing supported health agent products 45, 52
viewing supported patch management products 45, 52
viewing supported peer-to-peer software products 45, 52
virtual servers
for web access management 17

W

web access management
14
configuring a virtual server for 17
configuring timeout 15–16
configuring web server pool 14
web application
creating hosted content resource item 72
web application access
configuring 14
webtop and links assign action
adding to an access policy 67
webtop link
adding client 68
creating 67
webtops
configuring full 67

X

x509 certificates
for device trust 33, 41, 49