

# **BIG-IQ<sup>®</sup> Device: Device Management**

Version 4.5





# Table of Contents

<b>Legal Notices.....</b>	<b>7</b>
<b>Acknowledgments.....</b>	<b>9</b>
<b>Chapter 1: BIG-IQ Device: Device Management Overview.....</b>	<b>17</b>
About BIG-IQ Device.....	18
Additional resources and documentation for BIG-IQ systems.....	18
About the BIG-IQ system user interface.....	19
Filtering for associated objects.....	19
Searching for specific objects.....	19
Customizing panel order.....	19
Specifying idle timeout and default screen.....	20
<b>Chapter 2: Required BIG-IQ System Components.....</b>	<b>21</b>
Installing required BIG-IQ system components.....	22
<b>Chapter 3: Device Discovery.....</b>	<b>23</b>
About device discovery and management.....	24
Discovering devices.....	24
Discovering a large group of devices .....	26
Viewing and exporting device inventory details.....	26
Modifying device configurations.....	27
About managing BIG-IP devices in a device service clustering.....	28
Viewing properties and state of BIG-IP in a device service clustering .....	28
Viewing and synchronizing configurations for BIG-IP devices in a DSC .....	29
About static and dynamic device groups.....	29
Creating static group of managed devices.....	30
Creating a dynamic group of managed devices.....	30
<b>Chapter 4: Upgrading BIG-IP System Software.....</b>	<b>33</b>
About upgrading BIG-IP system software.....	34
Downloading software images.....	34
Upgrading a device.....	34
Upgrading a legacy device.....	35
<b>Chapter 5: Templates for Configuration Management.....</b>	<b>37</b>
About configuration templates.....	38
Creating a configuration template.....	38
Applying a configuration template to a managed device.....	38

<b>Chapter 6: UCS File Backup and Restoration.....</b>	<b>41</b>
About UCS files.....	42
Creating a backup UCS file.....	42
Restoring a UCS file backup.....	43
<b>Chapter 7: SSL Certificate Monitoring.....</b>	<b>45</b>
About SSL certificate monitoring.....	46
Monitoring SSL certificate expiration dates.....	46
<b>Chapter 8: Users, User Groups, and Roles.....</b>	<b>47</b>
Overview: Users, user groups, and roles.....	48
Changing the default password for the administrator user.....	48
Adding a locally-authenticated BIG-IQ user.....	48
Adding a remotely-authenticated LDAP user.....	49
Adding a remotely-authenticated RADIUS user.....	49
Creating a user group.....	49
About user roles.....	50
Roles definitions.....	50
Associating a user or user group with a role .....	51
Disassociating a user from a role.....	51
<b>Chapter 9: BIG-IQ High Availability.....</b>	<b>53</b>
About a high availability active-active cluster.....	54
Implementing an active-active high availability configuration.....	54
<b>Chapter 10: License Management.....</b>	<b>55</b>
Overview: Licensing options.....	56
About pool licenses.....	56
Automatically activating a pool license .....	56
Manually activating a pool license.....	57
Assigning a pool license to a BIG-IP VE.....	57
Revoking a pool license from a BIG-IP VE.....	58
About utility licenses.....	58
Automatically activating a utility license.....	58
Manually activating a utility license.....	59
Assigning a utility license to a BIG-IP device.....	60
Downloading a utility license usage report.....	60
Automatically submitting a utility license usage report to F5.....	61
Revoking a utility license from BIG-IP VE.....	61
About volume licenses.....	61
Automatically activating a volume license.....	61
Manually activating a volume license.....	62

Assigning a volume license to a BIG-IP VE.....63  
Revoking a volume license from a BIG-IP VE.....64



# Legal Notices

---

## Publication Date

This document was published on July 2, 2015.

## Publication Number

MAN-0498-03

## 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](mailto:bazsi@balabit.hu)), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller ([nisse@lysator.liu.se](mailto: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](http://www.gnu.org/copyleft/lgpl.html).

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

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

This product includes software developed by Oracle America, Inc. Copyright ©2012.

