

BIG-IQ[®] System: Licensing and Initial Setup

Version 4.5



Table of Contents

Legal Notices.....	5
Acknowledgments.....	7
 Chapter 1: BIG-IQ System Introduction.....	 15
Overview: BIG-IQ system.....	16
Additional resources and documentation for BIG-IQ systems.....	16
About incorporating BIG-IQ system securely into your network.....	17
Open ports required for device management.....	17
 Chapter 2: BIG-IQ User Interface.....	 19
About the BIG-IQ system user interface.....	20
Filtering for associated objects.....	20
Searching for specific objects.....	20
Customizing panel order.....	20
 Chapter 3: Software Download, Licensing, and Initial Configuration.....	 21
About downloading software, licensing and initial configuration.....	22
Downloading software images.....	22
Installing and upgrading BIG-IQ System software.....	22
Automatic license activation.....	23
Manual license activation.....	23
Defining DNS and NTP servers for the BIG-IQ system.....	24
Changing the default password for the administrator user.....	25
Overview: SNMP and SMTP alerts.....	25
About integrating with SNMP version 1 or 2 for alerts.....	25
Configuring SNMP version 1 or 2 for alerts.....	25
About integrating with SNMP version 3 for alerts.....	26
Configuring SNMP version 3 for alerts.....	26
About integrating with SMTP for alerts.....	27
Specifying alert conditions.....	27
About authentication integration.....	28
Configuring authentication with LDAP.....	28
Configuring authentication with RADIUS.....	30
 Chapter 4: Users, User Groups, and Roles.....	 31
Overview: Users, user groups, and roles.....	32
About default passwords for pre-defined users.....	32
Changing the default password for the administrator user.....	32
Adding a locally-authenticated BIG-IQ user.....	33

About user roles.....	33
Roles definitions.....	33
Associating a user or user group with a role	34
Disassociating a user from a role.....	34
Chapter 5: Additional Network Configuration Options.....	35
About additional network configuration options.....	36
Configuring an additional VLAN.....	36
Chapter 6: BIG-IQ High Availability.....	37
About a high availability active-active cluster.....	38
Configuring BIG-IQ system in an active-active high availability cluster.....	38
Chapter 7: BIG-IQ System Management.....	39
Installing and upgrading BIG-IQ System software.....	40
About UCS files.....	40
Creating a backup UCS file.....	41

Legal Notices

Publication Date

This document was published on January 21, 2015.

Publication Number

MAN-0497-03

Copyright

Copyright © 2015, 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, Application Acceleration Manager, Application Security Manager, APM, 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, iCall, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAC (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Applications Services, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix (except Germany), Traffix [DESIGN] (except Germany), 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.

Acknowledgments

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

This product includes node-static software, copyright © 2010-2014 Alexis Sellier.

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opensv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

This product includes cookies software, copyright © 2014, Jed Schmidt, <http://jed.is/>, and distributed under the MIT license.

This product includes node-fastcgi software, copyright © 2013, Fabio Massaioli, and distributed under the MIT license.

This product includes socket.io software, copyright © 2013, Guillermo Rauch, and distributed under the MIT license.

This product includes node-querystring software, copyright © 2012. Irakli Gozalishvili. All rights reserved.

This product includes TinyRadius software, copyright © 1991, 1999 Free Software Foundation, Inc., and distributed under the GNU Lesser GPL version 2.1 license.

This product includes angular-ui software, which is distributed under the MIT license. Copyright © 2012-2014, AngularUI Team.

This product includes CodeMirror software, which is distributed under the MIT license. Copyright © 2014, Marijn Haverbeke.

This product includes Quartz Scheduler software, which is distributed under the Apache 2.0 license. Copyright © Terracotta, Inc.

Chapter

1

BIG-IQ System Introduction

- *Overview: BIG-IQ system*
- *About incorporating BIG-IQ system securely into your network*

Overview: BIG-IQ system

The BIG-IQ® system is a tool that streamlines the management of F5 devices in your network. Because it is based on the same platform as BIG-IP® devices, it includes full product support, security patches, and internal and external security audits (AuthN and AuthZ checks). The specific functionality offered is dependent on your software license.

Cloud administrators use BIG-IQ Cloud to provide cloud tenants self-service access to shared computing resources such as networks, servers, storage, applications, and services. Cloud resources can be private or public, depending on the customer's requirements. Each tenant has restricted and dedicated access to cloud resources based on a specific user account or tenant role, ensuring that tenants have access only to their own resources. Cloud resources are easily expanded and reallocated as needed, providing flexible resource balancing.

Firewall managers use BIG-IQ Security to manage security firewalls for multiple devices from a central location. Firewall management includes discovering, editing, and deploying firewall configurations, as well as consolidating shared firewall objects. Once a firewall device is designated for central management, it is no longer managed locally unless there is an exceptional need.

Web-Application Security managers also use BIG-IQ Security to centrally manage policy files and attack-signature files. Multiple BIG-IP® devices can share the same policy and attack-signature files for filtering HTTP, HTTPS, and other web traffic for known attack patterns.

Network administrators use BIG-IQ Device to interact with all of the managed F5 devices in their network. This centralized management includes the ability upgrade F5 devices, update configurations, and reallocate licenses as needed.

