BIG-IQ™ Network Security Administration

Version 4.3

Table of Contents

Legal Notices

Publication Date

This document was published on March 6, 2014.

Publication Number

MAN-0509-01

Copyright

Trademarks

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 developed by Oracle America, Inc. Copyright ©2012.

1. Java Technology Restrictions. Licensee shall not create, modify, change the behavior of, or authorize licensees of licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developer.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icon including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at http://www.oraclc.com/html/3party.html; (b) not do anything harmful to or inconsistent with Oracle's

rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.

3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portion of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.
5. Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table I-I (Commercial Features In Java SE Product Editions) of tile Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

This product includes software developed by members of the CentOS Project under the GNU Public License, copyright ©2004-2011 by the CentOS Project.

This product includes software developed by members of the OpenJDK Project under the GNU Public License Version 2, copyright ©2012 by Oracle Corporation.

This product includes software developed by The VMWare Guest Components Team under the GNU Public License Version 2, copyright ©1999-2011 by VMWare, Inc.

This product includes software developed by The Netty Project under the Apache Public License Version 2, copyright ©2008-2012 by The Netty Project.

This product includes software developed by Stephen Colebourne under the Apache Public License Version 2, copyright ©2001-2011 Joda.org.

This product includes software developed by the GlassFish Community under the GNU Public License Version 2 with classpath exception, copyright ©2012 Oracle Corporation.

This product includes software developed by the Mort Bay Consulting under the Apache Public License Version 2, copyright ©1995-2012 Mort Bay Consulting.

This product contains software developed by members of the Jackson Project under the GNU Lesser General Public License Version 2.1, ©2007 – 2012 by the Jackson Project".

This product contains software developed by QOS.ch under the MIT License, ©2004 – 2011 by QOS.ch.

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 jQuery Foundation and other contributors, distributed under the MIT License. Copyright ©2014 jQuery Foundation and other contributors (http://jquery.com/).

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

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

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

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

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

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

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

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

This software incorporates JFreeChart, ©2000-2007 by Object Refinery Limited and Contributors, which is protected under the GNU Lesser General Public License (LGPL).

This product contains software developed by the Mojarra project. Source code for the Mojarra software may be obtained at https://javaserverfaces.dev.java.net/.

This product includes JZlib software, Copyright © 2000-2011 ymnk, JCraft,Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes Apache Lucene software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes Apache MINA software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes OData4J software, distributed under the Apache License version 2.0.

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes software developed by Addy Osmani, and distributed under the MIT license. Copyright © 2012 Addy Osmani.

This product includes software developed by Charles Davison, and distributed under the MIT license. Copyright © 2013 Charles Davison.

This product includes software developed by The Dojo Foundation, and distributed under the MIT license. Copyright © 2010-2011, The Dojo Foundation.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes Apache Ant software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes isc-dhcp software. Copyright © 2004-2013 by Internet Systems Consortium, Inc. ("ISC"); Copyright © 1995-2003 by Internet Software Consortium.

Permission to use, copy, modify, and/or 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" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

This product includes jQuery Sparklines software, developed by Gareth Watts, and distributed under the new BSD license.

This product includes jsdifflib software, developed by Chas Emerick, and distributed under the BSD license.

This product includes winston software, copyright © 2010, by Charlie Robbins.

This product includes Q software developed by Kristopher Michael Kowal, and distributed under the MIT license. Copyright © 2009-2013 Kristopher Michael Kowal.

This product includes SlickGrid software developed by Michael Liebman, and distributed under the MIT license.

This product includes JCraft Jsch software developed by Atsuhiko Yamanaka, copyright © 2002-2012 Atsuhiko Yamanaka, JCraft, Inc. All rights reserved.

This product includes DP_DateExtensions software developed by Jim Davis, Copyright © 1996-2004, The Depressed Press of Boston (depressedpres.com). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the DEPRESSED PRESS OF BOSTON (DEPRESSEDPRESS.COM) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All code not authored by the Depressed Press is attributed (where possible) to its rightful owners/authors, used with permission and should be assumed to be under copyright restrictions as well.

This product includes Angular software developed by Google, Inc., http://angularjs.org, copyright © 2010-2012 Google, Inc., and distributed under the MIT license.

This product includes node.js software, copyright © Joyent, Inc. and other Node contributors. All rights reserved.

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

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

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

This product includes the epoxy.js library for backbone, copyright © 2012-2013 Greg MacWilliam. (http://epoxyjs.org)

This product includes Javamail software, copyright ©1997-2013 Oracle and/or its affiliates, all rights reserved; and copyright © 2009-2013 Jason Mehrens, all rights reserved. This software is distributed under the GPLv2 license.

This product includes Leaflet software, copyright © 2010-2014, Vladimir Agafonkin, and copyright © 2010-2011, CloudMade; all rights reserved. This software is distributed under the BSD license.

This product includes underscore software, copyright © 2009-2014 Jeremy Ashkenas, DocumentCloud, and Investigative Reporters & Editors.

Chapter 1

Overview: BIG-IQ Security

About BIG-IQ Security and firewall management

BIG-IQ™ Security is a platform designed for the central management of security firewalls for multiple BIG-IP® systems, where firewall administrators have installed and provisioned the Advanced Firewall Manager™ (AFM™) module.

The BIG-IQ Security system provides:

- Device discovery with import of firewalls referenced by discovered devices
- Management of shared objects (address lists, port lists, rule lists, policies, and schedules)
- L3/L4 firewall policy support, including staged and enforced policies
- Firewall audit log used to record every firewall policy change and event
- Role-based access control
- Deploying configurations from snapshots and the ability to preview differences between snapshots
- Multi-user editing through a locking mechanism

Managing a firewall configuration includes discovering, importing, editing, and deploying changes to the firewall configuration, as well as consolidation of shared firewall objects (policies, rule lists, rules, address lists, port lists, and schedules). BIG-IQ Security provides a centralized management platform so you can perform all these tasks from a single location. Rather than log into each device to manage the security policy locally, it is more expedient to use one interface to manage many devices. Not only does this simplify logistics, but you can maintain a common set of firewall configuration objects and deploy a common set of policies, rule lists, and other shared objects to multiple, similar devices from a central interface.

Bringing a device under central management means that its configuration is stored in the BIG-IQ Security database, which is the authoritative source for all firewall configuration entities. This database is also known as the working configuration or working-configuration set.

Once a device is under central management, do not make changes locally (on the BIG-IP device) unless there is an exceptional need. If changes are made locally for any reason, reimport the device to reconcile those changes with the BIG-IQ Security working configuration set. Unless local changes are reconciled, the deployment process will overwrite any local changes.

In addition, BIG-IQ Security is aware of functionality in one BIG-IP system version but not in another. This means, for example, that it prohibits using policies on BIG-IP devices that do not have the software version required to support them.

About filtering

With filtering, you can rapidly narrow the search scope to more easily locate an entity within the GUI. Filtering reduces the set of data that is visible in the GUI.

Filtering is accessed through the Filter field. You can click any object in a panel to populate the Filter field and preview the filtering results.

Filtering the BIG-IQ Security GUI

Filter techniques can be important for troubleshooting firewalls.

1. To search in the GUI, type a text string in the Filter field and click **Apply**. (The string moves under the Filter field.)

Assume you have configured the shared object `schedule1`. If you type `schedule1` in the Filter field and click **Apply**, the following line appears under the field: `Related to Shared Objects:schedule1`

2. Clear the filter results by clicking the **x** to the right of the string.

About panels

BIG-IQ™ Security system panels expand to display details such as settings or properties for a particular device or shared object. These expanded panels include an arrow slanted at a 45-degree angle on the right side of their banners. If the arrow is slanted up, you can click it to expand the panel. If the arrow is slanted down, you can click it to collapse the panel. You can also click **Cancel** to close the expanded panel without saving edits or initiating actions.

You can reorder panels by dragging-and-dropping them to new locations. The customized order persists until you clear the browser's history, cache, and/or cookies.

The BIG-IQ Security interface consists of the following panels:

Devices
Displays the set of BIG-IP devices that BIG-IQ Security has discovered. From this panel, you can initiate device discovery and display device properties. You can also remove devices and reimport devices.

Firewalls
Displays discovered/imported network firewalls residing on discovered BIG-IP devices.

Policies
Displays the policies available. Rules for each policy type (staged or enforced) and each context form their own list, and are processed both in the context hierarchy and in the order within each context list.

Rule Lists
Displays discovered/imported rule lists that you can share among multiple firewalls. From this panel, you can display and edit rule list details.

Snapshots
Displays a list of imported snapshots. From this panel, you can back up, restore, and deploy the BIG-IQ working configuration to a specific configuration state or deploy a specific set of working configuration edits back to a BIG-IP device.

Shared Objects
Displays the address lists, port lists, and schedules that you can share among multiple firewalls. From this panel, you can display and edit object details.

Deployment
Enables deployment, to a target BIG-IP device, of any change that occurred to any configuration object. After you have completed edits to a firewall policy, you can create a deployment task to push configuration object changes out to BIG-IP devices.

Expanding panels

Hover in the panel header and click the + icon to expand the panels.

For the Shared Objects panel, hover over the header for each object type (address lists, port lists, or schedules) and click the + icon.

Reordering panels

To reorder panels, drag-and-drop them to the new locations of your choice.

The customized order persists until you clear the browser history/cache/cookies.

About tooltips

The BIG-IQ™ Security system uses tooltips to provide additional information. That additional information varies according to the context.

Tooltips show the name of the shared object when you hover over the name in a list. For example, if you hover over the name of an address list in the Shared Objects panel, you see the full, expanded name of the shared object.

If you hover over that same object from inside a rule, you see the data in the shared object. For an address list, for example, you see a listing of the addresses, address ranges, and/or nested address lists in the selected address list.

About browser resolution

F5® recommends a minimum screen resolution of 1280 x 1024 to properly display and use the panels efficiently.

It is possible to shrink the browser screen so that GUI elements (panels, scroll bars, icons) no longer appear in the visible screen. Should this occur, use the browser's zoom-out function to shrink the panels and controls.

About user preferences

As a firewall policy editor, you can customize the BIG-IQ™ Security GUI to minimize the information displayed and to simplify routine editing sessions. The first customization concerns the set of panels displayed for a particular user. For example, if you never perform deployments, you might decide to hide the Deployments blade.

Note: *This customization does not create an access issue. Users still have access to the resources required by their roles; they just choose not to display them.*

The second customization concerns the set of firewall types shown in panels. If you do not use certain types, you might decide to hide them to avoid confusion and to minimize scrolling in the panel.

User preference settings persist across user sessions. If the user logs out, they see the same settings when logging back in.

By default, BIG-IQ Security replicates user preferences through BIG-IQ high-availability (HA).

Setting user preferences

1. Log in to the BIG-IQ™ Security system.

2. At the top-right of the screen in the black banner, hover over the **admin** icon.
3. When **User settings** appears, click it to display the Settings popup screen.
4. Edit the check box options as required for your role.

Option	Description
Show Panels	Select or clear the check boxes as required. By default, the GUI displays all panels.
Show Firewall Types	Select or clear the check boxes as required. By default, the GUI displays all firewall contexts in the Firewall Contexts panel.

5. Click **Save** to save your preferences. Click **Close** to close the popup screen without saving your selections.

Your preferences are now in effect and persist across user sessions. If you log out, you will see the same settings when you log back in.

About roles

Different users have different responsibilities. As a Firewall manager, you need a way to limit user privileges based on those responsibilities.

To assist you, the BIG-IQ™ Security system is created with the following default set of roles.

Administrator
This role is responsible for overall management of the platform. Users with this role can add individual users, install updates, activate licenses, and configure HA and networks.

Firewall_Deploy
This role permits viewing and deploying for all firewall configuration objects for all firewall devices under management. Users with this role cannot edit configuration objects, discover devices, or reimport devices or otherwise make changes to the working configuration of the BIG-IQ system. This role cannot create, edit, or delete snapshots. Also, this role does not have access to System/Overview or Networking.

Firewall_Edit
With this role, the user can view and modify all configuration objects for all firewall devices under management, including the ability to create, modify, or delete all shared and firewall-specific objects. Users with only this role cannot deploy configuration changes to remote devices under management. Also, this role does not have access to System/Overview or Networking.

Firewall_View
With this role, the user can view all configuration objects and tasks for all firewall devices under management across all devices. Users with this role cannot edit objects and cannot initiate a discovery or deployment task.

Firewall_Manager
This role encompasses the roles of Firewall_View, Firewall_Edit, and Firewall_Deploy. A user logging in with this role bypasses the SYSTEM panel and is logged directly into BIG-IQ Security.

Security_Manager
This role combines the privileges of Firewall_View, Firewall_Edit, and Firewall_Deploy. A user logging in with this role is logged directly into BIG-IQ Security. A user logging in with this role can also access BIG-IQ ASM.

Roles persist and are available after a BIG-IQ system failover.

You can associate multiple roles with a given user; for example, you can grant a user the edit (Firewall_Edit) and the deploy (Firewall_Deploy) roles.

About users

The BIG-IQ™ Security system is created with the following users.

admin
This user can create firewall managers and assign roles to them. This user cannot access the command shell or the system console.

root
This user can access the system console.

Users persist and are available after a BIG-IQ system failover.

Creating users

It is the Firewall manager's responsibility to ensure the creation of the right set of users and the association of those users with the right roles (sets of privileges). By managing user roles, the Firewall manager places controls on specific functions (view, edit, and deploy).

Users and roles persist and are available after a BIG-IQ™ system failover.

1. Log in with administrator credentials.
2. At the top of the screen in the black banner, hover over **System** and click **Users**.
3. Hover in the Users banner and click the + icon.
4. Edit the fields as required.

Option	Description
User name	Enter the user's login name.
Full Name	Enter the user's actual name. This field can contain a combination of symbols, letters (upper and lowercase), numbers and spaces.
Password	Enter the password for this user.
Confirm Password	Retype the password.