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

## Acknowledgments

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 Mojarrá project. Source code for the Mojarrá software may be obtained at <https://javaserverfaces.dev.java.net/>.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This product includes 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

## Acknowledgments

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 Device: Device Management Overview**

---

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

## About BIG-IQ Device

---

BIG-IQ<sup>®</sup> Device offers you the flexibility to deploy software images, and configurations, and monitor and distribute licenses and license pools for managed BIG-IP<sup>®</sup> devices. BIG-IQ Device also provides you with an inventory management tool so that you can easily view and export detailed information about every device you are managing. This centralized device management saves you time because you can perform multiple deployments to a number of BIG-IP devices, without having to log in to each of them individually. The inventory management functionality keeps you apprised of every detail about your managed devices, helping you to better manage your assets.

### Additional resources and documentation for BIG-IQ systems

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

Document	Description
BIG-IQ <sup>®</sup> Systems Virtual Editions Setup guides	BIG-IQ <sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> Device: Device Management</i>	This guide provides details about how to deploy software images, licenses, and configurations to managed BIG-IP <sup>®</sup> devices.
<i>BIG-IQ<sup>®</sup> Cloud: Cloud Administration</i>	This guide contains information to help a cloud administrator manage cloud resources, devices, applications, and tenants (users).
<i>BIG-IQ<sup>®</sup> Cloud: Tenant User Guide</i>	This guide contains information to help tenants manage applications.
<i>BIG-IQ<sup>®</sup> Application Delivery Controller: Administration</i>	This guide provides details about how to centrally manage BIG-IP <sup>®</sup> Local Traffic Manager <sup>™</sup> applications.
<i>BIG-IQ<sup>®</sup> Security: Administration</i>	This guide contains information used to centrally manage BIG-IP <sup>®</sup> firewalls, policies, rule lists (as well as other shared objects), and users.
<i>Platform Guide: BIG-IQ<sup>®</sup> 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 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.

## Specifying idle timeout and default screen

Before you can specify the global administrator user settings, you must first license the BIG-IQ system.

You can define the minutes the BIG-IQ system waits before logging you out as well as specify the default screen displayed when you log in.

1. Log in to BIG-IQ System with your administrator user name and password.
2. In the right corner of the screen hover **admin** and click **Global User Settings** when it appears.
3. In the **Idle Timeout (minutes)** field, type the number of idle minutes you want the BIG-IQ system to wait before logging you out.
4. From the **Default View** list, select the screen you want to view upon logging in to the BIG-IQ system.
5. Click the **Save** button.

---

# Chapter

# 2

---

## Required BIG-IQ System Components

---

- *Installing required BIG-IQ system components*
-

### Installing required BIG-IQ system components

---

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

You must install and keep up-to-date certain BIG-IQ system components on all BIG-IP devices that are to be brought under central management. Otherwise, device discovery will fail. These required components provide a REST framework required for the BIG-IQ platform. To install these components manually, run the commands from the command line.

---

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

---

1. Log in to the BIG-IQ system command line as the root user.
2. Establish SSH trust between the BIG-IQ system and the managed BIG-IP device:  

```
ssh-copy-id root@<BIG-IP Management IP Address>
```

This step is optional. However, if you do not establish trust, you will be required to provide the BIG-IP system's root password multiple times.
3. Navigate to the folder in which the required files reside:  

```
cd /usr/lib/dco/packages/upd-adc
```
4. Run the installation script:  

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

Where *<password>* is the administrator password for the BIG-IP device.
5. Revoke SSH trust between the BIG-IQ system and the managed BIG-IP device:  

```
ssh-keygen -R <BIG-IP Management IP address>
```

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

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

---

# Chapter

# 3

---

## Device Discovery

---

- *About device discovery and management*
- *About managing BIG-IP devices in a device service clustering*
- *About static and dynamic device groups*

## About device discovery and management

---

You use the BIG-IQ<sup>®</sup> system to centrally manage resources located on BIG-IP<sup>®</sup> devices in your local network, in a public cloud like Amazon EC2, or in combination.

The first step to managing devices is making the BIG-IQ system aware of them through the discovery process. To discover a device, you provide the BIG-IQ system with the device IP address, user name, and password. Alternatively, you can upload a CSV file to discover a large number of devices. When you discover a device, you place it into a group. These groups help you organize devices with similar features, like those in a particular department or running a certain software version.

After you discover devices, you can view and export inventory details about those devices for easy asset management, and you can modify device configurations as required without having to log in to each device individually.

