

BIG-IQ™ Web Application Security Administration

Version 4.3



Table of Contents

Legal Notices.....	5
Acknowledgments.....	7
 Chapter 1: Understanding BIG-IQ Web Application Security.....	 13
Overview: BIG-IQ Web Application Security.....	14
About BIG-IQ roles.....	14
About BIG-IQ users.....	14
Creating users.....	15
Associating users with roles.....	15
Disassociating users from roles.....	15
 Chapter 2: Device Management.....	 17
Overview: BIG-IQ device management.....	18
Discovering devices.....	18
Monitoring device health and performance.....	19
Displaying policy properties.....	19
Device properties.....	19
About rediscovering devices.....	20
Rediscovering devices.....	20
Removing devices.....	21
 Chapter 3: Security Policies.....	 23
About viewing ASM security policies with BIG-IQ	24
Displaying security policy properties.....	24
Reimporting security policies.....	24
Exporting security policies using BIG-IQ.....	25
Removing security policies with BIG-IQ.....	25
 Chapter 4: Signature Files.....	 27
About signature files.....	28
Updating signature files.....	28
Updating and pushing signature files	28
Viewing signature file properties.....	28
Signature file properties.....	29
 Chapter 5: Virtual Servers.....	 31
About virtual servers in BIG-IQ Web Application Security.....	32
Displaying virtual server properties.....	32
Changing virtual servers.....	33

Removing links between virtual servers and policies.....	33
Chapter 6: Deployment.....	35
About BIG-IQ Web Application Security deployments.....	36
Adding deployments.....	36
Managing deployments.....	37
Chapter 7: Audit Log.....	39
About the audit log.....	40
Audit log properties.....	40
Managing the audit log using SSH.....	40
Managing the audit log using the GUI.....	41

Legal Notices

Publication Date

This document was published on February 21, 2014.

Publication Number

MAN-0510-01

Copyright

Copyright © 2014, F5 Networks, Inc. All rights reserved.

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

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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

Patents

This product may be protected by one or more patents indicated at:

<http://www.f5.com/about/guidelines-policies/patents>

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

This product includes cryptographic software written by Eric Young (ey@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.oracle.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 the 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://jaserverfaces.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 jsdiff 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

Understanding BIG-IQ Web Application Security

- *Overview: BIG-IQ Web Application Security*
 - *About BIG-IQ roles*
 - *About BIG-IQ users*
-

Overview: BIG-IQ Web Application Security

BIG-IQ™ Web Application Security enables enterprise-wide management and configuration of multiple BIG-IP® devices from a central management platform. You can centrally manage BIG-IP devices and security policies, and import policies from files on those devices.

For each device discovered, an additional virtual server is created to hold all security policies that are not related to any virtual server on the device. To deploy a policy to a device, the policy must be attached to one of the device's virtual servers. Policies can be deployed to a device that already has the policy by overwriting it. If the policy does not yet exist on the device, you have the option to deploy it as a new policy attached to an available virtual server or as an inactive policy.

From this central management platform, you can perform the following actions through a REST API:

- Import ASM policies from files.
- Import ASM policies from discovered devices.
- Distribute policies to devices.
- Export policies, including an option to export policy files in XML format.

About BIG-IQ roles

Different users have different responsibilities. Therefore, system administrators need a way to differentiate between users to limit user privileges based on those responsibilities.

To assist administrators with this, the BIG-IQ™ Web Application Security module provides these default roles:

Administrator

This role has access to all BIG-IQ modules, including Web Application Security.

ASM_Manager

This role has administrator-level rights for the BIG-IQ Web Application Security module only.

Roles persist and are available after a BIG-IQ system failover. You can associate multiple roles with a given user.

About BIG-IQ users

BIG-IQ™ Web Application Security provides these default users:

admin

This user can assign roles to users, but cannot access the command shell or system console.

root

This user can access the system console.

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

Creating users

By creating users and managing user roles, you place controls on specific functions (view, edit, and deploy).

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 specific 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. Alternatively, if you select the user, the BIG-IQ™ system highlights the roles associated with that user.

Disassociating users from roles

To disable a user's ability to perform a given function, disassociate the role (set 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 disassociated from the role and no longer has the privileges associated with the role.