BIG-IQ Application Delivery Controller (ADC) offers you the flexibility to deploy software images, and configurations, and monitor and distribute licenses and license pools for managed BIG-IP devices.

Additional resources and documentation for BIG-IQ systems

You can access all of the following BIG-IQ® system documentation from the AskF5™ Knowledge Base located at <http://support.f5.com/>.

Document	Description
BIG-IQ® Systems Virtual Editions Setup guides	BIG-IQ® Virtual Edition (VE) runs as a guest in a virtual environment using supported hypervisors. Each of these guides is specific to one of the hypervisor environments supported for the BIG-IQ system.
<i>BIG-IQ® System: Licensing and Initial Setup</i>	This guide provides the network administrators with basic BIG-IQ system concepts and describes the tasks required to license and set up the BIG-IQ system in their network, including how to add users and assign roles to those users.
<i>BIG-IQ® Device: Device Management</i>	This guide provides details about how to deploy software images, licenses, and configurations to managed BIG-IP® devices.
<i>BIG-IQ® Cloud: Cloud Administration</i>	This guide contains information to help a cloud administrator manage cloud resources, devices, applications, and tenants (users).
<i>BIG-IQ® Cloud: Tenant User Guide</i>	This guide contains information to help tenants manage applications.
<i>BIG-IQ® Application Delivery Controller: Administration</i>	This guide provides details about how to centrally manage BIG-IP® Local Traffic Manager™ applications.

Document	Description
<i>BIG-IQ® Security: Administration</i>	This guide contains information used to centrally manage BIG-IP® firewalls, policies, rule lists (as well as other shared objects), and users.
<i>Platform Guide: BIG-IQ® 7000 Series</i>	This guide provides information about setting up and managing the BIG-IQ 7000 hardware platform.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

About incorporating BIG-IQ system securely into your network

To successfully manage devices in your network, including BIG-IQ peer systems, the BIG-IQ system requires communication over HTTPS port 443. The BIG-IQ administrator can provide fine-grained access to various roles, which are verified by authorization checks (AuthN and AuthZ). Authenticated users have access only to the resources explicitly granted by the BIG-IQ administrator. Additional security is provided through bidirectional trust and verification through key and certificate exchange and additional support for LDAP and RADIUS authentication.

Open ports required for device management

The BIG-IQ system requires bilateral communication with the devices in your network in order to successfully manage them. For this communication, the following ports are open by default to allow for the required two-way communication.

Open Port	Purpose
TCP 443 (HTTPS)	Discovering, monitoring, and configuring managed devices
TCP 443 (HTTPS) and TCP 22 (SSH)	Upgrade BIG-IP devices running version 11.3-11.6
TCP 443 (HTTPS)	Upgrade BIG-IP devices running version 12.0
TCP 443 (HTTPS)	Replicating and synchronizing BIG-IQ systems

Chapter 2

BIG-IQ User Interface

- *About the BIG-IQ system user interface*
-

About the BIG-IQ system user interface

The BIG-IQ® system interface is composed of panels. Each panel contains objects that correspond to a BIG-IQ feature. Depending on the number of panels and the resolution of your screen, some panels may be collapsed and show as colored bars on either side of the screen. You can cursor over the collapsed panels to locate the one you want, and click the panel to open. To associate items from different panels, click an object, and drag and drop it onto the object with which you want to associate it.

Filtering for associated objects

The BIG-IQ® system helps you easily see an object's relationship to another object, even if the objects are in different panels.

1. To display only items associated with a specific object, hover over the object, click the gear icon, and then select **Show Only Related Items**.
The screen refreshes to display only associated objects in each panel.
2. To highlight only items associated with a specific object, hover over the object, click the gear icon, and then select **Highlight Related Items**.
The screen refreshes, highlighting only associated objects in each panel, and displaying unassociated objects in a gray font.
3. To remove a filter, click the **X** icon next to the filtered object in a panel.

Searching for specific objects

The BIG-IQ® system interface makes it easy to search for a specific object. This can be especially helpful as the number of objects increase when you add more users, applications, servers, and so forth.

1. To search for a specific object, in the Filter field at the top of the screen, type all or part of an object's name.
2. Click the **Apply** button.
The screen refreshes to display only the objects associated with the term you typed in the Filter field.
3. To further refine the filter, type another term into the Filter field, and click the **Apply** button again.
4. To remove a filter term, click the **X** icon next to it.

Customizing panel order

You can customize the BIG-IQ® system interface by reordering the panels.

1. Click the header of a panel and drag it to a new location, then release the mouse button.
The panel displays in the new location.
2. Repeat step 1 until you are satisfied with the order of the panels.

Chapter

3

Software Download, Licensing, and Initial Configuration

- *About downloading software, licensing and initial configuration*
 - *Overview: SNMP and SMTP alerts*
 - *About authentication integration*
-

About downloading software, licensing and initial configuration

BIG-IQ® system runs as a virtual machine in specifically-supported hypervisors or on the BIG-IQ 7000 series platform. After you set up your virtual environment or your platform, you can download the BIG-IQ software, and then license the BIG-IQ system. You initiate the license activation process with the base registration key.

The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license. If the system has access to the internet, you select an option to automatically contact the F5 license server and activate the license. If the system is not connected to the internet, you can manually retrieve the activation key from a system that is connected to the internet, and transfer it to the BIG-IQ system.