### Discovering devices

After you license and perform the initial configuration for the BIG-IQ<sup>®</sup> system, you can discover BIG-IP<sup>®</sup> devices running version 11.3.0 or later. For proper communication between the managing BIG-IQ system and the devices it manages, you must configure the BIG-IQ system with a route to each F5 device you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

---

**Important:** *If the BIG-IP devices are running a version earlier than version 11.3.0, you must upgrade the legacy device before you can successfully discover it.*

---

Discovering BIG-IP devices is the first step to managing them.

1. Log in to BIG-IQ Device with the administrator user name and password.
2. Hover over the Devices header, click the + icon when it appears, and then select **New Device**. The Devices panel expands to show the New Device screen.
3. For devices on the same subnet as the BIG-IQ system, in the **IP Address** field, specify the IP address of the device:
  - For devices in your local network, or located on an OpenStack or VMware cloud device, type the IP address of the device.
  - For devices located on Amazon EC2 cloud, type the device's external self IP address.

The preferred address for discovering a BIG-IP device is its management IP address.

4. (This step applies only when the BIG-IQ system is hosted on AWS version 4.4 or later.) If the BIG-IQ system and the BIG-IP device are on different subnets, then you need to log in to the BIG-IQ system using SSH to specify an IP route between them.
  - If the BIG-IQ system and the BIG-IP device communicate using the management IP address, then there must be a default route specified. If there is no default route, issue a `route` command.
    1. Use SSH to log in to the BIG-IQ system's management IP address as an admin user.
    2. Type the following command: `run /util bash`
    3. Type the following command: `route <route name> {gw <x.x.x.x> network default}`
  - If the BIG-IQ system and the BIG-IP device use something other than the management IP address to communicate, then issue a `tmsh route` command.

1. Use SSH to log in to the BIG-IQ system's management IP address as an admin user.
2. Type the following command: `create net route <route name> {gw <x.x.x.x> network default}`

---

*Note:* Where <route name> is a user-provided name to identify the new route, and <x.x.x.x> is the IP address of the default gateway for the internal network.

---

5. (This step applies only if the BIG-IQ system is not hosted on AWS version 4.4 or later.) If the BIG-IQ system and the BIG-IP device are on different subnets, then you need to log in to the BIG-IQ system using SSH to specify an IP route between them.
  - If the BIG-IQ system and the BIG-IP device communicate using the management IP address, then there must be a default route specified. If there is no default route, issue a `route` command.
    1. Use SSH to log in to the BIG-IQ system's management IP address as the root user.
    2. Type the following command: `route <route name> {gw <x.x.x.x> network default}`
  - If the BIG-IQ system and the BIG-IP device use something other than the management IP address to communicate, then issue a `tmsh route` command.
    1. Use SSH to log in to the BIG-IQ system's management IP address as the root user.
    2. Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

---

*Note:* Where <route name> is a user-provided name to identify the new route, and <x.x.x.x> is the IP address of the default gateway for the internal network.

---

6. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.
7. For the **Auto Update Framework** setting, select the **Update Automatically** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.  
For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework.

---

**Important:** When you update the REST framework for BIG-IP devices running version 11.6 or earlier, the traffic management interface (TMM) restarts. Before you update the REST framework on a BIG-IP device, verify that no critical network traffic is targeted to that device. Additionally, In any system upgrade scenario, the potential exists for unexpected errors. Because there is not currently an automatic recovery and rollback feature, if an upgrade fails, it is conceivable that a BIG-IP device would not be left in the pre-discovery state. If you want to roll back the upgrade due to an error or any other reason, the recommended recovery for this situation is to perform a partition restore (restoring both the pre-discovery management components and any related configuration).

---

8. Click the **Add** button.

The BIG-IQ system populates the properties of the device that you added, and displays the device in the Devices panel. Its configuration files display in the Configuration panel.

## Discovering a large group of devices

After you license and perform the initial configuration for the BIG-IQ<sup>®</sup> system, you can discover BIG-IP<sup>®</sup> devices running version 11.3.0 or later. For proper communication between the managing BIG-IQ system and the devices it manages, you must configure the BIG-IQ system with a route to each F5 device you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

Before you discover a large group of devices, you must save the information in a .csv file in one of the following formats:

- [address], [userName], [password], [automaticFrameworkUpdate?], [rootUser], [rootPassword], for example: 192.168.2.xxx, admin, password, true, root, password Use this option if you want BIG-IQ Device to automatically update the framework required to manage the devices.
- [address], [userName], [password], for example: 192.168.2.xxx, admin, password

If you have a large number of devices to discover, discovering them in a group saves you a significant amount of time, because you are not required to provide the device identification details for each individual device. Instead, you can upload a CSV file that contains the IP address, user name, and password for the devices you want to discover.