Chapter

2

Device Management

- *Overview: BIG-IQ device management*
 - *Discovering devices*
 - *Monitoring device health and performance*
 - *Displaying policy properties*
 - *About rediscovering devices*
 - *Removing devices*
-

Overview: BIG-IQ device management

The process of designating a device for central management by BIG-IQ™ Web Application Security is known as discovery.

Once a BIG-IP device is discovered, all security policies and virtual servers on the device come under management by the BIG-IQ system.

For each device discovered, the system creates an extra virtual server to hold all policies not related to any virtual server in the discovered device.

After discovery, BIG-IQ Web Application Security enables a view of devices and properties, policies, and virtual servers associated with those devices and a way to perform device-specific and policy-specific actions.

To view all devices managed by BIG-IQ Web Application Security, navigate to the Devices panel.

Discovering devices

Before discovering one or more BIG-IP® devices, required BIG-IQ™ components must be installed and kept up-to-date on those BIG-IP devices.

Once a device is under central management, information about the device and objects stored on the device are located in the BIG-IQ database, which is the authoritative source for all configuration objects.

Note: Do not manage the BIG-IP device locally. If you make changes locally, you (or another Administrator) might overwrite those changes when performing a deployment from the BIG-IQ system.

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.

User Name	Enter the user's login name. For example: admin.
------------------	--

Password	Enter the password for this user.
-----------------	-----------------------------------

Auto Update Framework	Select this check box to force an update of the REST framework on the BIG-IP device.
------------------------------	--

Certain BIG-IQ system components should be installed and kept up-to-date on all BIG-IP devices brought under central management. These components

Option	Description
	provide a REST framework that supports the required Java-based management services.
Check box	Clear this check box (the default setting) to ensure that the discovery process does not overwrite the source of imported policies already on the BIG-IQ system.

4. Click **Add**.

After discovery, the BIG-IP device is listed in the Devices panel by its FQDN and internal self IP address.

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.

Displaying policy properties

With BIG-IQ™ Web Application Security, you can easily view 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 check box options.

Device properties	Description
Host Name	Fully-qualified domain name (FQDN), identified at discovery time.
Management Address	Management address of the BIG-IP® device, used for communication between it and the BIG-IQ™ system.
Product	Product identification.
Version	Version and hotfix level of the device under management.
Status	Active/Inactive.
Check box	Used during discovery or rediscovery processes to allow (or prevent) the overwriting of imported policies that already exist on BIG-IQ Web Application Security.

Signature file properties	Description
Version	Device current signature file version.
Auto update enabled	Check box used to enable automatic Update & push for signature files.

About rediscovering devices

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

However, some scenarios that might require rediscovery include:

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

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

The rediscovery process is modal. This means that once rediscovery starts, the process blocks you from performing any other tasks or interacting with BIG-IQ Web Application Security in any way until the process completes or is canceled.

Rediscovering devices

If configurations fall out of sync between BIG-IQ™ Web Application Security and managed BIG-IP® devices, you can rediscover devices to bring the systems back into sync.

1. To begin the rediscovery process, navigate to the Devices panel.
2. Hover in the header for the device you want to rediscover, and then click the **gear** icon to display the expanded panel containing device properties and actions.
You cannot change any properties displayed on this screen.
3. In the expanded panel, click **Rediscover**.
During rediscovery, a **Cancel Task** button appears in the dialog box after the task has identified the device and started importing policies. If you click **Cancel Task**, the import is canceled and management authority over the device is rescinded.

You have completely removed the BIG-IP device and all related entities (policies and virtual servers) and rediscovered the device.

If a policy has identified the device being rediscovered as its source, the policy source type is changed to FILE, which means that the device retains the policy's source file and it can be deployed to other devices.

Removing devices

BIG-IQ™ Web Application Security provides a way to rescind management authority (RMA) over BIG-IP® devices. RMA removes the device and all related entities from the BIG-IQ database.

1. To begin the removal process, navigate to the Devices panel.
2. Hover in the Devices header and click the **gear** icon to display the expanded Properties panel.
3. In the expanded Properties panel, click **Remove**.

The BIG-IP device and all related entities (security policies and virtual servers) are removed from the BIG-IQ system and the BIG-IP device can be managed locally.