Downloading software images

Download software images for new installations, upgrades, or hot fixes to managed physical and virtual devices with just a few clicks.

1. Browse to the F5 Downloads site, <https://downloads.f5.com>, and locate the image you want to download.
2. Log in to BIG-IQ Device with the administrator user name and password.
3. At the top of the screen, click **Provisioning**.
4. Hover over the Images header, and click the + icon when it appears, and then click **New Software Image**.
5. Click the **Choose File** button and navigate to the shared images directory and click on the software image you want to download to BIG-IQ Device.
The software image appears in the Images panel.

The software image is now available for you to install on a managed device.

Installing and upgrading BIG-IQ System software

Before you perform an initial BIG-IQ® System software installation, or software upgrade, you must perform the following tasks:

- Activate, or reactivate, your current license to ensure that you have a valid service check date.
- Download the ISO file for the upgrade from F5 Downloads to `/shared/images` on BIG-IQ System. If you need to create this directory, use the exact name `/shared/images`.
- For upgrades only, create a backup of the user configuration set (UCS), locate it in the `/var/local/ucs` directory on the source installation location, and copy the UCS file to another system for safe keeping.

Use this procedure when you are ready to perform an initial BIG-IQ System software installation or upgrade a to a more recent software version.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, expand **Management Group** or **HA Peer Group** by clicking the arrow next to it.
4. Click the gear icon next to **localhost**, and then click **Properties**.

5. Click **Software Update**.
6. Click the **Update** button.
7. From the **Software Image** list, select the new image or browse to the location to which you saved it.
8. From the **Install Location** list, select the volume to which you want to install the image.
9. For the **Options** setting, select one:
 - To automatically reboot the BIG-IQ System to the specified volume immediately after the software is installed, select **Reboot after Live Install**.
 - To manually reboot the BIG-IQ System at another time from the **System > Properties** screen, select **Set Default Boot Location**.
10. Click the **Apply** button.

BIG-IQ System installs the selected software. For upgrades, BIG-IQ System also rolls forward the UCS file.

Automatic license activation

You must have a base registration key to license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the BIG-IQ® system is connected to the public internet, you can use this procedure to activate its license.

1. Using a browser on which you have configured the management interface, type
`https://<varname><management_IP_address><varname>where <management_IP_address>`
 is the address you specified for device management.
 This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.
 The License Agreement displays.
6. To accept the License Agreement, click the **Agree** button.
7. Click **User Administration**.
8. In the **Old Password** fields, type the default admin and root passwords, and then type a new password in the **Password** and **Confirm Password** fields.
9. Click **Properties**.
10. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.
 The FQDN can consist of letters and numbers, as well as the characters underscore (`_`), dash (`-`), or period (`.`).
11. Click the **Save** button to save your configuration.

Manual license activation

You must have a base registration key to license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the BIG-IQ® system is not connected to the public internet, this procedure can activate its license.

1. Using a browser on which you have configured the management interface, type `https://<varname><management_IP_address><varname>` where `<management_IP_address>` is the address you specified for device management.
This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
6. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.
Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
7. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
8. To accept the License Agreement, click the **Agree** button.
9. Click **User Administration**.
10. In the **Old Password** fields, type the default admin and root passwords, and then type a new password in the **Password** and **Confirm Password** fields.
11. Click **Properties**.
12. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.
The FQDN can consist of letters and numbers, as well as the characters underscore (`_`), dash (`-`), or period (`.`).
13. Click the **Save** button to save your configuration.

Defining DNS and NTP servers for the BIG-IQ system

After you license the BIG-IQ[®] system, you can specify the DNS and NTP servers.

Setting your DNS server and domain allows the BIG-IQ system to properly parse IP addresses. Defining the NTP server ensures that the BIG-IQ system's clock is synchronized with Coordinated Universal Time (UTC).

1. Log in to BIG-IQ System with your administrator user name and password.
2. On the BIG-IQ Systems panel, click the gear icon next to the group name for which you want to define the DNS and NTP servers, and then click **Properties**.
3. Click **Services**.
4. In the **DNS Lookup Servers** field, type the IP address of your DNS server.
5. In the **DNS Search Domains** field, type the name of your search domain.
The DNS search domain list allows the BIG-IQ system to search for local domain lookups to resolve local host names.
6. In the **Time Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.
7. Click the **Save** button to save your configuration.

Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system to automatically create the administrator user.

After you initially license and configure the BIG-IQ system, it is important to change the administrator role password from the default, `admin`.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, for **Admin User**, click the gear icon and then **Properties**.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click the **Add** button.

Overview: SNMP and SMTP alerts

You can easily manage the health of your network by configuring the BIG-IQ® system to alert you when specific events occur for your managed devices. You can receive notifications by having the BIG-IQ system send traps to your SNMP manager and you can also configure the BIG-IQ system to send alerts for certain events to a specified individual. SNMP is an industry standard protocol for monitoring devices on IP networks. BIG-IQ Device integrates easily with your SNMP manager, allowing you to centrally manage collected data. Once configured, the SNMP agent sends data collected from BIG-IQ Device to your third-party SNMP manager. BIG-IQ Device is compatible with SNMPv1, SNMPv2c, and SNMPv3. Additionally, you can specify SNMP events to also trigger SMTP alerts.

About integrating with SNMP version 1 or 2 for alerts

To prepare BIG-IQ® Device to interface with your SNMP version 1 or 2 manager, you must do three things, all accomplished in one task.