5. Click **Add** to save your edits and create the user. Click **Cancel** to close the panel without saving your entries.

You can now associate this user with a specific role (set of privileges).

Associating users with roles

To control what users are able to accomplish, associate roles (sets of privileges) with particular users.

1. Log in with administrator credentials.
2. At the top of the screen in the black banner, hover over **System** and click **Users**.

3. In the Users panel, click the user that you want to associate with a role and drag-and-drop the user onto the role (Roles panel). Conversely, you can also drag-and-drop the role onto the user.

The user now has the necessary privileges. To confirm, click the **gear** icon for the role and view the User Role Properties screen. To the right of **Active Users**, view the list of users associated with the role. Or, click the **gear** icon for the user and to the right of **User Roles**, view the list of roles associated with the user. Or, select the user and the BIG-IQ™ Security system highlights the roles associated with that user.

Disassociating users from roles

To disable a user's ability to perform a given function, disassociate roles (sets of privileges) from that user.

1. Log in with administrator credentials.
2. At the top of the screen in the black banner, hover over **System** and click **Users**.
3. In the Roles panel, hover over the role that contains the user you want to disassociate and click the **gear** icon.
4. To the right of **Active Users**, view the list of users associated with the role.
5. Click the **x** icon next to the user that you want to disassociate from the role.
6. Click **Save**.

The user is now disassociated from the role and no longer has the privileges associated with the role.

About multi-user editing

With the BIG-IQ™ Security system, multiple firewall editors can edit shared firewall policy objects simultaneously. This is accomplished through a locking mechanism that avoids conflicts and merges. Initially, the user interface presents all firewall configuration objects as read-only. When a firewall editor initiates an editing session, he/she locks the object. Once an object is locked, no one can modify or delete that object except the holder of the lock or users with privileges sufficient to break the lock (admin, Firewall_Manager, or Security_Manager).

BIG-IQ Security uses a single repository to hold firewall policies. With this single-copy design, multiple editors share the editing task through a locking mechanism. The system saves each editorial change.

Each firewall editor has their own copy of a firewall policy (a point-in-time snapshot of the policy managed by BIG-IQ across all devices) and can make changes. When done, an editor can push the changes to the preferred state as one, complete set of changes. Then, a firewall administrator can review a policy change as a single entity before committing it.

For example:

1. If a firewall editor needs to edit Portlist_1, AddressList_2, and Rulelist_5, the editor locks those objects.
2. When the edit pass is complete, the editor saves the object, which clears the lock.

If an editor wants to edit an object that is already locked, the system informs the editor that the object is locked and provides a way to clear the lock if the editor has sufficient privileges.

When the lock is cleared, the next firewall editor receives the latest version of the object and any referenced shared objects. Thus, merges and conflicts are avoided.

Deleting an object automatically clears all locks associated with it.

BIG-IQ Security supports:

- Multiple, independent locks.
- Locking/unlocking at the firewall level. Locking a firewall locks all shared objects referenced by all of the device's firewalls/rules.
- Locking/unlocking on an object-by-object basis where the object is defined as a shared object or a firewall.

Locking configuration objects for editing

Before editing a configuration object, you must establish a lock on that object.

Note: *If you have editing privileges, you can lock firewalls, policies, rule lists, address lists, port lists, and schedules.*

---

1. Navigate to the object that you want to edit.
2. Hover in the header for that object, and click the **gear** icon to expand the panel and display object details.

   If an Edit button is visible, you can edit the object. If the object is already locked, a lock header is visible and there is no Edit button available.

   The lock header provides a date and time stamp of the lock.
3. If an Edit button is visible, click it to lock the object for editing.
   A lock appears on the object and a lock header is displayed.
4. Edit as appropriate.
5. When finished, click **Save**. If you navigate away from the panel without saving, the GUI displays a dialog box asking if you want to save changes. Click **Yes** or **No** or click **Cancel** to dismiss the dialog box and return to the location where you were editing.

The lock on the object is released. If you click **Cancel**, the lock is also released but any edits will be discarded.

Viewing locks on all configuration objects

BIG-IQ™ Security provides a way to view all locked configuration objects from a single popup screen.

1. Examine all panels to locate locked configuration objects.
2. Navigate to a locked object.
3. Hover over the lock icon.

   A tooltip is displayed that shows the owner of the lock and the date and time the lock was created, as well as a link labeled **View All**.
4. Click **View All**.

The Locks popup screen is displayed showing type, name, user, date and time, and a description for all locked objects.

Clearing locks on configuration objects

The owner of a lock can always clear that lock. Other roles (Administrator, Firewall_Manager, Security_Manager) also carry sufficient privileges to clear locks held by any user.

1. Examine all panels to locate locked configuration objects.
2. Search for the object whose lock you want to clear.

3. Hover over the lock icon to the left of the object's name in the panel.

   A tooltip is displayed that shows the owner of the lock and the date and time the lock was created, as well as a link labeled **View All**. If your role carries sufficient privileges, you will also see a link labeled **Unlock**.

4. In the tooltip, click **Unlock**.
5. In the confirmation dialog box, click **Unlock**.

The lock is cleared.

Clearing multiple locks or all locks

BIG-IQ™ Security provides a way to clear multiple locks or all locks from a single popup screen, providing that the user carries sufficient privileges.

1. Examine all panels to locate locked configuration objects.
2. Hover over the lock icon to the left of any locked object in any panel.

   A tooltip is displayed that shows the owner of the lock and the date and time the lock was created as well as a link labeled **View All**. If your role carries sufficient privileges, you will also see a link labeled **Unlock**.

3. In the tooltip, click **Unlock**.
4. In the popup screen that appears, select or clear check boxes as appropriate. Select the check box at the top to clear all locks.
5. Click **Unlock**.
6. In the confirmation dialog box, click **Unlock**.

The locks are cleared.

Configuring BIG-IP devices to accept traffic

If you use the BIG-IP® device's self IP address to discover it, you must configure that device to accept traffic from a BIG-IQ™ Security system. Specifically, if the BIG-IP device has the Virtual Server & Self IP Contexts option set to Reject or Drop, the BIG-IP device will not accept traffic from the BIG-IQ system. Use the following procedure to set this option to Accept.

Alternately, you can add a rule to handle traffic between the self IP addresses of the BIG-IQ Security system and the self IP addresses of the specific BIG-IP device being discovered. In this scenario, you can leave the Virtual Server & Self IP Contexts option set to Reject or Drop.

In this case, ensure the following ports remain open:

- 22 (SSH, TCP protocol)
- 443 (HTTPS, TCP protocol)
- 4353 (iQuery, TCP protocol)

Note: *Whichever scenario you choose, configure the BIG-IP device to allow traffic to/from the self IP addresses of both BIG-IQ nodes in a BIG-IQ HA pair.*

---

1. On the BIG-IP device, navigate to **Security** > **Options** > **Network Firewall**.
2. From the **Virtual Server & Self IP Contexts** drop-down list, select **Accept**.

3. Click **Update**.

Packets with BIG-IQ Security as the source are then able to pass through the BIG-IP firewall and traverse the system.

About BIG-IQ active-standby, high-availability configurations

To ensure that you always have access to the BIG-IP® devices under BIG-IQ™ management, install two BIG-IQ systems in an active-standby, high-availability (HA) configuration. Configuring a high-availability pair is optional. However, if the active BIG-IQ system in the high-availability configuration fails, the standby peer will become active, enabling you to continue to manage devices.

BIG-IQ Network Security performs asynchronous replication, which means that data is replicated continuously, asynchronously, as changes are made or commands are run on the active system.

Terminology is important in understanding the status of the HA relationship. The following table lists and defines some important terms displayed in the top left of the application banner.

Primary
Initiate the pairing from the primary node. This is the node that wins if a conflict occurs. If both nodes are up and communicating, this is the node that determines which node is active.

Secondary
Any other node. Currently, BIG-IQ Network Security supports a 2-node pairing.

Active
Node that is running commands. Normal operation is indicated by Active (Primary) at the top of the interface.

Standby
Carries a yellow status bar indicating its standby status and instructing the user to perform all module-related activity on the active node.

If you see the status indications Active (Secondary) and Standby (Primary), you have failed over to the node that is not the primary.

In the unlikely event of network segmentation, both systems may report that they are active.

The following table lists the phases encountered while the cluster is forming.

State	Status	Description (Phase)
UNKNOWN	Collecting	Initial discovery and credential exchange.
SYNCHRONIZING	Active	Compatibility validation complete, synchronizing configuration information and establishing primary/secondary relationship. The system copies the configuration of the primary node to the secondary node (or, peer). The secondary is restarted using that configuration. If the peer encounters errors downloading the configuration from the primary/active node, you must delete the HA pair, investigate the causes of the error(s), and attempt to form the pair again.

State	Status	Description (Phase)
		.
DOWN	Active	It is normal for this state to appear. After a brief period, the state will update itself; no user action is necessary. After synchronization of the initial configuration data, the secondary device's REST services will be restarted to accept the new configuration and complete the configuration synchronization.
STANDBY	Active	Pairing completed. The standby system will now display a yellow banner across the top of its UI indicating that changes to individual modules should take place on the active node. Changes to system-level settings will still be performed on each individual device.

Configuring BIG-IQ high-availability systems

To configure BIG-IQ™ systems for high-availability, you must have two licensed BIG-IQ systems, installed with the required system components. For the high-availability pair to synchronize properly, each must be running the same BIG-IQ version, and the clocks on each system must be synchronized within 60 seconds and remain synchronized. Prior to establishing the pair, examine the NTP settings at the BIG-IQ system level and the current system time value.

Note: *Perform the following procedure on the active BIG-IQ system.*

1. Log in to the BIG-IQ system, using administrator credentials.
2. In the black banner, hover over **System** and then click **Overview**.
3. Select the High Availability tab.
4. Edit the following fields:

Option	Description
Peer IP Address	For the peer BIG-IQ system, enter the self IP address, also known as the HA Communication Address. To obtain this address, navigate to **System** > **Networking** on the peer device.
User Name	Enter the administrative user name for the peer.
Password	Enter the administrative password for the peer.

5. To save the configuration, click **Save**.
6. Observe the phases encountered while the cluster is forming. One node discovers the other and exchanges credentials with it. Compatibility validation is completed and configuration information is synchronized. The configuration of the device being paired is overwritten by the active system. The configurations do not merge.

   If discovery fails, a delete button is displayed. Verify the information you entered. If you have entered incorrect information, click **Delete** to remove it. Then, repeat the process using correct information.

The active BIG-IQ system discovers its peer and displays status. The standby system displays a warning banner at the top of the application, informing the user to not attempt editing data on it.

Configuring a BIG-IQ high-availability communication network

On BIG-IQ™ systems, HA traffic travels over an HA communication network. It is recommended that an HA communication network be created to handle this traffic and to keep it separate from discovery traffic.

Perform these steps on both peers in the HA pair.

1. Log in to the BIG-IQ system, using administrator credentials.
2. In the black banner, hover over **System** and then click **Networking**.
3. From the **VLAN** panel, hover over the header and select +.
4. Edit the following fields:

Option	Description
Name	For
Description	Enter an optional description.
Interface	From the drop-down, select **1.2**.

5. Click **Add**.
6. From the **Self IP Addresses** panel, hover over the header and click +.
7. Edit the following fields:

Option	Description
Name	Use the self IP address as the name. Format: nn.nn.n.nnn.
Address	Enter the IP address to be used. Include the subnet mask. Format: nn.nn.n.nnn/nn.
VLAN	From the drop-down, select **1.2**.
Description	Enter an optional description.

8. Click **Add**.
9. Return to the Self IP Properties panel and select the **Use for HA Peer Communication** check box .
10. Click **Save**.

Splitting a BIG-IQ high-availability pair

To change or reconfigure peers in a BIG-IQ™ high-availability pair, you must first delete the HA relationship.

1. Log in to the active BIG-IQ system, using administrator credentials.
2. In the black banner, hover over **System** and then click **Overview**.
3. At left, click **High Availability**.
4. Click **Delete**.

Caution: *After the pair is split, each BIG-IQ system operates as a standalone and, initially, operates off the same configuration. Each configuration can be updated independently. Changes made on one system do not propagate to the other.*

Forcing active BIG-IQ high-availability systems to standby

If both BIG-IQ™ systems in an active-standby, high-availability pair become active, a warning message is displayed at the top left of the application header. This can occur in the unlikely event of network segmentation or a communication failure. If this scenario occurs, move one system back into standby mode.

Note: *Configuration replication does not occur while both systems are active.*

1. Log in to one BIG-IQ system, using administrator credentials.
2. In the black banner, hover over **System** and then click **Overview**.
3. At left, click **High Availability**.
4. Click **Force Standby**.
5. To save the change, click **Save**.

This BIG-IQ system is forced into standby mode.

About BIG-IQ Network Security automatic failback

In a BIG-IQ™ Network Security automatic failback scenario, the active node goes down and the standby node takes over. When the active node comes back up, it takes over automatically.

This process includes a failover/recovery trigger timer, which is the time it takes a peer to understand that the other peer in the pair has failed and to respond appropriately.

Chapter 2

Managing Devices

About device discovery

The process of importing a firewall device's configuration or designating a firewall device for central management by BIG-IQ™ Security is called *discovery*.

After discovery, BIG-IQ Security provides a way to view device properties and to perform device-specific and firewall-specific actions through a centralized management platform.

BIG-IQ Security lists devices under management in the Devices panel.

Before discovering devices, you must install specific components required by the BIG-IQ system on each BIG-IP® device you want to manage. Installing these components results in a REST framework that supports the required Java-based management services.

Discovering devices

Before discovering one or more BIG-IP® devices, ensure the required BIG-IQ™ components are installed on those devices.