Chapter

3

Security Policies

- *About viewing ASM security policies with BIG-IQ*

About viewing ASM security policies with BIG-IQ

To view ASM™ security policies that BIG-IQ™ Web Application Security has imported from discovered BIG-IP® devices, navigate to the Policies panel. Each policy is assigned a unique identifier that it carries across the enterprise. This ensures that each policy is shown only once in the Policies panel no matter how many devices it exists in.

In the BIG-IQ Web Application Security repository, policies are in XML format.

Displaying security policy properties

With BIG-IQ™ Web Application Security, you can easily view the properties of individual security policies.

1. Navigate to the Policies panel.
2. Hover over the header for the specific policy, and click the **gear** icon to display the expanded panel containing properties and actions.

Policy properties

Policy properties are read-only and displayed for informational purposes only.

Property	Description
Name	Name of the policy.
Full Path	Full path, including partition, to the policy on the BIG-IP® device.
Description	Optional description for the policy.
Last Updated At	FQDN for the BIG-IP device where the policy was last updated.
Last Updated Time	Time the policy was last updated in YYYY-MM-DDTHH:MM:SSZ format. Example: 2013-11-14T16:16:03Z.
Last Policy Name	Policy name, including partition.
Source Device	FQDN and self IP address for the BIG-IP device where the policy is located.

Reimporting security policies

If security policies fall out of sync between BIG-IQ™ Web Application Security and the policy sources on managed BIG-IP® devices, you can reimport policies to bring them back into sync.

1. Navigate to the Policies panel.
2. Hover over the banner for the policy you want to reimport, and click the **gear** icon to display the expanded panel containing properties and actions.
3. Click the **Reimport from Device** button to the right of the **Source Device** field.

This action is not available if the policy source is a file. In such cases, click **Change Source** to change the **Source Device** field to list devices containing the specified policy.

Exporting security policies using BIG-IQ

Use BIG-IQ™ Web Application Security to export security policies (download the policy XML file) from the module to an application or to a user-designated location.

1. Navigate to the Policies panel.
2. Hover over the banner for the policy you want to export, and click the **gear** icon to display the expanded panel containing properties and actions.
3. Click the **Export** button at the top of the panel.
4. In the dialog box, select either **Open with** and select an application from the drop-down menu, or **Save File** and provide a location.
5. Click **Save**.

Removing security policies with BIG-IQ

BIG-IQ™ Web Application Security provides a way to remove ASM™ security policies from the BIG-IQ database.

1. Navigate to the Policies panel.
2. Hover over the banner for the policy you want to remove, and click the **gear** icon to display the expanded panel containing properties and actions.
3. Click the **Remove** button at the top of the expanded panel.

After removal, you will not receive a confirmation dialog box.

Security policies are removed from the BIG-IQ system and security policies can be managed locally.

Chapter

4

Signature Files

- *About signature files*
 - *Updating signature files*
 - *Updating and pushing signature files*
 - *Viewing signature file properties*
-

About signature files

The Signature files panel in BIG-IQ™ Web Application Security lists the signature files for each discovered BIG-IP® device, and enables you to view the properties for these files.

Currently, Administrators can manage signature files for one BIG-IP device from the BIG-IP Configuration Utility. Through BIG-IQ Web Application Security, however, signature files and signature file updates for multiple devices can be centrally managed from the BIG-IQ platform.

Managing signatures from the BIG-IQ platform enables the administrator to spend less time on signature updates.

Note: This feature is available to users with the Administrator role or the Security_Manager role.

Updating signature files

Use the BIG-IQ™ Web Application Security Signature files panel to update signatures.

1. Log in with Administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.
3. Hover over the panel header, and then click the **gear** icon to expand and display the Update settings.
4. Use the **Interval** drop-down list to modify settings for scheduling updates.
5. Edit the Current running task settings as needed. Click the **Update & push** button to update the signature files and push them to the server.
6. When finished, click **Save** to update all signatures or **Cancel** to close the panel without saving your edits.

Updating and pushing signature files

Use the BIG-IQ™ Web Application Security Signature files panel to begin the process for updating and pushing the signature files.