- Configure SNMP agent
- Configure SNMP access
- Create an SNMP trap destination

Configuring SNMP version 1 or 2 for alerts

You configure the SNMP agent and provide specific access to BIG-IQ® Device so that the SNMP manager can collect data.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. In the BIG-IQ Systems panel, click the gear icon next to the HA Peer Group you are configuring, and then click **Properties**.
4. Click **SNMP Config**.
The screen displays the SNMP Agent Properties settings.

5. In the **Contact Information** field, type the name and email address of the person who is responsible for SNMP administration, and in the **Machine Location** field, type the location of the SNMP manager system.
These details are for informational purposes only, and have no impact on how BIG-IQ Device interfaces with your SNMP manager.
6. To download the F5-specific MIBs, click the **Download MIB** link.
7. In the **Addresses/Networks** fields, type the IP address and networks (and the netmask if applicable) that the SNMP manager is allowed to access.
8. To add another address, click the plus (+) sign.
9. Click the **Save** button located at the top of the panel.
10. Click the **Access** tab.
The SNMP Access settings display.
11. In the New v1/v2 Access Records section, from the **Type** list, select the appropriate protocol for the SNMP manager's IP address.
12. In the **Community** field, type the name of the associated community.
13. Click the **Traps** tab.
14. In the New v1/v2c Destinations section, from the **Version** list, select the version of SNMP you are using.
15. In the **Community**, **Destination**, and **Port** fields, type, respectively, the community name, IP address, and port for the trap destination.
16. To configure additional SNMP trap destination, click the plus (+) sign and specify the settings
17. Click the **Save** button located at the top of the panel.

You can now specify alert settings.

About integrating with SNMP version 3 for alerts

To prepare BIG-IQ[®] Device to interface with your SNMP version 3 manager, you must do three things, all accomplished in one task.

- Configure SNMP agent
- Configure SNMP access
- Create an SNMP trap destination

Configuring SNMP version 3 for alerts

You configure the SNMP agent and provide specific access to BIG-IQ[®] Device so that the SNMP manager can collect data.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Click **SNMP Config**.
The screen displays the SNMP Agent Properties settings.
4. In the **Contact Information** field, type the name and email address of the person who is responsible for SNMP administration, and in the **Machine Location** field, type the location of the SNMP manager system.
These details are for informational purposes only, and have no impact on how BIG-IQ Device interfaces with your SNMP manager.

5. To download the F5-specific MIBs, click the **Download MIB** link.
6. In the **Addresses/Networks** fields, type the IP address and networks (and the netmask if applicable) that the SNMP manager is allowed to access.
7. To add another address, click the plus (+) sign.
8. In the New v3 Access Records section, in the **User Name** field, type the SNMP manager's user name.
9. If you want to specify the authentication protocol for SNMP traps, from the **Auth Type** list, select the type that you want the system to use.
 - **MD5** specifies digest algorithm.
 - **SHA** specifies secure hash algorithm.
10. If you selected an **Auth Type**, from the **Privacy** list, also select the type of encryption you want the system to use to encrypt SNMP traps.
 - **AES** specifies Advanced Encryption Standard
 - **DES** for Data Encryption Standard.
11. In the **Privacy Password** field, type the required password for access.
 SNMPv3 has special requirements when you create plain-text passwords on a router or switch:
 - The password must be at least eight characters long.
 - The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
12. In the **OID** field, type the object identifier (OID) you want to associate with this user.
13. Click the **Save** button located at the top of the panel.

You can now specify alert settings.

About integrating with SMTP for alerts

To have a specific recipient receive an email message when an alert is triggered by a system event, configure BIG-IQ® Device to deliver locally-generated email messages using the internet-standard for electronic mail transmission, Simple Mail Transfer Protocol (SMTP). Sending an email alert ensures that administrators are immediately notified when a specific system event occurs so they can quickly troubleshoot potential issues.

Specifying alert conditions

After you configure SNMP and or SMTP integration, you can specify the alerts that prompt BIG-IQ® System to send an email to the specified recipients.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Click the gear icon next to the group for which you want to specify alert conditions, and then click **Properties**.
4. Click **Alert Conditions**.
5. Select the check box next to each event that should trigger an alert email.
6. If a threshold is associated with the condition, in the adjacent **Threshold** field, type a value on which you want to trigger an alert email.
7. Click the **Save** button.

About authentication integration

Integrating BIG-IQ® systems with your authentication server allows you to remotely manage user access based on specific BIG-IQ system roles and associated permissions.

The BIG-IQ system is compatible with RADIUS and LDAP protocols.