---

**Important:** When you update the REST framework for BIG-IP devices running version 11.6 or earlier, the traffic management interface (TMM) restarts. Before you update the REST framework on a BIG-IP device, verify that no critical network traffic is targeted to that device. Additionally, in any system upgrade scenario, the potential exists for unexpected errors. Because there is not currently an automatic recovery and rollback feature, if an upgrade fails, it is conceivable that a BIG-IP device would not be left in the pre-discovery state. If you want to roll back the upgrade due to an error or any other reason, the recommended recovery for this situation is to perform a partition restore (restoring both the pre-discovery management components and any related configuration).

---

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Devices header, click the + icon when it appears, and then select **Import Devices**.
4. From the **Group Name** list select the group to which you want to add the imported devices.
5. Click the **Choose File** button and select the CSV file to which you exported the device list.  
Alternatively, you can navigate to the CSV file on your computer and drag and drop it to the Import Devices screen.
6. Click the **Discover** button to complete the discovery process.  
If there was a format error for the data in the .csv file, discovery fails and BIG-IQ Device returns an error.

The BIG-IQ system populates the properties of the device that you added, and displays the device in the Devices panel. Its configuration files display in the Configuration panel.

## Viewing and exporting device inventory details

You can view detailed data about the managed devices in your network. Information includes associated IP addresses, platform type, license details, software version, and so forth. In addition to viewing this information, you can also export it to a CSV file and edit the data as required to create reports for asset management.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. In the Devices panel, click the gear icon next to the device you want to view, and then select **Properties**. The panel expands to display device properties.
4. To export the data to a CSV file, click the **Export** button.  
You can modify the report as required in Microsoft Excel.

## Modifying device configurations

You must first discover a device before you can modify its configuration.

---

***Note:** The BIG-IQ Device REST proxy is enabled by default to allow you to edit configurations. If you have disabled the REST proxy, re-enable it by clicking the gear icon for the **Device**, clicking **Permissions**, and selecting the **Enable REST Proxy** check box.*

---

With BIG-IQ® Device, you can easily view and modify configuration details for a device from one central location. For example, after you discover several devices, you might want to review the network settings for those devices to ensure that they are correctly configured. To do this, you start by filtering objects. *Filtering* network objects by their associated devices helps you refine the view to show only those you want to see. You can then select the particular properties you want to modify. This centralized configuration management saves time, because you are not required to physically interface with individual devices in your network.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. 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.
3. 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.
4. Click the **Apply** button.  
The screen refreshes to display only the objects associated with the term you typed in the Filter field.
5. To further refine the filter, type another term into the Filter field, and click the **Apply** button again.
6. To remove a filter term, click the **X** icon next to it.
7. Once you have located items associated for a particular configuration, click the gear icon next to the object you want to modify, and then click **Properties**.
8. Modify the editable fields as required.
9. Click the **Save and Deploy** button.  
Valid changes you make to this object become effective on the managed device immediately after you click the **Save and Deploy** button.  
If the changes you make are invalid, BIG-IQ Device displays an error and allows you to re-edit the property.
10. To add a new object:
  - a) Hover on the panel header and click the + sign when it appears.  
The + sign appears only if you are permitted to add that object.
  - b) Specify the properties of the new object.
  - c) Click the **Add and Deploy** button.

Settings you specify for this object become effective on the managed device immediately after you click the **Add and Deploy** button.

11. Click the **Save** button.

## About managing BIG-IP devices in a device service clustering

---

Device service clustering, or DSC<sup>®</sup>, is an underlying architecture within BIG-IP<sup>®</sup> Traffic Management Operation System (TMOS<sup>®</sup>). DSC provides synchronization and failover of BIG-IP system configuration data at user-defined levels of granularity, among multiple BIG-IP devices on a network. When your network includes BIG-IP devices running version 11.5 and later that are configured in a DSC, BIG-IQ<sup>®</sup> Device populates the DSC Groups panel with the device's details when you discover those devices.