Once a device is under central management, the device's configuration is stored in the BIG-IQ Security database, which is the authoritative source for all configuration entities (shared objects). After that point, do not manage the firewall device locally unless there is an exceptional need.

During discovery, **Remove Device** appears in the dialog box after the task has identified the device and started importing the firewall configuration. If you click **Remove Device**, the import is canceled and management authority over the device is rescinded. The device is removed.

1. To begin the discovery process, navigate to the Devices panel.
   At first login, this panel is empty because there are no discovered devices.
2. Hover over the Devices header and click the + icon to display the property fields for a new device.
3. Edit the property fields as required.

Option	Description
Device Address	Enter the internal self IP for the BIG-IP® device. ***Note:*** *Each managed device must be configured with a communication route from its internal self IP or management IP address to a BIG-IQ system internal self IP address on a configured BIG-IP VLAN. Otherwise, discovery will fail. F5 recommends that you use a self IP address (on the BIG-IP device) in order to gain access to additional functionality that is not provided through the management port.*
Cluster Name	Enter a name for the cluster. Optional, but highly recommended.
User Name	Enter the user's login name. For example: fw_admin.
Password	Enter the password for this user.
Snapshot	Ensure that this check box is selected (the default) to take a snapshot of the configuration on the BIG-IP device before importing.

Option	Description
Auto Update Framework	Select this check box to update the REST framework installed on the BIG-IP device. It is required that certain BIG-IQ system components be installed and kept up-to-date on all BIG-IP devices brought under central management. These components provide a REST framework on the BIG-IP devices that support the required Java-based management services. To ensure the framework is up-to-date, select this check box.

4. Click **Add**.

After discovery, the BIG-IP device is listed in the Devices panel by its FQDN and internal self IP or management IP address. Also, the system lists the snapshot of the working configuration taken during import in the Snapshots panel. The system imports the firewall policy for this device and makes it available for configuration management.

About declaring management authority

The process of bringing a device under central management is known as *declaring management authority (DMA)*. The firewall administrator initiates DMA through device discovery and import (or reimport).

The DMA process is modal. Once the process starts, you are blocked from performing any other tasks or interacting with BIG-IQ™ Security in any way until the process is complete or canceled. Before starting a discovery or reimport process, it is important to understand how you will resolve any conflicts that arise.

Note: *In this scenario, a conflict is defined as two shared objects in the same partition having the same name, but containing different data.*

About conflict resolution

A conflict is found when two shared objects in the same partition have the same name but different data. Conflicts prevent the discovery process from running to completion.

Note: *It is the responsibility of the Firewall manager to know how to resolve conflicts between shared objects and to deploy the resolution. If you encounter conflicts during discovery, import, or reimport, you must resolve those conflicts before you can interact further with BIG-IQ™ Security.*

If conflicts are found, BIG-IQ Security displays the Resolve Conflicts dialog box, which lists all conflicts found, displays detailed differences for conflicting shared objects, and provides for conflict resolution.

Although conflict resolution often results in changes to either the BIG-IP® configuration or the BIG-IQ configuration, no changes are applied until they are deployed. You can deploy changes when a deployment task displays a status of READY TO DEPLOY.

Resolving conflicts

After reimporting a BIG-IP® device, use the Resolve Conflicts dialog box to view the differences between configurations and to resolve conflicts.

The Resolve Conflicts dialog box also provides a **Cancel Task** button. If you click **Cancel Task**, the reimport is canceled. Management authority over the device is not rescinded, and the device is not removed.

1. To begin the reimport process, navigate to the Devices panel.
2. Hover in the header for the device you want to reimport and when the **gear** icon appears, click it to display the expanded panel, containing device properties and actions.

   You cannot change any of the properties displayed on this screen, except the Snapshot check box, which is optional. To ensure that a snapshot is taken prior to import, leave the check box selected.
3. In the expanded panel, click **Reimport**.
4. When the Resolve Conflicts dialog box appears, conflicting shared objects are highlighted in blue in the upper half of the dialog box. Click the shared object to view details in the lower half of the dialog box. The object's configuration on the BIG-IP device is displayed on the left and the object's configuration on BIG-IQ™ Security is displayed on the right.

   A gray area indicates that an object has been removed. Yellow indicates that a line has changed, and green indicates that an object has been added or modified.
5. Examine differences. From the Action dropdown, select one of the following for each object in conflict:

Option	Description
No Action	Take no action. This option does not resolve the conflict and prevents the discovery process from completing. If you are not ready to resolve the conflicts but need to perform other firewall management tasks, cancel the discovery process and return to it later. The device is not brought under management.
Keep Both	Retain both objects as configured. BIG-IQ Security changes the name on the incoming object to resolve the conflict. Then, it updates rules with the new object name. The new object name includes the device name so it can easily be found.
Keep BIG-IP Version	Keep the object as configured on the BIG-IP device and overwrite the object as configured in the central BIG-IQ Security database.
Keep BIG-IQ Version	Keep the object as configured on BIG-IQ Security and overwrite the object as configured on the BIG-IP device.

6. Or, from the Action dropdown to the right of *Apply this action to all conflicts:*, select an action to resolve all existing conflicts.

After conflict resolution, the device's configuration is refreshed and synchronized with the configuration stored in BIG-IQ Security.

Displaying device properties

1. To display properties for an individual device, hover over the header for that device (in the Devices panel).
2. Click the **gear** icon to display and expand the panel containing device properties.

Device properties

Device properties are displayed for informational purposes and are read-only, except the Snapshot and Auto Update Framework check boxes.

Device Property	Description
Host Name	Displays the fully-qualified domain name (FQDN), identified at discovery time.
Cluster Name	Displays the BIG-IP® device cluster name, provided by the user at discovery time.
IP Address	Displays the IP address of the BIG-IP device, used for communication between it and the BIG-IQ Security system.
Product	Identifies the product.
Version	Identifies the version and hotfix level of the device under management.
Snapshot	Check box used to invoke a snapshot prior to reimporting the BIG-IP device's working configuration.
Auto Update Framework	Check box used to update the REST framework on the BIG-IP device.

About the device inventory

From the Devices panel, you can display an inventory of device properties and accompanying details for all devices under BIG-IQ™ Security central management. For further use, you can export this inventory to a CSV file.

Reimporting devices

Once configurations are in sync between BIG-IP® devices and the BIG-IQ™ Security system, there is seldom a need to reimport a BIG-IP device.

Some possible reasons to reimport include:

- Additions, deletions, or changes made to self IPs or virtual servers on the BIG-IP device.
- Changes to policies, firewall rules, or shared objects made locally on the BIG-IP device.
- Updates made to the BIG-IP device's software that need to be recognized by BIG-IQ™ Security.

If any of these reasons occur, you must reimport to reconcile any changes with the configuration maintained on BIG-IQ Security. If you do not reconcile changes, a subsequent deployment process will overwrite any changes made locally.

The reimport process is modal. Once reimport starts, the process blocks you from performing any other tasks or interacting with BIG-IQ Security in any way until the process completes or is canceled.

During reimport, a **Remove Device** button appears in the dialog box after the task has identified the device and started importing the firewall configuration. If you click **Remove Device**, the reimport is canceled, management authority over the device is rescinded, and the device is removed.

1. To begin the reimport process, navigate to the Devices panel.

2. Hover in the header for the device you want to reimport and when the **gear** icon appears, click it to display the expanded panel, containing device properties and actions.

   You cannot change any of the properties displayed on this screen, except the Snapshot check box, which is optional. To ensure that a snapshot is taken prior to import, leave the check box selected.

3. In the expanded panel, click **Reimport**.

After reimport, the firewall policy for the selected device is refreshed and synchronized with the configuration stored in BIG-IQ Security.

Monitoring device health and performance

Before you can view device properties and health, you must discover at least one device.

With the BIG-IQ™ system, you can easily assess the health and performance of your network.

1. Navigate to the Devices panel.
2. Hover over the banner of the device you want to monitor and when the **gear** icon appears, click it to expand the panel.
3. In the expanded panel, view health data under device properties.

About device configuration sets

Possible configuration sets for a firewall device centrally managed by the BIG-IQ™ Security system include:

Current configuration set
The configuration of the BIG-IQ® device as discovered by BIG-IP Security. The current configuration is updated during a reimport and before calculating differences during the deployment process. After deployment (and after the resolution of any conflicting shared objects), BIG-IQ Security overwrites the BIG-IP current configuration (if the option to USE BIG-IQ is chosen).

Working configuration set
The configuration as maintained by the BIG-IQ Security system. Initially, the working configuration is created when the firewall manager elects to manage the device from BIG-IQ Security (DMA). It is the configuration that is edited on BIG-IQ Security and deployed back to BIG-IP devices.

Device discovery states

The following table displays states that occur during the discovery process.

NEW
SUBTASK_INIT
LOAD_LICENSE
QUERY_LICENSE

IDENTIFY_LICENSE
PENDING_IDENTIFIED_DEVICE
IDENTIFY_DEVICE_COMPLETE
DELAY_REFRESH_COMPLETE
REFRESH_DEVICE_COMPLETE
QUERY_RUNNING_CONFIG
RUNNING_IMPORT_COMPLETE
RUNNING_IMPORT_RULELISTS_COMPLETE
RUNNING_IMPORT_FIREWALLS_COMPLETE
WORKING_IMPORT_COMPLETE
WORKING_IMPORT_RULELISTS_COMPLETE
WORKING_IMPORT_FIREWALLS_COMPLETE
WORKING_IMPORT_COMPLETE
WORKING_IMPORT_RULELISTS_COMPLETE
WORKING_IMPORT_FIREWALLS_COMPLETE
PENDING_CONFLICTS
PENDING_CANCEL
CONFLICT_RESOLUTION_COMPLETE
IMPORT_ADDRESS_LISTS_COMPLETE
IMPORT_PORT_LISTS_COMPLETE
IMPORT_SCHEDULES_LISTS_COMPLETE
UPDATING_RULES_COMPLETE
REFRESH_RULE_LISTS_COMPLETE
IMPORT_RULE_LISTS_COMPLETE
IMPORT_RULES_COMPLETE
UPDATING_FIREWALLS_COMPLETE
IMPORT_FIREWALLS_COMPLETE
COMPLETE
FAILED
FAILED_MAX_EXCEEDED

Chapter 3

Managing Firewall Contexts

About managing firewalls in BIG-IQ Security

Firewalls provide policy-based access control to and from address and port pairs, inside and outside the network. Using a combination of contexts, a firewall can apply rules in a number of different ways, including at a global level, per virtual server, per route domain, and even for the management port or a self IP address.

IN BIG-IQ® Security, the Firewall Contexts panel displays network firewalls imported from discovered BIG-IP® devices.

Each row in the panel contains the firewall name, its type, and its parent device on the partition it resides in. Note that an *administrative partition* is a part of the BIG-IP configuration that is accessible only to a particular group of administrators. The default partition for all BIG-IP configurations, /Common, is accessible to all administrators. A sufficiently-privileged administrator can make additional partitions. Each partition corresponds to a folder (with the same name) to hold its configuration objects.

You can edit inline rules from the Firewall Contexts panel. You can edit all other firewall shared objects only from within the object's panel. For example, you can edit rule lists, including the reordering of rules, only from the Rule Lists panel.

To get help about an individual firewall, click that firewall's row and then click the help icon. For details on a specific firewall, hover over the row for that firewall and when the **gear** icon appears, click it.

Firewall context types

Consult the following table for information about the firewall context types.

Firewall context type	Description
Global (global)	On a BIG-IP® device, packets are processed by the global firewall before they get to the route domain, virtual server, or self IP firewalls. The global firewall collects rules that apply to all traffic that traverses the firewall; global rules are checked first.
Route domain (rd)	There can be more than one configured route domain firewall on a device; each listed by its ID. The default route domain firewall on the BIG-IP device is Route Domain 0. Even if you have not configured a route domain, you can apply route domain rules to Route Domain 0. Packets are processed by the route domain firewall after the global firewall and before they are processed by the associated virtual server or self IP firewalls. The route domain firewall collects rules that apply to a specific route domain defined on the server.
Virtual servers (vip)	The virtual server firewall collects rules that apply to the selected existing virtual server only. Packets that pass through the virtual server are assessed by this firewall. Virtual server rules are checked after route domain rules.
Self IP (self-ip)	The self IP firewall consists of an IP packet filter configured on the self IP address (internal or external). Any IP packet that passes through the self IP is processed by this firewall. The self IP firewall collects firewall rules that apply to the self IP address on the BIG-IP device. Self IP rules are checked after route domain rules.
Management (mgmt)	Labeled Management Port on a BIG-IP device. The Management firewall (single firewall per management interface) consists of an IP packet filter configured on the management port and collects firewall rules that apply to the management port. BIG-IQ™ Security does not support configuring rule lists on policies on the management firewall.

Firewall properties

The Properties tab displays the properties for the selected firewall. All fields are for information purposes only and cannot be edited with the exception of the (optional) description.

Property	Description
Name	Displays the name as shown in the GUI: global for the global firewall; management-ip for the management IP firewall; 0 for route domain; IP address for self-ip; name for vip.
Description	Displays an (optional) description for the firewall.
Partition	Usually displays /Common. An *administrative partition* is a part of the BIG-IP configuration that is accessible only to a particular group of administrators. The default partition for all BIG-IP configurations, /Common, is accessible to all administrators. A sufficiently-privileged administrator can make additional partitions. Each partition corresponds to a folder (with the same name) to hold its configuration objects.
Type	Displays one of the following: global (global); route-domain (rd); virtual server (vip); self-ip (self-ip); management-ip (mgmt).
Route Domain Only: Route Domain ID	Displays a number that identifies the route domain.
Virtual server (VIP), self IP, and Management Only: IP Address	Informational, read-only field displaying the IP address retrieved (if available) during DMA.
Device	Displays the name of the BIG-IP® device where the firewall resides.