Configuring authentication with LDAP

Before integrating LDAP authentication with the BIG-IQ® system, you must first:

- Use an LDAP browser to familiarize yourself with the groups and users in your directory's structure and their position in the hierarchy of organizational units (OUs).
- Decide how you want to map user names. The first option is to map users directly to their Distinguished Name (DN) in the directory with a user bind template in the form of `uid=<username>, ou=people, o=sevenSeas`. For example, when you map John Smith's user name with his DN as `uid=<jsmith>, ou=people, o=sevenSeas` and he logs in as `jsmith`, he is properly authenticated with his user name in the directory through his DN. The second option is to allow users to log in with names that do not map directly to their DN, by specifying a `userSearchFilter` in the form of `(&(uid=%s))` when creating the provider. For example, if John Smith's DN is `cn=John Smith, ou=people, o=sevenSeas`, but you would like him to be able to log in with `jsmith`, specify a `userSearchFilter` in the form of `(&(jsmith=%s))`. If your directory does not allow anonymous binds, you must also specify a `bindUser` and `bindPassword` so that the BIG-IQ system can validate the user's credentials.
- Determine which groups in your directory to map into BIG-IQ groups. If you configured a `bindUser` and `bindPassword` for users, the BIG-IQ system displays a list of groups from which to choose. If you have not, you must know the DN for each group.
- Identify the DN under which all users and groups can be found. This is the root bind DN for your directory and is expressed as `rootDN` when you create a provider. The BIG-IQ system uses the root bind DN as a starting point when searching for users and groups.
- Determine the host IP address for the LDAP server. The default port is 389, if not specified otherwise.

When you configure the BIG-IQ system for user authentication through your company's LDAP service, you can associate existing and new users added to the LDAP service with specific BIG-IQ roles. The permissions associated with those roles are based on the user credentials. The BIG-IQ system integration is compatible with LDAP server versions 2 and 3, and OpenLDAP directory, Apache Directory Server, and Active Directory

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. In the BIG-IQ Systems panel, click the gear icon next to the HA Peer Group you are configuring, and then click **Properties**.
4. Click **Auth Provider**.
5. From the **User Directory** list, select **Remote LDAP**.
The screen refreshes to display LDAP provider properties.
6. In the **Name** field, type a name for this new provider.
This must be a unique name.
7. In the **Host** field, type the IP address of your LDAP server.
8. If your Active Directory server uses a port other than the default, 389, in the **Port** field, type the number of the alternative port.

9. If you want BIG-IQ System to use an SSL port to communicate with the LDAP server, select the **Enabled** check box for the **SSL Enabled** setting.

Note that the **Port** setting automatically changes to 636.

10. If your LDAP server does not allow anonymous binds, in the **Bind User** and **Bind User Password** fields, type the full distinguished names and passwords for users with query access.

11. In the **Root DN** field, type the root context that contains users and groups.

The root context must be a full distinguished name.

12. From the **Authentication Method** list, select an option.

- **None** - Select this option to prompt the LDAP server to ignore the user name and password.
- **Simple** - Select this option to require a user name and password for authentication.

13. In the **Search Scope** field, type a number to specify the depth at which searches are made.

The default is 2. Alternatively, you can specify 0 for search only on the named object or 1 for a one-level search scope.

14. In the **Search Filter** field, type the LDAP filter expression that determines how users are found.

The search filter is determined by your LDAP implementation.

15. In the **Connect Timeout** field, type the number of milliseconds after which the BIG-IP® system stops trying to connect to the LDAP server.

16. In the **Read Timeout** field, type the number of seconds after which the BIG-IP system stops waiting for a response to a query.

17. In the **User Display Name Attribute** field, type LDAP field to use for the name BIG-IQ System displays.

When using Active Directory, this is typically `displayName`.

18. To direct bind to a distinguished name, in the **User Bind Template** field, type the name.

For example, `cn={username},ou=people,o=sevenSeas`.

Now, when a user logs in, BIG-IQ System inserts their user name into the template in place of the token, and the resulting distinguished name is used to bind to the directory.

19. To prompt the LDAP provider to search for groups based on a specific display name attribute, in the **Group Display Name Attribute** field, type an attribute.

This attribute is typically `cn`.

20. Leave the **Group Search Filter** at its default query to return all groups under the provided rootDN.

Alternatively, if you have a large number of groups (more than 100), you can narrow base the search on a specific term by typing a query with a `{searchterm}` token in this field.

For example: `(&objectCategory=group)(|(cn={searchterm}*))`

21. To specify a query for finding a users group, in the **Group Membership Filter** field, type a query string.

Use the token `{userDN}` anywhere that the user's distinguished name should be supplied in the LDAP query.

You can use a `{username}` token as a substitute to the user's login name in a query.

Leave this setting at the default `(|(member={username})(uniqueMember={username}))` unless the provider is Active Directory.

22. To specify a query attribute for finding users in a particular group, in the **Group Membership User Attribute** field, type the attribute.

When using Active Directory, use `memberof`. For example:

`(memberof=cn=group_name,ou=organizational_unit,dc=domain_component)`

For other LDAP directories, use `groupMembershipFilter`. For example:

`(groupMembership=cn=group_name,ou=organizational_unit,o=organization)`

23. Select the **Perform Test** check box to test this provider.
24. Click the **Save** button.

The BIG-IQ system now authenticates users against the configured LDAP server.

Configuring authentication with RADIUS

You must first license the BIG-IQ system and specify DNS settings before you can specify authentication settings.

When you configure the BIG-IQ® system for user authentication through your company's RADIUS service, you can associate existing and new users added to the RADIUS service with specific BIG-IQ roles. The permissions associated with those roles are based on the user credentials.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. In the BIG-IQ Systems panel, click the gear icon next to the HA Peer Group you are configuring, and then click **Properties**.
4. Click **Auth Provider**.
5. From the **User Directory** list, select **Remote RADIUS**.
6. In the **Name** field, type a name for this new provider.
This must be a unique name.
7. In the **Host** and **Port** fields, type the RADIUS server's IP address (or fully qualified domain name) and port number.
8. In the **Secret** field, type the case-sensitive text string used to validate communication.
9. To validate the user after adding it, in the **Test Connection User** and **Test Connection Password** fields, type the user name and password.
10. Click the **Save** button.