1. Log in with Administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.
3. Hover over the panel header, and then click the **gear** icon to expand and display the update settings.
4. Under Current running task, for the **Run now** setting, click the **Update & push** button.

The update process begins immediately.

Viewing signature file properties

Use the BIG-IQ™ Web Application Security Signature files panel to expand and view signature file properties.

1. Log in with administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.
3. Hover over a specific signature file, and then click the **gear** icon to expand and display the panel containing property details.
4. When finished, click **Cancel**.

Signature file properties

Signature file properties are read-only and displayed for informational purposes only.

Property	Description
Name	Name of the signature file. Example: Sig_vanc_1
File version	Example: 20131103_042020
Product version	Version on the BIG-IP® device.

Chapter

5

Virtual Servers

- *About virtual servers in BIG-IQ Web Application Security*
-

About virtual servers in BIG-IQ Web Application Security

Through the Virtual Servers panel, BIG-IQ™ Web Application Security displays the virtual servers on each discovered BIG-IP® device and enables you to view the properties for these virtual servers.

For each device discovered, the BIG-IQ system creates an extra virtual server to hold all security policies not related to any virtual server in the discovered device.

Displaying virtual server properties

With BIG-IQ™ Web Application Security, you can easily view virtual server properties.

1. To display properties for an individual virtual server, hover over the header for that virtual server (in the Virtual Servers panel).
2. Click the **gear** icon to expand and display the panel containing virtual server properties.
Properties are read-only. The only actions you can take in the expanded panel concern the attached policies.

Option	Description
Name	Name of the virtual server.
Full Path	Path, including partition, to the virtual server.
IP Address	Self IP address of the BIG-IP® device.
Is Inactive Policies Holder	Yes/No.
Device	FQDN of the BIG-IP device.
Attached Policies	Remove/Change.

Virtual server properties

Virtual server properties are read-only and displayed for informational purposes only.

Property	Description
Name	Name of the virtual server.
Full Path	Full path, including partition, to the virtual server on the BIG-IP® device.
Description	Optional description of the virtual server.
IP Address	Self IP address of the BIG-IP device.
Is Inactive Policies Holder	Yes/No.
Device	FQDN of the BIG-IP device.
Attached Policies	Remove/Change/Add attached policies.

Changing virtual servers

Use the BIG-IQ™ Web Application Security Virtual Server expanded panel to add policies to a virtual server or remove policies from the virtual server they are attached to. You can change the virtual server a given policy is attached to.

Note: *You can add but not remove or change security policies to an inactive virtual server. You can add security policies (instead of replace them) to an active virtual server only if it does not have a security policy already.*

1. To begin the process, navigate to the Virtual Servers panel.
2. Hover in the Virtual Servers header and click the **gear** icon to display the expanded Properties panel.
3. In the expanded panel to the right of **Attached Policies**, click **Change**.
4. In the Modal dialog box, select the policies you want to add to the current virtual server and click **Add**.

The selected policies are added to or changed from the current virtual server.

Removing links between virtual servers and policies

You can use BIG-IQ™ Web Application Security to remove the link between a virtual server and a policy.

1. To begin the process, navigate to the Virtual Servers panel.
2. Hover in the Virtual Servers header and click the **gear** icon to display the expanded Properties panel.
3. In the expanded Properties panel, click **Remove**.

The link between the policy and the virtual server is deleted. This means that if the policy is attached to the virtual server on the remote BIG-IP® device, the link between them is deleted during the deployment process.

Chapter 6

Deployment

- *About BIG-IQ Web Application Security deployments*
-

About BIG-IQ Web Application Security deployments

The BIG-IQ™ Web Application Security system displays individual deployments and their status (one action per row in the Deployment panel). To distribute policies to selected BIG-IP® devices, create deployments from the Deployment panel.

You can deploy security policies to a device that already has the policy by overwriting the existing security policy. If the security policy does not yet exist on the device, you can deploy it as a new policy attached to an available virtual server or you can deploy it as an inactive policy.

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

During the evaluation process, BIG-IQ Web Application 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.

During the distribution phase, security policies are pushed out to remote BIG-IP devices. Any changes made locally to the BIG-IP device are overwritten.