About the Firewall Context panel tabs

The Firewall Contexts panel expands to display the following tabs:

- Properties. Displays firewall properties for informational purposes and are read-only, except the (optional) description.
- Enforced. Displays policies or rules/rule lists whose actions are executed.
- Staged. Displays policies whose actions are not live and are not executed.

You can assign to a firewall an enforced policy or a set of explicitly-defined rules and rule lists. The firewall cannot have both in force at the same time. However, you can configure simultaneously on the same firewall both staged policies and enforced inline rules and rule lists.

Adding an enforced policy

The Enforced tab (Firewall Contexts panel) displays policies or rules/rule lists whose actions (accept, accept decisively, drop, reject) are executed. You are restricted to a single, enforced policy on any specific firewall.

If you have an enforced policy on a firewall, you cannot also have inline rules and rule lists on that same firewall.

The Enforced tab displays policies if policies are supported for the selected firewall.

Note: *Policies can be enforced in one context and staged in another.*

---

1. From the expanded Policy panel Enforced tab, click **Edit** to establish a lock. If necessary, review *Locking configuration objects for editing*.
2. In the Enforced tab, add a policy by dragging-and-dropping a policy from the Policies panel or click the **Add Policy** link to display a list of policies.
3. In the popup screen, select the policy you want to enforce and click **Add**.

   If the firewall has inline rules already configured, you are notified that adding a policy will result in the removal of all existing rules and rule lists
4. In the Enforced tab, create a rule by clicking **Create Rule** and populating the fields as appropriate or add a rule list by clicking **Add Rule List**. If you click **Add Rule List**, select a rule list from the Rule Lists popup screen and then click **Add**.

   A new row appears in the table. This row contains a template, including defaults, for the new rule.
5. Edit the fields as appropriate.

   Click **Tab** to advance from field to field.

   You can also add rules by right-clicking in the last rule in the table and selecting **Add rule before** or **Add rule after**. If you right-click after the bottom row in the Rules table, you can select the option **Add rule**. You can then reorder rules by dragging-and-dropping them until they are in the correct execution order.
6. To add a rule list, click **Add Rule List**.
7. In the popup screen that appears, select the name of the rule list that you want to add and click **Add**.
8. When finished, click **Save**.
9. To clear a lock, click the **Unlock** link.
10. To remove policies, click the **X** icon following the policy name.

Adding a staged policy

The Staged tab (Firewalls Contexts panel) displays policies whose actions are not live; actions (accept, accept decisively, drop, reject) are not executed. Rather, actions are logged. Thus, you can stage a policy first and examine the logs to determine how the policy has affected traffic. Then, you can determine the timing for turning the policy from staged to enforced.

Rule and rule lists are not allowed on staged policies.

Note: *A policy can be staged in one context and enforced in another.*

---

1. From the expanded Policy panel Staged tab, click **Edit** to establish a lock. If necessary, review *Locking configuration objects for editing*.
2. In the Staged tab, add a policy by dragging-and-dropping a policy from the Policies panel or click the **Add Policy** link to display a list of policies.
3. In the popup, select the policy you want to stage and click **Add**.
4. When finished, click **Save**.
5. To remove policies, click the **x** icon following the policy name.

About BIG-IP system firewall contexts

A firewall context is the category of object to which a rule applies. In this case, category refers to Global, Route Domain, Virtual Server, Self IP, or Management.

It is possible to have multiple layers of firewalls on a single BIG-IP® device. These layers constitute the firewall hierarchy. Within the firewall hierarchy, rules progress from Global, to Route Domain, and then to either Virtual Server or Self IP. Management port rules are processed separately and are not processed as part of the hierarchy. Rules can be viewed and reorganized separately within each context.

If a packet matches a firewall rule within a given context, that action is applied to the packet, and the packet then moves to the next context for further processing. If the packet is accepted, it travels on to the next context. If the packet is accepted decisively, it goes directly to its destination. If the packet is dropped or rejected, all processing stops for that packet; it travels no further.

On each firewall, you can have rules, rule lists, or policies that are enforced or staged. Rules, rule lists, or policies are processed in order within their context and within the context hierarchy. Rules for the Management Port are processed separately and not as part of the context hierarchy.

About global firewalls

A *global firewall* is an IP packet filter that resides on a global firewall on a BIG-IP® device. Except for packets traveling to the management firewall, it is the first firewall that an IP packet encounters. Any packet reaching a BIG-IP device must pass through the global firewall first.

When you create firewall rules, rule lists, or policies, you can select one of several contexts. Global is one of the contexts you can select. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

About route domain firewalls

A *route domain firewall* is an IP packet filter that resides on a route domain firewall on a BIG-IP® device.

A *route domain* is a BIG-IP system object that represents a particular network configuration. After creating a route domain, you can associate various BIG-IP system objects with the domain: unique VLANs, routing table entries such as a default gateway and static routes, self IP addresses, virtual servers, pool members, and firewalls.

When a route domain firewall is configured to apply to one route domain it means that any IP packet that passes through the route domain is assessed and possibly filtered out by the configured firewall.

When you create firewall rules, rule lists, or policies, you can select one of several contexts. Route domain is one of the contexts you can select. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

Route domain rules apply to a specific route domain configured on the server. Route domain rules are checked after global rules. Even if you have not configured a route domain, you can apply route domain rules to `Route Domain 0`, which is effectively the same as the global rule context.

Route domain rules are collected in the Route Domain context. Route domain rules apply to a specific route domain defined on the server. Route domain rules are checked after global rules.

About virtual server firewalls

A *virtual server firewall* is an IP packet filter configured on the virtual server and, therefore, designated for client-side traffic. Any IP packet that passes through the virtual server IP address is assessed and possibly filtered out by this firewall.

When you create firewall rules, rule lists, or policies, you can select one of several contexts, including virtual server. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

Virtual server rules apply to the selected virtual server only. Virtual server rules are checked after route domain rules.

About self IP firewalls

A *self IP firewall* is an IP packet filter configured on the self IP address, a firewall designated for server-side traffic. Any IP packet that passes through the self IP is assessed and possibly filtered out by this firewall.

A self IP address is an IP address on a BIG-IP® system that is associated with a VLAN and used to access hosts in that VLAN. By virtue of its netmask, a self IP address represents an address space; that is, a range of IP addresses spanning the hosts in the VLAN, rather than a single host address.

A static self IP address is an IP address that is assigned to the system and does not migrate between BIG-IP systems. By default, the self IP addresses created with the Configuration utility are static self IP addresses. One self IP address must be defined for each VLAN.

When you create firewall rules, rule lists, or policies, you can select one of several contexts, including self IP. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

The self IP context collects firewall rules that apply to the self IP address on the BIG-IP device. Self IP rules are checked after route domain rules.

About management firewalls

A *management firewall* is an IP packet filter configured on the management IP address and, therefore, designated to examine management traffic. Any IP packet that passes through the management IP address is assessed and possibly filtered out by this firewall.

The network software compares IP packets to the criteria specified in management firewall rules. If a packet matches the criteria, then the system takes the action specified by the rule. If a packet does not match a rule, then the software compares the packet against the next rule. If a packet does not match any rule, the packet is accepted.

Management firewalls collect firewall rules that apply to the management port on the BIG-IP® device. Management port firewalls are outside the firewall context hierarchy and management port rules are checked independently of other rules.

Note: *Policies and rule lists are not permitted on management firewalls. For management firewalls, only inline rules are allowed. To add inline rules, drag-and-drop them onto the management firewall.*

You can also drag-and-drop address lists, and port lists onto management firewalls.

Chapter 4

Managing Shared Objects

About shared objects

In BIG-IQ™ Security, the shared objects that you can view and manage include:

Address lists
Collections of IPv4 or IPv6 addresses, address ranges, and subnets. These collections are saved on a server and used by policies, rule lists, and rules to allow or deny access to specific IP addresses in IP packets. Firewall rules compare all addresses or address ranges in a given address list to either the source or the destination IP address, depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Port lists
Collections of ports and port ranges. These collections are saved on a server and used by policies, rule lists, and rules to allow or deny access to specific IP addresses in IP packets. As with address lists, firewall rules compare all ports and port ranges in a given port list to either the source or the destination port, depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Schedules
Schedules are assigned to firewall rules, rule lists, and policies to control when rules, rule lists, and policies are active on the firewall. In the Shared Objects panel, you can hover over schedule names to see the name displayed in a tooltip. This feature is useful if the schedule name is longer than the panel.

Renaming shared objects

BIG-IQ™ Security does not support renaming a shared object.

As an alternative to renaming, you can create a new shared object and replace the original shared object where it is in use.

1. Create the new shared object. Consider cloning the object as the fastest and most reliable way to create a new object with the same content as the original but a new name.
2. Locate every instance of the original shared object by hovering over the gear icon associated with the object and selecting **Show Related Items**. As a result, all objects are grayed out except instances where the object is used. In addition, a count is added to the panel header, indicating the number of times the object is used within that panel.
3. Navigate to each instance where the original shared object is in use and replace it with a reference to the newly-created shared object.
4. Remove the original shared object. Note that you cannot remove a shared object that is still in use.

Duplicating shared objects

1. Navigate to the shared object you want to duplicate and hover over the name.
2. When the **gear** icon appears, click it.
3. From the expanded panel, click **Clone**. The system displays a copy of the shared object with blank Name and Description property fields.
4. Enter a unique name, (optional) description, and any other edits.

5. When finished, click **Save**. The cloned shared object is added to the existing list in the Shared Objects panel.

Removing shared objects

1. Navigate to the shared object you want to remove and hover over the name.
2. When the **gear** icon appears, click it.
3. From the expanded panel, click **Remove**. If the shared object is being used by another shared object, policy, rule, or rule list, a popup appears informing you that you cannot remove shared objects that are in use. Click **OK** to acknowledge this message. If the shared object can be removed, a popup appears confirming the removal. Click **OK** to confirm.

About address lists

Address lists are collections of IPv4 or IPv6 addresses, address ranges, nested address lists, or subnets saved on a server and available for use in firewall rules, rule lists, and policies.

Firewall rules refer to address lists to allow or deny access to specific IP addresses in IP packets. Firewall rules compare all addresses from the list to either the source or the destination IP address (in IP packets), depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Address lists are containers and must contain at least one address entry. You cannot create an empty address list; you cannot remove an entry in an address list if it is the only one.

Where address lists are visible in the expanded panels for Firewall Contexts, Policies, and Rule Lists, you can hover over nested address lists to see the first-level content displayed in a tooltip. The content (addresses, ranges, and nested address lists) is displayed whether or not the address list is locked for editing.

If a policy, rule list, or rule is locked for editing, you can right-click an address, address range, or address list in the locked object and remove that address, address range, or address list.

To view address list names that are longer than the display field, hover over the name to see the full name displayed in the tooltip.

Note: *Before nesting an address list inside an address list, check to be sure this option is supported on your BIG-IP® device.*

Managing address lists

From the BIG-IQ™ Security Shared Objects panel, you can add address lists or select address lists for deeper inspection or edit. From the expanded panel, you can clone, edit, or remove addresses, address ranges, or nested address lists.

You can define one or more reusable lists of addresses, and you can select one or more address lists to be included in a firewall rule.

Note: *Address lists are containers and must contain at least one entry. You cannot create an empty address list; you cannot remove an entry in an address list if it is the only one.*

---

1. To add an address list, hover over the Address Lists banner and click the + icon. In the expanded panel, populate the property fields as required. All boxes outlined in gold are required. The Partition field is outlined in gold and although it is pre-populated with Common, it is an editable field. Click Tab to advance from field to field. When you are finished, click **Add**.
2. To edit an address list, hover over the address list name and click the **gear** icon. In the expanded panel, click **Edit** to lock the object. Edit the Address List Properties and the Addresses areas as required. Click Tab to advance from field to field. When finished, click **Save** or **Save and Close**.
3. To duplicate an address list, hover over the address list that you want to duplicate. Click the **gear** icon. In the expanded Address Lists panel, click **Clone**. The system displays a copy of the address list with blank Name and Description property fields. The Partition property field is pre-populated with Common. Enter a unique name, (optional) description, partition and any other edits to the address list entries. When finished, click **Add**. The cloned address list is added to the existing list of address lists.
4. To remove an address list, hover over the address list name that you want to remove and then click the **gear** icon. In the expanded Address Lists panel, click **Remove**. If the address list is being used by another address list, a policy, rule, or rule list, a popup screen appears informing you that you cannot remove shared objects that are in use. Click **OK** to acknowledge this message. If the shared object can be removed, a popup screen appears confirming the removal. Click **OK** to confirm.
5. To add addresses, address ranges, or nested address lists to an existing address list, hover over the address list name that you want to add to and then click the **gear** icon. Click **Edit** to lock the object. Then, click the + icon to the right of an address. A new row is added to the Addresses table under that row. Next, select Address, Address Range, or Address List from the drop-down list under the Type column. If you select, Address List, in the Addresses column, type the first letter of an existing address list. A list of existing address lists appears. Select an address list from the list. When finished, click **Save** or **Save and Close**.
6. To add address lists to firewalls and rules (used in rule lists and policies), navigate to the firewall or rule and lock it for editing. If you are editing a firewall, be sure to select the Enforced tab so that Enforced Firewall Rules are visible. Then, expand the Address Lists panel, select the address list you want to add, and drag-and-drop it onto the firewall or rule.
7. To remove entries from an existing address list, click the address list name that you want to remove an entry from and then click the **gear** icon. Click **Edit** to lock the object. Next, click the **X** icon to the right of the address, address range, or address list that you want to remove. Then, click **Save and Close**.