You can now associate RADIUS server users and groups to BIG-IQ system roles.

Chapter 4

Users, User Groups, and Roles

- *Overview: Users, user groups, and roles*
 - *About user roles*
-

Overview: Users, user groups, and roles

A *user* is an individual to whom you provide resources. You provide access to users for specific BIG-IQ® system functionality through authentication. You can associate a user with a specific role, or associate a user with a user group and then associate the group with a role.

A *role* is defined by its specific privileges. A *user group* is a group of individuals that have access to the same resources. When you associate a role with a user or user group, that user or user group is granted all of the role's corresponding privileges.

By default, the BIG-IQ® system provides the following default user types:

Default user type	Default password	Access rights
admin	admin	This user type can access all aspects of the BIG-IQ system from the system's user interface.
root	default	This user has access to all aspects of the BIG-IQ system from the system's console command line.

User types persist and are available after a BIG-IQ system failover. You can authenticate users locally on the BIG-IQ system or remotely through LDAP or RADIUS.

About default passwords for pre-defined users

When you initially license the BIG-IQ® system, it creates the following administrative roles with a default password.

- admin
- root

Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system to automatically create the administrator user.

After you initially license and configure the BIG-IQ system, it is important to change the administrator role password from the default, `admin`.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, for **Admin User**, click the gear icon and then **Properties**.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click the **Add** button.

Adding a locally-authenticated BIG-IQ user

You create a user so you can then associate that user with a particular role to define access to specific BIG-IQ® system resources.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. Hover over the Users header, and click the + icon when it appears.
The panel expands to display the User properties.
4. From the **Auth Type Provider** list, select **Local**.
5. In the **Full Name** field, type a name to identify this user.
The full name can contain a combination of symbols, letters, numbers and spaces.
6. In the **Password** and **Confirm Password** fields, type the password for the new user.
7. Click the **Add** button.

You can now associate this user with a role.

About user roles

As a system manager, you need a way to differentiate between users and to limit user privileges based on their responsibilities. To assist you, the BIG-IQ® system has created a default set of roles you can assign to a user. Roles persist and are available after a BIG-IQ system failover.

Roles definitions

BIG-IQ® system ships with several standard roles, which you can assign to individual users.

Role	Description
Administrator	Responsible for overall administration of all licensed aspects of the BIG-IQ system, which can include BIG-IQ Cloud, BIG-IQ Security, BIG-IQ System, and BIG-IQ ADC management. These responsibilities include adding individual users, assigning roles, discovering BIG-IP® systems, installing updates, activating licenses, and configuring a BIG-IQ high availability (HA) configuration.
Device Manager	Responsible for device administration including device discovery, group creation, licensing, and management of software images, UCS backups, templates, connectors, certificates, self IP addresses, VLANs, and interfaces. This role must first create a group before discovering and managing devices.
Network Security Deploy	Can view and deploy firewall configuration objects associated with managed firewall devices.

Role	Description
Network Security Edit	Can view and modify configuration objects associated with managed firewall devices, including the ability to create, modify, or delete all shared and firewall-specific objects.
Network Security Manager	Has all of the privileges assigned to the Network Security View, Network Security Edit, and Network Security Deploy roles.
Network Security View	Can only view configuration objects and tasks for all firewall devices under management.
Security Manager	Has all of the privileges assigned to the Network Security View, Network Security Edit, and Network Security Deploy roles.
Web App Security Manager	Responsible for administration of the individual components of web application security, including associated devices, policies, virtual servers, signature files, and deployments.

Associating a user or user group with a role

Before you can associate a user or user group with a role, you must create a user or user group.

When you associate a user or user group with a role, you define the resources users can view and modify. You can associate multiple roles with a given user.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users or User Groups panel, click the name you want to associate with a role, and drag and drop it on a role in the Roles panel.
A confirmation pop-up screen opens.
4. Click the **Confirm** button to assign the user or user group to the selected role.

This user or user group now has access to the resources associated with the role you specified.

Disassociating a user from a role

Use this procedure to disassociate a user from an assigned role.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **System >Users**.
3. Click the name of the user you want to edit.
4. For the User Roles property, delete the user role that you want to disassociate from this user.
5. Click the **Save** button to save your changes.

This user no longer has the privileges associated with the role you deleted.

Chapter

5

Additional Network Configuration Options

- *About additional network configuration options*
 - *Configuring an additional VLAN*
-

About additional network configuration options

During the licensing and initial configuration procedures, you configure a single VLAN and associated self IP addresses. This is all the networking configuration required to start managing devices. However, if you find you need additional VLANs, the BIG-IQ® system provides you with the ability to add them as required.

Configuring an additional VLAN

You must have licensed the BIG-IQ® system before you can add a VLAN.

You have the option to configure an additional VLAN after you license and perform the initial configuration of the BIG-IQ system.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the VLANs panel and click the + sign when it appears.
4. In the **Name** and **Description** fields, type a name and description to identify this new VLAN.
5. From the **Device** list, select the BIG-IQ system to associate with this new VLAN.
6. From the **Interface** list, select the port that you want this VLAN to use.

