BIG-IP® Access Policy Manager®: Managing OPSWAT Libraries

Version 11.2.1

IT agility. Your way.

Table of Contents

Table of Contents

Legal Notices

Publication Date

This document was published on August 31, 2012.

Publication Number

MAN-0411-01

Copyright

Trademarks

Patents

This product may be protected by U.S. Patent 7,114,180. This list is believed to be current as of August 31, 2012.

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

Chapter 1

Maintaining OPSWAT Libraries with a Sync-Failover Device Group

Topics:

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

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 an IP address, administrator user name, and administrator password for the remote BIG-IP® device.
   This IP address can be either a management IP address or a self IP address.
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 an IP address, administrator user name, and administrator password for the remote BIG-IP® device.
   This IP address can be either a management IP address or a self IP address.
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 the 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. 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 **Selected** 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.
5. For the **Network Failover** setting:
   - Select the **Enabled** check box if you want device group members to handle failover communications by way of network connectivity.
   - Clear the **Enabled** check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

   Serial failover is not available for device groups with more than two members.
6. Click **Finished**.

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

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 to 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 configurations of all devices in the device group. 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 antivirus and firewall support in the installed OPSWAT version

After you install an OPSWAT update to one or more systems, from the system that performed the update, you can view details of the OPSWAT version, including supported antivirus and firewall features for all supported platforms.

1. 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.
2. Click the **Device Status** button.
   The **Device Status** screen appears and shows the installed OPSWAT version.
3. 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.
4. 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.
5. From the list boxes at the top of the screen, select the page to view. You can select **Antivirus** or **Firewall**, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.
6. Click the **Show** button to view the list of supported products for the type and platform you selected.

A page displays all supported products and implemented features for the OPSWAT version you specified.

Implementation result

As a result of the implementation, you have uploaded an OPSWAT update to a BIG-IP® system, and installed it to one or multiple systems in a device group.

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

Chapter 2

Maintaining OPSWAT Libraries with a Sync-Only Device Group

Topics:

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

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 an IP address, administrator user name, and administrator password for the remote BIG-IP® device.
   This IP address can be either a management IP address or a self IP address.
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 an IP address, administrator user name, and administrator password for the remote BIG-IP® device.
   This IP address can be either a management IP address or a self IP address.
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 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. 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. For the **Automatic Sync** setting, select the **Enabled** check box.
6. 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 antivirus and firewall support in the installed OPSWAT version

After you install an OPSWAT update to one or more systems, from the system that performed the update, you can view details of the OPSWAT version, including supported antivirus and firewall features for all supported platforms.

1. 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.
2. Click the **Device Status** button.
   The **Device Status** screen appears and shows the installed OPSWAT version.
3. 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.
4. 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.
5. From the list boxes at the top of the screen, select the page to view. You can select **Antivirus** or **Firewall**, and you can select to view supported products for **Windows**, **Mac**, or **Linux**.
6. Click the **Show** button to view the list of supported products for the type and platform you selected.

A page displays all supported products and implemented features for the OPSWAT version you specified.

Implementation result

As a result of the implementation, you have uploaded an OPSWAT update to a BIG-IP® system, and installed it to one or multiple systems in a device group.

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

Index