Address list properties and addresses

Property	Description
Name	Text field naming the address list.
Description	Optional description of the address list.
Partition	Field pre-populated with Common (the default). This field is editable when creating or cloning address lists.
Type	After locking the address list for editing, select one of the following: • Address. Then, enter the address in the Addresses field. You can also enter an address range in this field by entering a range in the format: n.n.n.n-n.n.n.n. • Address range. The Addresses field becomes 2 fields separated by "to." Enter the beginning address and ending addresses in these fields as appropriate. • Address list. When you type the first letter of a saved list, the Addresses field is populated with a picker list that displays saved address lists. You then select from the list.

Property	Description
Addresses	IPv4 or IPv6 address, address range, or nested address list. There are many ways an IPv4 or IPv6 address or address range can be constructed. The following methods and examples are not meant to be exhaustive. IPv4 format: *a.b.c.d*[/*prefix*]. For example: `60.63.10.10` IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329` IPv6 abbreviated form is supported. You can shorten IPv6 addresses as defined in RFC 4291. You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. Example IPv6 subnet: `2001:db8:a::/64`. You can append a route domain to an address using the format %RouteDomainID/Mask. For example: `12.2.0.0%44/16`.
Description	Optional text field used to describe the address, address range, or nested address list.

About port lists

Port lists are collections of ports, port ranges, or port lists saved on a server and available for use in firewall rules, rule lists, and policies.

Firewall rules refer to port lists to allow or deny access to specific ports in IP packets. They compare a packet's source port and/or destination port with the ports in a port list. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Port lists are containers and must contain at least one entry. You cannot create an empty port list; you cannot remove an entry in a port list if it is the only one.

Where port lists are visible in the expanded panels for Firewall Contexts, Policies, and Rule Lists, you can hover over port lists to see the first-level content displayed in a tooltip. The content is displayed whether or not the port list is locked for editing.

If a policy, rule list, or rule is locked for editing, you can right-click a port, port range, or port list in the locked object and remove that port, port range, or port list.

To view port list names that are longer than the display field, hover over the name to see the full name displayed in the tooltip.

Note: *Before nesting a port list inside a port list, check to be sure this option is supported on your BIG-IP® device.*

Managing port lists

From the BIG-IQ™ Security Shared Objects panel, you can add port lists or select port lists for deeper inspection or edit. From the expanded panel, you can clone, edit, or remove ports, port ranges, or nested port lists.

You can define one or more reusable lists of ports, and you can select one or more port lists to be included in a firewall rule.

Note: *Port lists are containers and must contain at least one entry. You cannot create an empty port list; you cannot remove an entry in a port list if it is the only one.*

---

1. To add a port list, hover over the Port Lists banner and click the + icon. In the expanded panel, populate the property fields as required. All boxes outlined in gold are required. The Partition field is outlined in gold and although it is pre-populated with Common, it is an editable field. Click Tab to advance from field to field. When finished, click **Add**.
2. To edit a port list, hover over the port list name and click the **gear** icon. In the expanded panel, click **Edit** to lock the object. Edit Port List Properties and the Ports areas as required. Click Tab to advance from field to field. When finished, click **Save** or **Save and Close**.
3. To duplicate port lists, hover over the port list that you want to duplicate. Click the **gear** icon. In the expanded Port Lists panel, click **Clone**. The system displays a copy of the port list with blank Name and Description property fields. The Partition property field is pre-populated with Common. Enter a unique name, (optional) description, partition and any other edits to the port list entries. When finished, click **Add**. The cloned port list is added to the existing list of port lists.
4. To remove a port list, hover over the port list name that you want to remove and then click the **gear** icon. In the expanded panel, click **Remove**. If the port list is being used by another port list, a policy, rule, or rule list, a popup screen appears informing you that the shared objects is in use. Click **OK** to acknowledge this message. If the shared object can be removed, a popup screen appears confirming the removal. Click **OK** to confirm.
5. To add ports, port ranges, or port lists to an existing port list, click the port list name that you want to add to and then click the **gear** icon. Click **Edit** to lock the object. Then, click the + icon to the right of a port. A new row is added to the Ports table under that row. In this new row, you can select Port, Port Range, or Port List from the drop-down list under the Type column. If you select, Port List, in the Ports column, type the first letter of an existing port list. A list of existing port lists appears. Select a port list from the list. When finished, click **Save** or **Save and Close**.
6. To add port lists to firewalls and rules (used in rule lists and policies), navigate to the firewall or rule and lock it for editing. If you are editing a firewall, be sure to select the Enforced tab so that Enforced Firewall Rules are visible. Then, expand the Port Lists panel, select the port list you want to add, and drag-and-drop it onto the firewall or rule.
7. To remove entries from an existing port list, click the port list name that you want to remove an entry from and then click the **gear** icon. Click **Edit** to lock the object. Next, click the **X** icon to the right of the port, port range, or port list that you want to remove. Then, click **Save and Close**. You can also remove ports, port ranges, or port lists from rule lists by expanding and locking the rule list, hovering over the item, right-clicking, and selecting **Remove item**.

Port list properties and ports

Property	Description
Name	Unique name used to identify the port list.
Description	Optional description for the port list.
Partition	Field pre-populated with Common (the default). This field is editable when creating or cloning port lists.

Property	Description
Type	After locking the port list for editing, select one of the following: • Port. Then, enter the port in the Ports field. You can also enter a port range in this field by entering a range in the format: n-n. Valid port numbers are 1-65535. • Port range. The Ports field becomes 2 fields separated by "to." Enter the beginning port and ending port in these fields as appropriate. • Port list. When you type the first letter of a saved list, the Ports field is populated with a picker list that displays saved port lists. You then select from the list.
Ports	Port, port range, or port list. Valid port numbers are 1-65535.
Description	Optional text field used to describe the port, port range, or nested port list.

About schedules

Schedules are assigned to rules, rule lists, and policies to control when these shared objects are actively evaluated.

By default, all rules, rule lists, and policies are on a continuously active schedule. Schedules are continuously active if created without any scheduling specifics (such as the hour that the schedule starts). If you apply a schedule to a rule, rule list, or policy, you can reduce the time that the rule, rule list, or policy is active.

Managing schedules

From the BIG-IQ™ Security GUI Shared Objects panel, you can add, edit, duplicate, or remove schedules.

You can also add a schedule to a firewall, policy, or rule by opening the firewall (or policy or rule), locking it for edit, and dragging-and-dropping the schedule onto the rule's State column.

Note: *You can define one or more reusable schedules, and you can select one or more schedules to be included in a firewall rule.*

1. To add schedules, hover over the Schedules banner and click the + icon. In the expanded panel, populate the property fields as required. Click Tab to advance from field to field. When you are finished, click **Add**.
2. To edit schedules, hover over a schedule name and click the **gear** icon. From the expanded panel, click **Edit** to lock the object. Edit the Schedule Properties as required. Click Tab to advance from field to field. When finished, click **Save**.
3. To remove schedules, hover over the schedule name that you want to remove and when the **gear** icon appears, click it. From the expanded panel, click **Remove**. If the schedule is being used by a policy, rule, or rule list, a popup screen appears informing you that you cannot remove shared objects that are

in use. Click **OK** to acknowledge this message. If the shared object can be removed, a popup screen appears confirming the removal. Click **OK** to confirm.

4. To add schedules by drag-and-drop to firewalls, policies, and rules, navigate to the firewall (policy or rule) and lock it for editing. Be sure the Enforced Firewall Rules are visible. Then, expand the Schedules panel, select the schedule you want to add, and drag-and-drop it onto the State column in the rule. When finished, click **Save**.

Cloning schedules

Use the expanded Shared Object panel to clone schedules and add them to the BIG-IQ™ Security database.

Then, assign schedules to firewall rules to control when the rules apply.

1. Under the Shared Objects header, click **Schedules** to expand the Schedules section and display the list of schedules.
2. Hover over the name of the schedule that you want to clone and when the **gear** icon appears, click it to expand the panel.
3. Click **Clone**.
4. Edit the fields as required. Your changes are saved automatically.

Option	Description
Name	Unique, user-provided name.
Description	Optional description for the schedule.
Partition	Accept the default (Common) or enter a partition name. Although pre-populated with Common, you can set the partition when cloning a schedule. No whitespace is allowed in the partition name.
Date Range	Click the field to display a calendar, and select a date in the calendar. When finished, click **Done**.
Time Span	Format: HH:MM. Time span start and end means you can set the schedule to run only during certain hours of the day. If you leave these fields blank, the schedule will run all day.
Day	Select all check boxes that apply. You must select at least one.

The cloned schedule appears in the Schedules section of the Shared Objects panel.

Schedule properties

Property	Description
Name	Unique name used to identify the schedule.
Description	Optional description for the schedule.
Partition	Informational, read-only field displaying the name of the partition associated with the schedule.
Date Range	Click the first field to display a calendar popup screen and select a start date. Click the second field

Property	Description
Note: *Using the GUI to specify the start and end dates and times is the preferred method. However, if you do specify dates manually, use the format: YYYY-MM-DD HH:MM:SS.*	to display a calendar and select an end date. You can specify: **Start date and no end date** The equivalent on the BIG-IP® system is After, which specifies that the schedule starts after the specified date and runs indefinitely. The schedule is activated starting on the selected date and runs until you change the start date or delete the schedule. Click in the field to choose a start date from a popup calendar. You can specified a start time in the same popup screen. **End date and no start date** The equivalent on the BIG-IP system is Until, which specifies that the schedule starts immediately and runs until a specified end date. The schedule is immediately activated and not disabled until the end date is reached. Click in the field to choose an end date from a popup calendar. You can specified an end time in the same popup screen. **Both a start date and an end date** The equivalent on the BIG-IP system is Between, which specifies that the schedule starts on the specified date and runs until the specified end date. Click in the fields to choose the start and end dates from a popup calendar. You can specified start and end times in the same popup screen. **Neither a start date nor an end date** The equivalent on the BIG-IP system is Indefinite, which specifies that the schedule starts immediately and runs indefinitely. The schedule remains active until you change the date range or delete the schedule.
Time Span	Time is specified in military time format: HH:MM. You can specify time manually or click in the fields and use the Choose Time popup screen. Click the first time span field and use the sliders to specify a start time in the popup screen. Click the second time span field and use the sliders to specify an end time in the popup screen. If you leave these fields blank, the schedule runs all day, which is the default on the BIG-IQ™ Security system and on BIG-IP devices. (This option is explicitly called All Day on BIG-IP devices.)
Day	Select check boxes for all days that apply. You must select at least one day per week.

Chapter 5

Managing Firewall Policies

About managing policies in BIG-IQ Security

A *policy* is a set of rules and/or rule lists. BIG-IP® network firewalls use policies to specify traffic-handling actions and to define the parameters for filtering network traffic. You can assign inline rules, rule lists, or a policy to a firewall. Use policies to facilitate assigning a common collection of rules consistently across multiple firewalls.

The network software compares IP packets to the criteria specified in policies. If a packet matches the criteria, then the system takes the action specified by the policy. If a packet does not match any rule in the policy, the software accepts the packet or passes it to the next policy, rule, or rule list.

In BIG-IQ® Security, the Policies panel displays the policies available for assignment to firewalls.

You can configure policies as enforced or staged:

- An enforced policy refers to a policy whose actions are executed. Actions include: accept, accept decisively, drop, and reject.

  You are restricted to assigning a single, enforced policy on any specific firewall. If you have an enforced policy on a firewall, you cannot also have inline rules and rule lists on that firewall.
- A staged policy refers to a policy that is evaluated but policy actions are not enforced. All activity is logged.

  You are restricted to assigning a single, staged policy on any specific firewall. You can have inline rules and rule lists assigned to a firewall (in the enforced area) and have a configured staged policy on that firewall. You cannot have inline rules/rule lists in the staged area.

Thus, you can stage a policy first and then examine logs to determine how the policy has affected traffic. Then, you can determine the timing for turning the policy from staged to enforced.

Policies can contain any combination of rules and rule lists. Policies cannot contain other policies. You can re-order rules within a policy.

Note: *The BIG-IQ™ Security system is aware of functionality implemented in one BIG-IP version but not in another. In terms of policies, this means that you are prohibited from dropping a policy onto a firewall on a BIG-IP device that does not have the software version required to support it.*

Adding policies

From the Policies panel, you can add policies.

1. Navigate to the Policies panel.
2. Hover in the Policies banner and click the + icon to display the New Policy panel. The Properties tab, as well as the Rules & Rule Lists tab are also visible.
3. On the Properties tab, edit the fields as required. All boxes outlined in gold are required fields.

Option	Description
Name	User-provided name for the policy. This field is read-only when editing a policy.
Description	Optional description for the policy.

Option	Description
Partition	Although pre-populated with Common (default), you can set the partition when creating or cloning policies by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name.

4. On the Rules & Rule Lists tab, click **Create Rule** or **Add Rule List**.
5. When finished, click **Add**.

A new policy is added to the Policies panel in the correct order alphabetically.

You can drag-and-drop a policy to add it to a firewall. To configure the same policy consistently across many firewalls, drag-and-drop the policy to multiple firewalls.

Managing policy properties

From the Policies panel, you can manage policies (edit policies, create/edit rules, and add rule lists). You can also reorder rules in policies. You cannot edit rule lists or reorder rules within rule lists from this panel.

1. Navigate to the Policies panel.
2. Hover in the policy banner and click the **gear** icon to display the Properties tab. (The Rules & Rule Lists tab is also visible.)
3. On the Properties tab, view or edit the properties as required.

Option	Description
Name	User-provided name for the policy. The text field accepts up to 128 characters. This field is read-only when editing a policy.
Description	Optional. Description for the policy. The text field accepts up to 128 characters.
Partition	Read-only field displaying the name of the partition associated with the policy.

4. When finished, click **Add** or **Save** as appropriate.

A new or saved policy is added to the Policies panel in the correct order alphabetically.

You can then drag-and-drop a policy to add it to a firewall. To configure the same policy consistently across many firewalls, drag-and-drop the policy to multiple firewalls.