The *interface* is a physical or virtual port that you use to connect the BIG-IQ system to managed devices in your network.

7. Click the **Add** button to save this VLAN.
8. Hover on the Self IP Addresses panel and click the + when it appears.
9. In the **Name** and **Address** and **Description** fields, type the name, and self IP address.
10. From the Device list, select the BIG-IQ system to associate with this new self IP address.
11. From the **VLAN** list, select the VLAN to which you want to associate this self IP address.
12. Click the **Add** button to save this self IP address.

Chapter

6

BIG-IQ High Availability

- *About a high availability active-active cluster*
- *Configuring BIG-IQ system in an active-active high availability cluster*

About a high availability active-active cluster

You can ensure that you always have access to managed BIG-IP® devices by installing two or more BIG-IP® systems in an active-active, high availability (HA) configuration. Any configuration change that occurs on one BIG-IP system is immediately synchronized with its peer devices. If a BIG-IP® system in an active-active HA configuration fails, a peer BIG-IP system takes over the device management.

***Note:** If you are configuring BIG-IQ Security you must configure an active-standby cluster. Refer to the BIG-IQ Security: Administration guide for detailed instructions.*

Configuring BIG-IQ system in an active-active high availability cluster

An active-active, high availability (HA) configuration ensures access to managed BIG-IP® devices in case one BIG-IP® system fails.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the BIG-IQ Systems header, click the + icon when it appears, and then click **Add Device**. The Add Device screen opens.
4. In the **IP Address** field, type the BIG-IQ System's self IP address.
5. In the **User name** and **Password** fields, type the administrative user name and password for the system.
6. From the **Group** list, select **Management Group**.
7. Click the **Save** button.

If discovery of the newly configured BIG-IQ system fails, a **Delete** button displays. Verify the correct self IP address and credentials. Then click the **Delete** button to remove the incorrect information, and re-type the self IP address, user name, and password.

Chapter

7

BIG-IQ System Management

- *Installing and upgrading BIG-IQ System software*
 - *About UCS files*
-

Installing and upgrading BIG-IQ System software

Before you perform an initial BIG-IQ® System software installation, or software upgrade, you must perform the following tasks:

- Activate, or reactivate, your current license to ensure that you have a valid service check date.
- Download the ISO file for the upgrade from F5 Downloads to `/shared/images` on BIG-IQ System. If you need to create this directory, use the exact name `/shared/images`.
- For upgrades only, create a backup of the user configuration set (UCS), locate it in the `/var/local/ucs` directory on the source installation location, and copy the UCS file to another system for safe keeping.

Use this procedure when you are ready to perform an initial BIG-IQ System software installation or upgrade a to a more recent software version.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, expand **Management Group** or **HA Peer Group** by clicking the arrow next to it.
4. Click the gear icon next to **localhost**, and then click **Properties**.
5. Click **Software Update**.
6. Click the **Update** button.
7. From the **Software Image** list, select the new image or browse to the location to which you saved it.
8. From the **Install Location** list, select the volume to which you want to install the image.
9. For the **Options** setting, select one:
 - To automatically reboot the BIG-IQ System to the specified volume immediately after the software is installed, select **Reboot after Live Install**.
 - To manually reboot the BIG-IQ System at another time from the **System > Properties** screen, select **Set Default Boot Location**.
10. Click the **Apply** button.

BIG-IQ System installs the selected software. For upgrades, BIG-IQ System also rolls forward the UCS file.

About UCS files

The configuration details of managed devices (including the BIG-IQ® system itself) are contained in a compressed user configuration set (UCS) file. The UCS file contains all of the information required to restore a device's configuration, such as:

- System-specific configuration files
- License
- User account and password information
- SSL certificates and keys

You can back up devices at regularly scheduled intervals and select the amount of time to save the backups.

Creating a backup UCS file

It is best practice to create a backup of the UCS file for each device in your network, including the BIG-IQ® system itself, on a regular basis and before performing a software upgrade. The UCS file backup provides your network with added stability in the event that a system needs to be restored.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Backups panel header, click the + sign when it appears, and then click **Add Backup**.
4. In the **Name** and **Description** fields, type a file name and description to identify this UCS backup file. The file name you define in the **Name** field must include the extension `.ucs`.
5. From the **Device** list, select the device for which you want to create the UCS file backup.
6. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.
7. To encrypt the backup file, select the **Encrypt Backup Files** check box.
8. Click the **Create** button
9. To view the status of the backup or change its description, click the gear icon.

This UCS backup file is now available for restoration.