Adding deployments

When you have completed edits to a policy, you can create a deployment to push changes from BIG-IQ™ Web Application Security to a target 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 New 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.
Select Devices to Evaluate	Available devices are listed to the right of the field. Select or clear check boxes as appropriate.

4. Click **Evaluate** to evaluate differences between the working configuration (BIG-IQ™ Web Application Security) and the configuration on the BIG-IP® device.

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.

Managing deployments

Distribute changes from BIG-IQ™ Web Application Security to managed BIG-IP® devices when a deployment displays a status of READY TO DEPLOY. 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.
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
Available Devices	List of BIG-IP® devices that can be selected for deployment.

3. Click **View Diffs** to view differences between the configuration on BIG-IQ™ Web Application Security and the BIG-IP device.

A dialog box appears displaying the differences. The display shows four columns: Type (type of entity changed), Change (add, modify, remove), On BIG-IQ (name of the entity on BIG-IQ Web Application Security), and On BIG-IP (name of the entity on the BIG-IP® device).

4. When ready to deploy, click **Deploy** to push changes to the selected BIG-IP device.

Deployment states are reflected at the top of the expanded panel. At the end of the deployment process, changes are distributed to the selected BIG-IP device.

Chapter 7

Audit Log

- *About the audit log*
 - *Audit log properties*
 - *Managing the audit log using SSH*
 - *Managing the audit log using the GUI*
-

About the audit log

In large customer environments, multiple users make changes to security policies. These policy changes occur in a central location, such as the BIG-IQ™ Web Application Security database, and not on individual BIG-IP® ASM™ devices. To address possible concerns, the BIG-IQ system provides an audit log that records all traffic (users, times, events, and so on). Users who can access the BIG-IQ console (shell) have access to this file.

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

Note: The audit log viewer retrieves entries from this database to display in the GUI.

Audit log properties

The audit log viewer in BIG-IQ™ Web Application Security displays these properties.

Item	Description
Date	Date of the audit log signature file entry.
Task status	Status for task, such as Passed.
Steps status	Status for each step.
Details	A link that displays details, such as date, sub task, action, status, error/message, and device IP.

Managing the audit log using SSH

You can review audit log contents periodically using SSH 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.

1. To examine audit logs using SSH, log in to the BIG-IQ™ system 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`.
In this example, **n** is the log number.
4. Once located, you can view or save the log locally through a method of your choice.

Managing the audit log using the GUI

You can view audit logs using the GUI.

1. To examine audit logs using the GUI, log in to the BIG-IQ™ system with Administrator or Security_Manager credentials.
2. Under Web Application Security, click **Audit Logs**.
Each entry listed represents the result of a signature file Update & push task.
3. To see the list of steps that occurred for that specific task, click the **Details** link.

Index

A

audit log
 about 40
 managing 40–41
 properties 40

B

BIG-IQ Web Application Security
 about 14

C

creating
 users 15

D

deployment
 about 36
 adding 36
 and configuration changes 36
 managing 37
 ready to deploy 37
 deployment properties 36
 device properties
 displaying 19
 devices
 discovery 18
 properties 19
 rediscovering 20
 removing 21
 discovery
 about 18

F

features
 BIG-IQ Web Application Security 14

H

health
 monitoring 19

M

monitoring
 health and performance 19

P

performance
 monitoring 19

policies
 properties 24
 policy properties
 displaying 24
 properties
 audit log 40
 deployment 36
 devices 19
 policies 24
 signature files 19, 29
 virtual servers 32
 propertiessignature files 28

R

rediscovery
 about 20
 removing devices 21
 removing security policies 25
 removing virtual servers 33
 roles
 about 14
 associating with users 15
 disassociating from users 15

S

security policies
 about 24
 exporting with BIG-IQ 25
 reimporting 24
 removing 25
 signature file properties
 viewing 28
 signature files
 properties 19, 29
 update and push 28
 Signature files panel
 about 28
 using 28

U

update and push
 signature files 28
 updating signature files 28
 users
 about 14
 associating with roles 15
 creating 15
 disassociating from roles 15

V

virtual server properties
 displaying 32

Index

virtual servers
 changing [33](#)
 properties [32](#)
 removing [33](#)

Virtual Servers panel
 about [32](#)