Cloning policies

Cloning enables you to quickly and easily create policies tailored to address any unique aspects of your network firewall environment. When you clone a policy, you create an exact copy of the policy which you can then edit to address any special considerations.

Users with the roles of Firewall_View or Firewall_Deploy cannot clone policies.

1. Navigate to the Policies panel.

2. Hover over the name of the policy that you want to clone and when the **gear** icon appears, click it to display the expanded panel.
3. Click **Clone**.
4. In the Properties tab, edit the fields as required. Click **Tab** to advance from field to field.

Option	Description
Name	Enter a unique name for the cloned policy. The clone cannot have the same name as the source policy unless the partition name is changed.
Description	Enter an optional description.
Partition	Although pre-populated with Common (default), you can set the partition when creating or cloning policies by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name.

5. In the Rules & Rule Lists tab, edit the fields as required to configure the clone. You can also click **Create Rule** to add a new rule. Or, click **Add Rule List**. From the popup displayed, select a rule list and click **Add**.
6. When finished, click **Add**. Any changes made are preserved. If you click **Cancel**, the policy is not cloned.

The cloned policy appears in the Policies panel.

Managing policy rules and rule lists

From the Policies panel, you can create rules and add rule lists. You can also reorder rules in policies. You cannot edit rule lists or reorder rules inside rule lists.

Note: *From the Firewalls panel, you can add and remove but not edit policies.*

1. Navigate to the Policies panel.
2. Hover in the banner for the specific policy you want to edit and click the **gear** icon.
3. If necessary, click the Rules & Rule Lists tab.
4. On the Rules & Rule Lists tab, click **Create Rule** or **Add Rule List**.
5. When finished, click **Save**.

The saved policy is added to the Policies panel in the correct order alphabetically.

You can then drag-and-drop a policy to add it to a firewall. To configure the same policy consistently across many firewalls, drag-and-drop the policy to multiple firewalls.

Removing policies

From the Policies panel, you can remove policies.

If a policy is in use or if any shared objects inside that policy are in use, you cannot remove it.

To see where a policy is used, click the policy and the name appears in the filter field. Then, click **Apply**. The GUI filters on that policy name and displays only the instances where the policy is used.

1. Navigate to the Policies panel.
2. Hover in the header of the policy you want to remove and click the **gear** icon.
3. In the banner, click **Remove**.
4. To permanently remove this policy from the BIG-IQ™ system, click **Remove** in the confirmation popup screen.

The policy is permanently removed.

About policy management using snapshots

It is possible to introduce errors during the editing of the firewall working-configuration set. In some cases, you might not detect these errors immediately. When you discover these errors, you will probably want to roll back to a previous state as quickly as possible to restore service. Then, you can triage to discover the root causes of any errors.

In one scenario, you might perform multiple emergency deployments in an attempt to fix a problem. If such attempts did not fix the issue, you might want to roll back to the most stable state prior to where you first saw the problem.

In another scenario, you might want to roll back after importing a device. For example, an administrator might import a device and as part of the import process, decide to overwrite the firewall-shared objects stored in the BIG-IQ™ database. Subsequently, the administrator decides that the import was a mistake and wants to roll back to the state of the shared objects before the import.

You can address all of these scenarios by restoring from a snapshot.

The BIG-IQ system provides the ability to create snapshots in these ways:

- During discovery, BIG-IQ Security takes a snapshot of the working-configuration set on the device. This is the default behavior (retain the check box selection).
- During a reimport, you can take a snapshot of the working-configuration set on the device before the reimport. This is the default behavior (retain the check box selection).
- During deployment, BIG-IQ Security takes a snapshot when you click **Evaluate**.
- At any time, you can create a user-defined snapshot from the Add Snapshot panel.

Chapter 6

Managing Rules and Rule Lists

About rules and rule lists

With the BIG-IQ™ Security system, you can manage rules and rule lists from the Rule Lists panel. You import and manage rules (and/or rule lists) from BIG-IP® devices. You can also define rules and rule lists within BIG-IQ Security and deploy back to the BIG-IP device.

Network firewalls use rules (and rule lists) to specify traffic-handling actions.

Rules are not independent objects and can exist only within rule lists or policies. You can define a list of rules for a specific firewall and/or refer to one or more shared rule lists (by name from other firewalls).

The network software compares IP packets to the criteria specified in rules. If a packet matches the criteria, then the system takes the action specified by the rule. If a packet does not match any rule from the list, the software accepts the packet or passes it to the next rule or rule list. For example, the system compares the packet to self IP rules if the packet is destined for a network associated with a self IP address that has firewall rules defined.

A packet must pass all tests to match successfully. For example, to match against a source subnet and several destination ports, a packet must originate from the given subnet and must also have one of the specified destination ports.

Rule lists are containers for rules. A rule list can contain thousands of ordered rules but cannot be nested inside another rule list. It is an ordered list of rules, which means that rules are run in the order they appear. However, you can reorder rules at any time.

Rules and rule lists can be applied to all firewall types:

- Global
- Route domain
- Virtual server
- Self IP
- Management (rules only)

You can reuse a rule list across multiple firewalls, such as the firewalls for self IPs, route domains, and the global firewall. To reuse rule lists, drag-and-drop them to firewalls and policies as you choose.

Adding rules

You can create specific rules in support of a specific firewall or policy, gather those rules in a rule list, and assign the rule list to the firewall or policy.

1. Hover in the Rule Lists banner and click the + icon to display the Properties tab and the Rules tab.
2. In the Properties tab, edit the Rule List Properties as required.

Option	Description
Name	Enter a name for the rule list.
Description	Enter an optional description.

3. In the Rules tab, click **Create Rule**.
   A new row appears in the table. The row contains a rule template, including defaults, for the new rule.
4. Edit as appropriate.

Click Tab to advance from field to field.

You can also add rules by right-clicking under the bottom row in the Rules table. The rule template is added to the bottom of the table. Once entered, you can reorder rules by dragging-and-dropping them until they are in the correct order.

5. When finished, click **Save**.
6. To remove a rule, hover over the rule name and right-click. From the drop-down menu, select **Delete Rule**. This drop-down menu also provides options to **Add rule before** and **Add rule after** (the rule you are hovering over).

The new rule list appears at the bottom of the Rule Lists panel.

Adding rule lists

To add rule lists, expand the Rule Lists panel to display the Properties tab and the Rules tab.

1. Hover in the Rule Lists banner and click the + icon to display the Properties tab and the Rules tab.
2. In the Properties tab, edit the fields as required.

Option	Description
Name	Enter a name for the rule list.
Description	Enter an optional description.
Partition	Although pre-populated with Common (default), you can set the partition when creating or cloning rule lists by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name.

3. In the Rules tab, click **Create Rule**.

   A new row appears in the table. This row contains a template, including defaults.
4. Edit as appropriate.

   Click Tab to advance from field to field.

   You can also add rules by right-clicking under the bottom row in the Rules table. The rule is added to the bottom of the table. You can then reorder rules by dragging and dropping them until they are in the correct order.
5. When finished, click **Save**.

The new rule list appears at the bottom of the Rule Lists panel.

Managing rule lists

You can manage the content of rule lists from the Rule Lists panel, including the order of rules in rule lists. You must lock a rule list before editing it.

1. Hover in the header for the rule list that you want to edit, and click the **gear** icon to display the Properties tab and the Rules tab.

2. In the Properties tab, edit the content you want to change.

Option	Description
Name	Change the name of the rule list.
Description	Enter or change an optional description.
Partition	Informational, read-only field. You can change the partition name only when creating or cloning a rule list.

3. In the Rules tab if the rule list is not already locked, click **Edit** to establish a lock.
4. Click the row of the rule you want to edit.
5. Edit as appropriate.

   Click Tab to advance from field to field.

   To reorder rules, simply drag-and-drop the rules until they are in the correct order.
6. When finished, click **Save**.

Changes made to the rule list are reflected the next time the Firewall Contexts or Policies panels are refreshed.

Cloning rule lists

Cloning enables you to quickly and easily create rule lists tailored to address any unique aspects of your network firewall environment. When you clone a rule list, you create an exact copy of the rule list which you can then edit to address any special considerations.

Users with the roles of Firewall_View or Firewall_Deploy cannot clone policies.

.

1. Navigate to the Rule Lists panel.
2. Hover over the name of the rule list that you want to clone and when the **gear** icon appears, click it to display the expanded panel.
3. Click **Clone**.
4. In the Properties tab, edit the fields as required. Click **Tab** to advance from field to field.

Option	Description
Name	Enter a name for the cloned rule list. The clone cannot have the same name as the source rule list unless the partition name is changed.
Description	Enter an optional description.
Partition	Although pre-populated with Common (default), you can set the partition when creating or cloning rule lists by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name.

5. In the Rules tab, edit the rules as required to configure the clone. You can also click **Create Rule** to add a new rule.
6. When finished, click **Add**. Any changes made are preserved. If you click **Cancel**, the rule list is not cloned.

The cloned rule list appears at the bottom of the Rule Lists panel.

Removing rule lists

To remove rule lists, expand the Rule Lists panel to display the Properties tab and the Rules tab.

1. Hover in the header of a rule list you want to remove and when the **gear** icon appears, click it to display the Properties tab and the Rules tab.
2. At the top of the expanded area, click **Remove**.
3. If safe to remove the rule list, a confirmation dialog box appears. Click **Remove** to confirm.

   If the rule list is in use, you cannot complete the removal. A popup appears informing you that you cannot remove the rule list because it is in use. Click **Close** to acknowledge this message and then click **Cancel** in the Remove popup screen. To see where a rule list is used, click the rule list and the name appears in the search field. Then click **Apply**. The GUI displays only those objects related to the search. To clear the search, click the **x** icon to the right of the search string.

The rule list disappears from the Rule Lists panel.

Rule and rule list properties

You can configure network firewalls after import into the BIG-IQ™ Security system through the Firewall Contexts panel. Or, you can edit imported rules, rule lists, or policies through the Rule Lists panel or the Policies panel. However, you must edit shared objects through the Shared Objects panel. Shared objects cannot be edited inside rules. The following table lists and describes the properties required when configuring network firewall rules and rule lists.

Property	Description
Name	Unique, user-provided name for the rule or rule list. If the name is a rule list name, it is preceded by referenceTo_ when dragged-and-dropped to a firewall or policy. For example: referenceTo_sys_sef_allow_all.
Address (Source)	There are many ways to construct an IPv4 or IPv6 address, address range, or address list. The following methods and examples are not meant to be exhaustive. IPv4 format: *a*.*b*.*c*.*d*[/*prefix*]. For example: `60.63.10.10` IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329` You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. An example of an IPv6 subnet is as follows: `2001:db8:a::/64`. You can append a route domain to an address using the format %RouteDomainID/Mask. For example, `12.2.0.0%44/16`. From the drop-down list, select: **Address** Enter the address in the Addresses field. You can also enter an address range in the Addresses field using the format: n.n.n.n-n.n.n.n. For example: 1.1.1.1-2.2.2.2.

Property	Description
	Address range Enter the beginning address in the first Addresses field and the ending address in the second Addresses field. **Address list** In the Addresses field, enter text to cause the display of stored address lists. You can select any of the address lists displayed. To the right, options are provided to add additional addresses, address ranges, or address lists (+) and to delete addresses, address ranges, or address lists (**X**). When finished, click **Save** or **Add**.
Port	Ports, port ranges, or port lists. From the drop-down list, select: **Port** Enter the port in the Ports field. You can also enter a port range in the port field by entering a range in the format: n-n. For example: 43-44. **Port range** Enter the beginning port in the first Ports field and the ending port in the second Ports field. **Port list** In the Ports field, enter text to cause the display of stored port lists. You can select any of the port lists displayed. To the right, options are provided to add additional ports, port ranges, or port lists (+) and to delete ports, port ranges, or port lists (**X**). When finished, click **Save** or **Add**.
VLAN	Name of the VLAN physically present on the device (Internal, External, or Any). The VLAN must be configured on the device or the deploy fails. When finished, click **Save** or **Add**.
Address (Destination)	There are many ways to construct an IPv4 or IPv6 address, address range, or address list. The following methods and examples are not meant to be exhaustive. IPv4 format: *a.b.c.d*[/*prefix*]. For example: `60.63.10.10` IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329` You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. An example of an IPv6 subnet is as follows: `2001:db8:a::/64`. You can append a route domain to an address using the format %RouteDomainID/Mask. For example, `12.2.0.0%44/16`. From the drop-down list, select: **Address** Enter the address in the Addresses field. You can also enter an address range in the Addresses field using the format: n.n.n.n-n.n.n.n. For example: 1.1.1.1-2.2.2.2. **Address range** Enter the beginning address in the first Addresses field and the ending address in the second Addresses field.

Property	Description
	Address list In the Addresses field, enter text to cause the display of stored address lists. You can select any of the address lists displayed. To the right, options are provided to add additional addresses, address ranges, or address lists (+) and to delete addresses, address ranges, or address lists (**X**). When finished, click **Save** or **Add**.
Port	Ports, port ranges, or port lists. From the drop-down list, select: **Port** Enter the port in the Ports field. You can also enter a port range in the port field by entering a range in the format: n-n. For example: 43-44. **Port range** Enter the beginning port in the first Ports field and the ending port in the second Ports field. **Port list** In the Ports field, enter text to cause the display of stored port lists. You can select any of the port lists displayed. To the right, options are provided to add additional ports, port ranges, or port lists (+) and to delete ports, port ranges, or port lists (**X**). When finished, click **Save** or **Add**.
Action	Click in the column and select one of the following: **accept** Allows packets with the specified source, destination, and protocol to pass through the firewall. Packets that match the rule, and are accepted, traverse the system as if the firewall is not present. **accept decisively** Allows packets with the specified source, destination, and protocol to pass through the firewall, and does not require any further processing by any of the further firewalls. Packets that match the rule, and are accepted, traverse the system as if the firewall is not present. If the Rule List is applied to a virtual server, management IP, or self IP firewall rule, then Accept Decisively is equivalent to Accept. **drop** Drops packets with the specified source, destination, and protocol. Dropping a packet is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached. **reject** Rejects packets with the specified source, destination, and protocol. When a packet is rejected the firewall sends a destination unreachable message to the sender. When finished, click **Save** or **Add**.
Description	Optional description for the current rule. To add a description, click in the column, enter text, and click **Save** or **Add**.

