BIG-IP® Access Policy Manager®: Syncing Access Policies

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0441-01

Copyright

Trademarks

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

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

Patents

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

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

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

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

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

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

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

Chapter 1

Synchronizing Access Policies

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.

Attention: *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.

Attention: *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.

Attention: *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 may exist in a different physical location from another BIG-IP in the same device group, and may 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 may 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: • `Sync initiated` - This status indicates that the sync is in progress, initiated from this device. • `Sync Completed` - This status indicates that the sync completed successfully to the specified device. • `Not available` - This status indicates that the device to which the sync was initiated was not available, or not available yet. • `Sync cancelled` - This status indicates that the sync was cancelled before it could complete to the specified device. • `User Changes Failed` - This status indicates that policy creation failed after the administrator resolved the conflicts. Sync success is set to Standby. • `Pending location specific updates` - This status indicates that the access policy on the specified device requires updates because of

Column	Description
	conflicts due to location-specific information. 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 may 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.

Index