Index

A

- active-active cluster
 - configuring for the BIG-IQ system [38](#)
- active-active pair
 - configuring for the BIG-IQ system [38](#)
- active directory
 - about integrating with [28](#)
- admin, *See* administrator
- Administrator role
 - defined [33](#)
- administrator user
 - and default password [32](#)
 - changing password for [25](#), [32](#)
- administrator user password
 - changing [25](#), [32](#)
- alert conditions
 - specifying [27](#)
- alerts
 - using [25](#)
- authentication
 - configuring with LDAP [28](#)
 - configuring with RADIUS [30](#)
- authentication integration
 - about [28](#)
- authorization checks
 - for secure communication [17](#)

B

- backups
 - about [40](#)
 - for UCS files [41](#)
- base registration key
 - about [23](#)
- BIG-IP devices
 - downloading software image for upgrades [22](#)
- BIG-IQ Cloud
 - about [16](#)
 - finding documentation for [16](#)
- BIG-IQ Device
 - about [16](#)
 - finding documentation for [16](#)
- BIG-IQ Security
 - about [16](#)
 - finding documentation for [16](#)
- BIG-IQ system
 - about [16](#)
 - about licensing [22](#)
 - downloading software image for [22](#)
 - reordering panels [20](#)
- BIG-IQ System
 - upgrading [22](#), [40](#)
- BIG-IQ System software
 - installing [22](#), [40](#)

C

- clusters
 - for high availability [38](#)
- communication
 - between BIG-IQ and managed devices [17](#)
- configuration
 - and initial setup [23](#)
- configurations
 - about creating backups [40](#)

D

- device availability
 - specifying alerts for [27](#)
- device backup
 - about [40](#)
 - and USC files [40](#)
- device groups availability
 - specifying alerts for [27](#)
- Device Manager role
 - defined [33](#)
- devices
 - alerting for system events [25](#)
- discovery address
 - defined [23](#)
 - viewing [36](#)
- DNS server
 - specifying for the BIG-IQ system [24](#)
- documentation, finding [16](#)
- dossier
 - providing [23](#)

E

- email alerts
 - about [27](#)

F

- failover [38](#)
- filtering process
 - finding associated objects [20](#)

G

- guides, finding [16](#)

H

- HA, *See* high availability cluster
- health
 - for devices [25](#)
 - specifying alerts for [27](#)
- high availability cluster
 - configuring [38](#)

- high availability configuration
 - about [38](#)
- HTTPS port 443
 - required for communication [17](#)

I

- initial configuration
 - for BIG-IQ system [23](#)
- integration
 - about authentication [28](#)
- interface
 - configuring for a new VLAN [36](#)
 - defined [36](#)

L

- LDAP
 - configuring authentication [28](#)
 - integrating authentication [28](#)
- license
 - activating automatically [23](#)
 - activating manually [23](#)
- license activation
 - for BIG-IQ system [23](#)

M

- manuals, finding [16](#)

N

- network
 - configuring additional VLAN [36](#)
 - incorporating BIG-IQ systems [22](#)
 - port 443 [22](#)
- networking
 - advanced [36](#)
- network security
 - about [17](#)
- Network Security Deploy role
 - defined [33](#)
- Network Security Edit role
 - defined [33](#)
- Network Security Manager role
 - defined [33](#)
- Network Security View role
 - defined [33](#)

O

- objects
 - finding associations [20](#)
 - searching for [20](#)

P

- Pacific Standard Time zone
 - as default for the BIG-IQ system [24](#)
- panels
 - reordering [20](#)

- password
 - changing for administrator user [25](#), [32](#)
- port 22
 - using [17](#)
- port 443
 - required for communication [17](#)
 - using [17](#)
- ports
 - required for communication with BIG-IQ [17](#)
 - required open [17](#)
- pre-defined users
 - and administrator role [32](#)
 - and root role [32](#)
- PST zone, See Pacific Standard Time zone

R

- RADIUS
 - configuring authentication with [30](#)
- release notes, finding [16](#)
- required port, for network communication [22](#)
- roles
 - associating with users and user groups [34](#)
 - defined [32](#)
 - for users [32–33](#)
- root user
 - and default password [32](#)

S

- search function
 - finding specific objects [20](#)
- security
 - for communication [17](#)
- Security Manager role
 - defined [33](#)
- self IP addresses
 - adding [36](#)
- SMTP server
 - about configuring [27](#)
- SNMP
 - configuring version 1 or 2 on BIG-IQ Device [25](#)
 - configuring version 3 for BIG-IQ Device [26](#)
- SNMP version 1 or 2
 - integrating BIG-IQ Device [25](#)
- SNMP version 3
 - integrating BIG-IQ Device [26](#)
- software
 - installing for BIG-IQ System [22](#), [40](#)
 - upgrading [22](#)
- software images
 - downloading [22](#)
- software upgrade
 - for BIG-IQ system [22](#), [40](#)
- system alerts
 - specifying [27](#)
- system user
 - adding [33](#)

T

- TCP port 22
 - using [17](#)
- TCP port 443
 - using [17](#)
- time zone
 - and default for the BIG-IQ system [24](#)
 - changing for the BIG-IQ system [24](#)
 - specifying a DNS server for the BIG-IQ system [24](#)
- time zone default
 - for the BIG-IQ system [24](#)
- troubleshooting
 - using email alerts [27](#)

U

- UCS file
 - about [40](#)
 - defined [40](#)
- UCS files
 - creating backup [41](#)
- upgrades
 - downloading software image [22](#)
- user authentication
 - configuring through RADIUS [30](#)

- user configuration set, See UCS file
- user groups
 - defined [32](#)
- user interface
 - and searching for specific objects [20](#)
 - customizing [20](#)
 - navigating [20](#)
- user roles
 - about [33](#)
 - associating with users and user groups [34](#)
- users
 - adding [33](#)
 - defined [32](#)
 - removing role from [34](#)

V

- VLAN
 - adding [36](#)

W

- Web App Security Manager role
 - defined [33](#)