Property	Description
Protocol	IP protocol to compare against the packet. Select the appropriate protocol from the drop-down list and click **Save** or **Add**. If you select ICMP or IPv6-ICMP, a gear icon appears. Click the **gear** icon to display the screen where you can change the Type code combinations for the ICMP and ICMPv6 protocols. The gear icon also appears if you select **Other** to enter the numeric value of the protocol. The default Type is **Any**. The default Code is **Any**. **For ICMP** Choose from a list of control messages, such as Echo Reply (0) and Destination Unreachable (3), or you can select Any to indicate that the system applies the rule for all ICMP messages. You can also select Other to specify an ICMP message not listed. The ICMP protocol contains definitions for the existing message type and number pairs. **For ICMPv6** Choose from a list of control messages, such as Packet Too Big (2) and Time Exceeded (3), or you can select Any to indicate that the system applies the rule for all ICMPv6 messages. You can also select Other to specify an ICMPv6 message not listed. The ICMPv6 protocol contains definitions for the existing message type and number pairs. If the value selected for Type is Any, the selected Code must be Any. If the value selected for Type is Other, the number entered must be in the range of `0 and 255`. **For ICMP** This field specifies the code returned in response to the specified ICMP message type. You can choose from a list of codes, each set appropriate to the associated type, such as No Code (0) (associated with Echo Reply (0)) and Host Unreachable (1) (associated with Destination Unreachable (3)), or you can select Any to indicate that the system applies the rule for all codes in response to that specific ICMP message. You can also select Other to specify a code not listed. The ICMP protocol contains definitions for the existing message code and number pairs. **For ICMPv6** This field specifies the code returned in response to the specified ICMPv6 message type. You can choose from a list of codes, each set appropriate to the associated type, such as No Code (0) (associated with Packet Too Big (2)) and fragment reassembly time exceeded (1) (associated with Time Exceeded (3)), or you can select Any to indicate that the system applies the rule for all codes in response to that specific ICMPv6 message. You can also select Other to specify a code not listed. The ICMPv6 protocol contains definitions for the existing message code and number pairs. If the value selected for Type is `Any`, the selected Code must be `Any`. If the value selected for Code is `Other`, the number entered must be in the range of `0 and 255`.
State	Click in the column and select an option from the drop-down list to specify whether the rule is enabled, disabled, or scheduled. The field is updated. Click **Save** or **Add** when you are ready to save your changes. If you select **scheduled** from the drop-down list, the Select Schedule drop-down list is displayed in the screen. Select a schedule and click **OK**.

Property	Description
	If you have assigned a schedule, then a gear icon appears to the right of the State setting in the State column. To make changes to the State setting, click the **gear** icon to invoke the Select Schedule popup screen. If you have no pre-defined schedules, you cannot assign the scheduled state to the rule.
Log	Click in the column and select an option from the drop-down list to specify whether or not the firewall software should write a log entry for any packets that match this rule. From the drop-down list, select **true** (log an entry) or **false** (do not log an entry). When finished, click **Save** or **Add**. To set or edit this setting, the discovered device must be at version 11.3 HF6 or later. The setting is not editable earlier than version 11.3 HF6. When a new rule is added to a firewall through the BIG-IQ Security GUI, editing is enabled for the Log setting even for devices with versions earlier than 11.3 HF6.

Chapter 7

Managing Snapshots

About snapshots

BIG-IQ™ Security uses snapshots to protect the working-configuration set of the Security module. Thus, at any time, you can back up, restore, and deploy the BIG-IQ working configuration to a specific configuration state, or deploy a specific set of working configuration edits back to a BIG-IP® device. You can also compare one snapshot against another, or compare a snapshot against the BIG-IQ working configuration.

The Snapshots panel displays a list of imported snapshots under the naming convention Import-self-ip. For example: Import-10.64.6.111. You can create a snapshot when you create a new deployment, or you can add snapshots through the New Snapshot panel and name the snapshot according to your own convention.

Adding snapshots

Add snapshots so that you can restore the BIG-IQ™ working configuration to a specific configuration state, or deploy a specific set of working configuration edits back to a BIG-IP® device.

1. Navigate to the Snapshots panel.
2. Hover in the Snapshots banner and click the + icon to display the New Snapshot panel.
3. Edit the property fields as required.

Option	Description
Name	Enter a name for the snapshot.
Description	Enter a description (optional) that will assist in remembering the reason for the snapshot.

After the process completes, the snapshot is listed in the Snapshots panel by its user-provided name, user account name, and the date and time the snapshot was taken.

Comparing snapshots

Use the Compare tab and the functionality it provides to compare one snapshot against another, or to compare a snapshot against the BIG-IQ™ Security working configuration.

1. Navigate to the Snapshots panel.
2. Select a snapshot, and click the **gear** icon to expand and display the panel.
3. Click the Compare tab to ensure that it is selected.
4. Select **Working Configuration** to compare the BIG-IQ Security working configuration against the selected snapshot. Select **Snapshot** to compare a snapshot against the selected snapshot.
5. To compare a snapshot with the selected snapshot, drag-and-drop that snapshot from the Snapshots panel to this area. Or, click the **Select Snapshot** link. Then, from the Select From Available Snapshots popup screen, select a snapshot and click **Select**.
6. Click **Evaluate** to start the comparison. The Differences popup screen appears.
7. To display the JSON for each difference found, click a row in the table.

   Textual JSON appears for each difference found; snapshot on the left and working configuration, or second snapshot on the right.

Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**).

Restoring the working configuration from a snapshot

From the expanded panel, you can restore the working configuration using a selected snapshot as input. This process does not delete any shared objects that might have been added since the snapshot was taken.

1. Navigate to the Snapshots panel.
2. Hover over the snapshot containing the configuration you want to restore to, and click the **gear** icon to expand and display the panel.
3. In the expanded panel, click the Compare tab.
4. In the Compare tab, you can compare the selected snapshot against the **Working Configuration** or another **Snapshot**.

Option	Description
Working Configuration	If you select **Working Configuration** and click **Evaluate**, a popup screen displays the differences in the JSON between the snapshot (at left in the table) and the working configuration (at right in the table). Click any row to view the JSON for the two objects. Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**). Click any row to view the JSON for the two objects.
Snapshot	If you select **Snapshot**, specify the snapshot selected by clicking **Select Snapshot** or by dragging-and-dropping a snapshot to the **Compare against** field. Then, click **Evaluate** to view the differences in the JSON between the two snapshots. Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**). Click any row to view the JSON for the two objects.

5. When you are satisfied that you are restoring the correct configuration, click **Restore** at the top of the expanded panel.
6. In the popup screen, click **OK** to confirm that you want to continue. This popup screen explains that you cannot interrupt the restore process and that it provides an all-or-nothing restoration.
7. Click **Close** when you receive the confirmation popup screen.

Chapter 8

Deploying Configuration Changes

About BIG-IQ Security deployments

The BIG-IQ™ Security system displays individual deployments and their status (one action per row in the Deployment panel).

After you have completed edits to a firewall and shared objects, you can create a deployment to distribute those changes to selected BIG-IP® devices.

To create a deployment, hover over the header of the Deployment panel and then click the + icon. Populate the fields as needed and click **Evaluate**.

During the evaluation process, BIG-IQ Security:

1. Contacts the selected remote BIG-IP devices and synchronizes the working-configuration sets for all.
2. Takes a snapshot of the working-configuration set for each BIG-IP device.
3. Compares the remote and local configurations.
4. Calculates the set of changes to be deployed (number and type of each change).
5. Displays the number and type of each change.

Changes are displayed as follows:

- ADDED. New shared objects added to a rule and called by an existing rule list, policy, or firewall are counted as ADDED. Newly-created shared objects that are not referenced in a firewall are not counted and are not distributed.
- MODIFIED. Existing objects already used by an existing rule list, policy, or firewall and subsequently edited are counted as MODIFIED.
- REMOVED. Existing objects used by an existing rule list, policy, or firewall and subsequently removed are counted as REMOVED. If a shared object is removed from a rule and is no longer being used by any other rules, it is marked for removal from the selected devices. It is not removed from the BIG-IQ Security system unless expressly deleted.

Note: *If an individual rule in a rule list, policy, or firewall has been changed, added, or removed, the entire modified object (rule list, policy, or firewall) is marked for deployment. This also applies to adding, modifying, or removing ports in a port list, or addresses in an address list.*

During the distribution phase, configuration changes are pushed out to remote BIG-IP devices. The working-configuration set is deployed or the selected BIG-IP device is rolled back to the state reflected in the snapshot. Any changes made locally to the BIG-IP device are overwritten.

With BIG-IQ Security, you can deploy up to 20 devices in a single deployment.

Adding deployments

When you have completed edits to a firewall policy, you can create a deployment to push out to a target device any change that occurred to any configuration object.

1. To begin the process, navigate to the Deployment panel.
2. Hover in the Deployment banner and click the + icon to display the Add Deployment panel.
3. Edit the fields as required. Your changes are saved automatically.

Option	Description
Deployment Name	Name for the deployment that indicates its purpose. It can be useful to develop a convention such as ticket numbers.

Option	Description
Description	Optional description, including the purpose of the deployment or other relevant information.
Deployment Source	Choose between **Use Working Config** and **Use A Snapshot**. To deploy the working configuration currently on the BIG-IQ™ system, select **Use Working Config** and click **Evaluate**. To deploy from a snapshot, select **Use a Snapshot** and from the popup screen, select the snapshot you want to deploy from and click **Evaluate**.
Select Devices to Evaluate	Available devices are listed. Select or clear check boxes as appropriate.

4. When you are satisfied that you understand the differences and that you are deploying the changes that you want to, click the **Deploy** button in the panel.

A deployment is created and listed in the Deployment panel along with its status. A status of READY TO DEPLOY indicates that the working-configuration set can be deployed or the selected BIG-IP® device can be rolled back to the state reflected in the snapshot.

Managing deployments

When a deployment displays a status of READY TO DEPLOY, you can distribute configuration changes. If there are no changes to deploy, a message displays to confirm this.

1. To begin the process, navigate to the Deployment panel.
2. Hover in the banner of the deployment you want to manage and click the **gear** icon to expand the panel and display task properties.

Option	Description
Deployment Name	User-provided name of the deployment task.
Description	Optional description, including the purpose of the deployment or other relevant information.
User	Name of the user who initiated the deployment.
Task Status	Status for deployment phases (evaluation and distribution).
Start Time	Time the deployment started in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: 2013-05-31T08:16:17-07:00
End Time	Time the deployment ended in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: 2013-05-31T08:16:36-07:00

3. Click **Evaluate** to evaluate differences between the selected snapshot and the current configuration.
4. Click **Evaluate** to evaluate differences between the selected snapshot and the current configuration.
5. When you are satisfied that you understand the differences and that you are deploying the changes that you want to, click the **Deploy** button in the panel.

Deployment states are displayed during the deployment process. The working-configuration set is deployed or if a snapshot was selected, the BIG-IP® device is rolled back to the state reflected in the snapshot.

Deploying from snapshots

You can use snapshots to restore a specific configuration state or to deploy a specific set of working configuration edits back to the BIG-IP® device.

1. To begin the process, navigate to the Deployment panel.
2. Hover in the Deployment banner and click the + icon to display the Add Deployment panel.
3. Edit the fields as required. Your changes are saved automatically.

Option	Description
Deployment Name	Name for the deployment that indicates its purpose. It can be useful to develop a convention such as ticket numbers.
Description	Optional description, including the purpose of the deployment or other relevant information.
Deployment Source	Choose between **Use Working Config** and **Use A Snapshot**. To deploy the working configuration currently on the BIG-IQ™ system, select **Use Working Config** and click **Evaluate**. To deploy from a snapshot, select **Use a Snapshot** and from the popup screen, select the snapshot you want to deploy from and click **Evaluate**.
Select Devices to Evaluate	Available devices are listed. Select or clear check boxes as appropriate.

4. When you see the message READY TO DEPLOY under the deployment name in the Deployment panel, click the **gear** icon to expand the panel. Under the text **Evaluate found the following changes:** you will see a device name followed by an arrow. Click the arrow to display differences. Differences are listed by: name, type, change (added, modified, deleted), and device (blank unless the type is **firewall**). Click an object name to view the JSON in the table under the list of differences.
5. When you are satisfied that you understand the differences and that you are deploying the changes that you want to, click the **Deploy** button in the panel.

The specific set of working-configuration edits is deployed to the selected BIG-IP device.

Device deployment states

The following table displays states that occur during the deployment process and a brief description of each state.

NEW	The deployment process has started.
COMPLETED_RETRIEVE_DEVICES	Devices have been successfully retrieved. All managed devices on the BIG-IQ™ Security system have been found.
FAILED_RETRIEVE_DEVICES	Failed to retrieve devices. Failed to find all managed devices on BIG-IQ Security.
COMPLETED_CHECK_DMA	Verified that the process of declaring management authority (DMA) is not currently running. The deployment process cannot run if DMA is running.
FAILED_CHECK_DMA	Verified that the process of DMA is currently running. The deployment process cannot run at the same time.

STARTED_REFRESH_CONFIG	Refresh of the current configuration for all devices included in deployment has started. This process pulls in any new configuration items from the BIG-IP® device in to the current configuration.
COMPLETED_REFRESH_CONFIG	Refresh of the current configuration for all devices included in deployment has started has completed. This process pulls in any new configuration items from the BIG-IP device in to the current configuration.
FAILED_REFRESH_CONFIG	Refresh of the BIG-IQ Security current configuration has failed. This refresh pulls in any new configuration items from the BIG-IP device in to the current configuration.
STARTED_SNAPSHOT	Snapshot of the working configuration has started.
COMPLETED_SNAPSHOT	Snapshot of the working configuration has completed.
FAILED_SNAPSHOT	Snapshot of the working configuration has failed.
START_DIFFERENCE	Preparing to start the process of enumerating differences between the snapshot taken and the current configuration.
STARTED_DIFFERENCE	Generating the differences between the snapshot taken and the current configuration has started.
COMPLETED_DIFFERENCE	The process of enumerating differences between the snapshot taken and the current configuration has completed.
FAILED_DIFFERENCE	The process of enumerating differences between the snapshot taken and the current configuration has failed.
STARTED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has started. This state transforms the difference data into a form that can be distributed.
COMPLETED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has completed. This state transforms the difference data into a form that can be distributed.
FAILED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has failed. This state transforms the difference data into a form that can be distributed.
START_DISTRIBUTION	Preparing to start the distribution process.
STARTED_DISTRIBUTION	The process of distributing configuration changes to specified devices has started.
FAILED_DISTRIBUTION	The process of distributing configuration changes has failed.
COMPLETED	The deployment process has completed.

Chapter 9

Managing Audit Logs

About the audit logs and the viewer

In large customer environments, multiple users make changes to security policies. These policy changes occur in a central location (the BIG-IQ™ Network Security database) not on individual BIG-IP® Advanced Firewall Manager™ (AFM™) devices.

BIG-IQ Network Security records every policy change (every configuration change to a working-configuration object) in the firewall audit log. A change is defined as: object created, object deleted, object modified. Thus, the audit log is an important tool for debugging and tracking changes to firewall devices.

To address these concerns, BIG-IQ Network Security provides an audit log that records all security traffic (users, times, events, and so on). Users who can access the BIG-IQ Network Security console (shell) have access to this file.

The audit log viewer retrieves entries from this database for display in the GUI.

In addition, all API traffic on the BIG-IQ system, every REST service command for all licensed modules, is logged in a central audit log (`restjavad-audit.n.log`).

Managing the audit log

You can review audit log contents periodically and archive contents locally for off-device processing, troubleshooting, and future reference.

In high-availability (HA) configurations, each node maintains its own audit log. Entries are synced after the HA configuration is set. If you have entries on the primary node and then configure HA, the previously-generated entries on the primary will not be replicated to the standby node; new entries will be replicated.

All deletions, whether performed manually through the Audit Log viewer or performed as part of a delete and archive operation, are not deleted on the standby node.

Also, archives are configured separately on each node.

Changes to the following working-configuration objects generate log entries:

- Firewalls
- Policies
- Rule lists
- Address lists
- Port lists
- Schedules
- Snapshots

The following actions also generate log entries:

- Add/edit BIG-IQ Network Security system roles. Tracking role modification provides auditing for the assignment of users to roles.
- Create/cancel device discovery and reimport.
- Delete previously-discovered device.
- Create/delete deployment task.
- Create difference task.
- Create/delete snapshot.
- Edit of system information (such as host name and internal self IP).

1. To examine audit logs using SSH, log in to the BIG-IQ Network Security device with Administrator or Security_Manager credentials.
2. Navigate to the audit log location: `/var/log/audit`.
3. Examine files with the naming convention: `audit.n.txt`.

   where **n** is the log number.
4. Once located, you can view or save the log locally through a method of your choice.

About the firewall audit log viewer

The Audit Log viewer retrieves entries from the audit log for display in the BIG-IQ™ Network Security GUI.

Note: *The Audit Log viewer is not updated dynamically. You must refresh the page to get new entries.*

All BIG-IQ system roles have read-only access and can view entries. Only users with the role of Administrator or Security_Manager can delete entries or modify configuration settings.

Viewing differences in the audit log viewer

Use the built-in firewall audit log viewer provided in BIG-IQ™ Network Security to examine differences between entries listed in the viewer. If differences are not found, a message is displayed.

1. Log in to the BIG-IQ Network Security system with Administrator or Security_Manager credentials.
2. To display the viewer, click the **Audit Logs** link in the black banner.
3. To display differences between object generations, click an object in the Object Name column. The Difference Viewer appears. Areas of differences are highlighted in gold. Additions to a generation are highlighted in green. Textual JSON appears for each difference found.
4. When finished, click **Close**.

Filtering entries in the audit log viewer

The Filter field at the top of the Audit Logs page enables you to rapidly narrow the scope displayed in the viewer and more easily locate an entry in the audit log. Filtering is text-based. Filtering is not case-sensitive. To clear the filter, click the **X** at the end of the search string under the Filter field. All BIG-IQ™ system roles have read-only access to the audit log and can filter entries.

1. Log in to BIG-IQ Network Security.
2. Click the **Audit Logs** link in the black banner under **Firewall**.
3. Note that you can use wild cards in all filtering operations. To filter on the:

Option	Description
Client IP	Enter the client IP address in the filter. Note that when a task is not initiated by a user, the entry in the Client IP column is blank.

Option	Description
Time (mix of letters and numbers)	Enter a date/time in any of the following formats: • mmm dd yyyy hh:mm:ss. Example: Jan 7 2014 8:30:00 • ddd mmm dd yyyy hh:mm. Example: Thu Jan 16 2014 11:01 • ddd mmm dd yyyy hh:mm:ss. Example: Thu Jan 16 2014 11:13:50 Formats are highly browser-dependent. Other formats might appear to filter successfully but are not supported. You must enter both a date and a time. Entering a single date/time results in a filter displaying all entries from the specified date/time to the current date/time. To filter on a range of times, enter the dates/times in one of the supported formats, separated by a hyphen. Example: jan 21 2014 11:04-jan 21 2014 11:05.
Time (numbers only)	Enter a date/time in any of the following formats: • m/d hh:mm:ss. Example: 1/1 12:14:15 • mm/dd hh:mm:ss. Example: 01/01 12:14:15 • m/d hh:mm. Example: 1/1 12:14 • m/d h:mm. Example: 1/1 2:14 • mm/dd hh:mm. Example: 01/01 12:14 • mm/dd/yy hh:mm:ss. Example: 01/01 12:14:15 • m/d/yy hh:mm:ss. Example: 1/1/14 12:14:15 • mm/dd/yy hh:mm. Example: 01/01/14 12:14 • m/d/yy hh:mm. Example: 1/1/14 12:14 • mm/dd/yyyy hh:mm:ss. Example: 1/1/2014 12:14:15 You must enter both a date and a time. Entering a single date/time results in a filter displaying all entries from the specified date/time to the current date/time. To filter on a range of times, enter the dates/times in one of the supported formats, separated by a hyphen. Example: 1/1 12:14:15-1/1 12:14:18.
Node	Enter the node name in the filter.
User	Enter the user in the filter.
Object Name	Enter the name of the object in the filter. If a partition name is displayed, do not include it in the filter. For example, *Common/AddressList_4* would be entered as *AddressList_4*. Note that entries in the Object Name column are links to the JSON representing the object. If the object does not have a name, the system places a dash in the column. The dash is also a link to the JSON.
Type	Enter the type in the filter. Note that *WC* stands for *working configuration*.
Action	Enter the action in the filter.
Version	Enter the version number in the filter.

4. Click **Apply**.

The result of a filter (or search) operation is a set of entries that match the filter criteria, sorted by time.

Deleting entries in the audit log viewer

All BIG-IQ™ system roles have read-only access to the audit log and can view entries. Security users with a role of either Administrator or Security_Manager can also delete entries.

There is no set limit on the number of entries that the viewer can display although the viewer will not display archived entries. You can prune entries to constrain the list to relevant data and a manageable size. Use the scroll bar to the right to scroll through entries.

Note: *Exercise care when deleting entries. Once deleted, entries cannot be retrieved.*

1. Log in to BIG-IQ Network Security with Administrator or Security_Manager credentials.
2. To view the audit log, click the **Audit Logs** link in the black banner under **Firewall**.
3. To delete:

Option	Description
A single entry	Select the check box for the entry you want to delete and then click **Remove**. You will not receive a confirmation dialog box.
All entries stored on this BIG-IQ system	Select the check box in the header row and then click **Remove**. In the confirmation dialog box, click **Yes** to confirm that you want to delete all entries. Note that this action removes all entries, not just those visible in the viewer page.
Multiple entries	Combine selecting with the Shift key, and then click **Remove**. You will not receive a confirmation dialog box.
A filtered batch of entries	Type a text string in the Filter field at the top of the page and click **Apply**. The result after applying the filter is a batched set of entries that match the criteria. Select the check box at the top of the table in the header row and click **Remove**. The batch of entries is removed. Note that if you delete a large batch of entries the operation may take some time if the system has a lot of entries. Also, you must keep the Audit Logs viewer open the entire time.

Firewall audit log entry properties

The firewall audit log viewer displays the following properties for each entry.

Event	Description
Client IP	IP address for the BIG-IQ system.
Time	User-friendly timeline of all changes, as well as tasks that were started and canceled. Time is preserved in UTC, but the GUI displays the time in the user's local time zone.
Node	FQDN for the BIG-IQ system that recorded the event.
User	User who initiated the action.

Event	Description
Object Name	Object identified by a user-friendly name; for example: newRule1, deploy-test, or Common/global. This entry is also a link; when activated, it shows the JSON for the object.
Type	Class or group of the object modified.
Action	Type of modification (New, Delete, or Update).
Version	Number of times the system generated the object.

Firewall audit log archival settings

The firewall Audit Logs viewer enables the following configuring settings to enable archiving audit log entries. In a high-availability (HA) configuration, audit log archives are replicated between BIG-IQ™ Network Security HA nodes. However, you can configure the archival settings separately on each node.

Setting	Description
Days to keep entries	Default is 30 days. The field must contain an integer between 1 and 366.
Check expiration at this time	Contains the hour and minute when expirations on entries will be checked. You can enter the hour and the minute manually (in the format hh:mm). Or, you can click in the field to view and edit in the Choose Time dialog box. Adjust the Hour and Minute sliders to reflect the desired hour and minute and the click **Done**.
When entries expire	Controls whether entries are deleted from the audit log when they expire or deleted from the audit log but archived to the audit log archive. Select **Delete** to delete the entry. (This action is permanent; you cannot get a deleted entry back.) Select **Delete and Archive** to delete the entry but archive it for future reference. Expired entries are saved to a predefined file at /var/log/firewall/archive-audit.0.txt.
Next run time	Informational, read-only setting, indicating the next time entries will be archived. Run time is expressed in the format: ddd mmm yyyy hh:mm:ss. Example: Tue Jan 28 2014 02:50:00.
Last run time	Informational, read-only setting, indicating the last time entries were archived. Run time is expressed in the format: ddd mmm yyyy hh:mm:ss. Example: Tue Jan 28 2014 02:50:00.
Last Error	Informational, read-only setting. The field contains the text *No error* or the error text for any errors found.
Last Error Time	Informational, read-only setting. Time in the field is expressed in the format: ddd mmm yyyy hh:mm:ss Example: Fri Jan 17 2014 23:50:00.

About the REST API audit log

The REST API audit log records all API traffic on the BIG-IQ™ system. It logs every REST service command for all licensed modules in a central audit log (`restjavad-audit.n.log`) located on the system.

Note: *The current iteration of the log is named* `restjavad-audit.0.log`*. When the log reaches a certain user-configured size, a new log is created and the number is incremented. You can configure and edit settings in* `/etc/restjavad.log.conf`*.*

Any user who can access the BIG-IQ Network Security console (shell) has access to this file.

Managing the REST API audit log

The REST API audit log contains an entry for every REST API command processed by the BIG-IQ™ system and is an essential source of information about the modules licensed under your BIG-IQ Network Security system. It can provide assistance in compliance, troubleshooting, and record-keeping. Use it to review log contents periodically, and to save contents locally for off-device processing and archiving.

1. Using SSH, log in to the BIG-IQ Network Security device with administrator credentials.
2. Navigate to the restjavad log location: `/var/log`.
3. Examine files with the naming convention: `restjavad-audit.n.log`.

   where **n** is the log number.
4. Once located, you can view or save the log locally through a method of your choice.

Chapter 10

Required BIG-IQ System Components

Installing required BIG-IQ system components

Installing BIG-IQ™ system components on a BIG-IP® device requires a licensed BIG-IP device running version 11.3 or later.

Certain BIG-IQ system components must be installed on all BIG-IP devices that are to be brought under central management. These required components provide a REST framework on the BIG-IP devices. To install these components manually, run the commands from the command line.

Important: *When running this installation script, the traffic management interface (TMM) on each BIG-IP device restarts. Therefore, before running this script, verify that no critical network traffic is targeted to the BIG-IP devices.*

---

1. Log in to the BIG-IQ system as the root user.
2. Establish SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-copy-id root@<BIG-IP Management IP Address>`

   This step is optional. However, if you do not establish trust, you will be required to provide the BIG-IP system's root password multiple times.
3. Navigate to the folder in which the required files reside:
   `cd /usr/lib/dco/packages/upd-adc`
4. Run the installation script:

   `./update_bigip.sh –a admin –p <password> <BIG-IP Management IP Address>`

   Where `<password>` is the administrator password for the BIG-IP device.
5. Revoke SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-keygen –R <BIG-IP Management IP address>`

   This step is not required if you did not establish trust in step 2.

Installing these BIG-IQ components results in a REST framework that supports the required Java-based management services.

Index

G

H

L

M

N

P

R

S

T

U

V

W