---

***Note:** For specific information about BIG-IP DSC groups, refer to the BIG-IP<sup>®</sup> Device Service Clustering: Administration guide.*

---

## Viewing properties and state of BIG-IP in a device service clustering

You must discover BIG-IP devices configured in a DSC before you can manage them from BIG-IQ Device. If you add a BIG-IP device to a DSC group after you discover it, you must hover on the Clusters header and click the refresh button when it appears. After you refresh the panel, BIG-IQ Device populates the panel with the BIG-IP devices you added to the DSC group.

BIG-IQ Device provides you a way to centrally view properties about BIG-IP devices configured in a cluster. These properties include sync and fail over settings and status, trust domain details, participating BIG-IP devices, and associated traffic groups. Viewing these properties from BIG-IQ Device eliminates the need for you to log on to each BIG-IP device in the cluster.

---

***Important:** BIG-IQ Device can discover only BIG-IP devices running version 11.5 or later when configured in a cluster.*

---

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Cluster Management**.
3. On the Clusters header, click the refresh button.  
Refreshing this panel ensures you have the most recent configuration for the devices in the DSC group.
4. Click the gear icon next to the DSC group you want to view, and then click **Properties**.  
The panel expands to display the properties for this DSC.
5. To validate the trust certificate associated with this DSC group, click the **View Details** button.  
A window opens to display the trust domain details.
6. To view the devices included in this DSC, click **Devices**.
7. To view the traffic groups associated with this DSC, click **Traffic Groups**.
8. To close the panel, click the **Close** button.

## Viewing and synchronizing configurations for BIG-IP devices in a DSC

You must discover BIG-IP devices configured in a DSC before you can manage them from BIG-IQ Device. If you add a BIG-IP device to a DSC group after you discover it, you must hover on the Clusters header and click the refresh button when it appears. After you refresh the panel, BIG-IQ Device populates the panel with the BIG-IP devices you added to the DSC group.

BIG-IQ Device provides you a way to view and synchronize configuration changes for BIG-IP devices in a DSC active-standby or active-active configuration. Synchronizing configurations from BIG-IQ Device eliminates the need for you to log on to each BIG-IP device in the DSC.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Cluster Management**.
3. On the Clusters header, click the refresh button.

Refreshing this panel ensures you have the most recent configuration for the devices in the DSC group.

4. Click the device for which you want to perform synchronization.
5. For the Sync Option setting, select one of the following options:
  - **Device to Group** - Select this option to prompt BIG-IQ Device to push this device's configuration out to every other device in this DSC group. When you select this option, BIG-IQ Device warns you if the configuration on this device is not as current as the configuration on the rest of the DSC group devices.
  - **Group to Device** - Select this option you add a new BIG-IP device to the DSC group and you want BIG-IQ Device to pull the group's configuration and load it onto that new DSC group member. When you select this option, BIG-IQ Device warns you if the configuration on this device is more current than the configuration on the rest of the DSC group devices.

6. Click the **Sync** button.

If a BIG-IP device in a DSC configuration was detected in your network, but not discovered from BIG-IQ Device, it displays with the Sync button unavailable. You must discover BIG-IP devices in a DSC configuration from BIG-IQ Device before you can synchronize configurations.

7. To close the panel, click the **Close** button.

## About static and dynamic device groups

---

To help you manage a large number of BIG-IP® devices, you can organize them into groups. You can create two different types of device groups:

- Static group
- Dynamic group

A *static group* contains a specific set of devices. You may want to create a static group for devices hosting certain applications, in a certain geographical location, or running specific version of BIG-IP software. In contrast, a *dynamic group* is essentially a saved query on against a static group. For example, if you create a static group that contained all of your managed BIG-IP devices and you wanted to view only those devices running a specific version of software, you would create a dynamic group with that parameter.

If you delete a managed BIG-IP device from the static group, that change reflects in the dynamic group when you view it.

### Creating static group of managed devices

You must license and discover BIG-IP<sup>®</sup> devices before you can place them into a group.

To help you manage a large number of devices, you can organize them into groups. For example, you could group devices by applications, geographical location, or department.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Devices header, click the + icon when it appears, and then select **New Group**.
4. In the **Display Name** field, type the name you want to use to identify this group.  
This name is displayed in the Devices panel. You can change this name at any time, after you save this group.
5. In the **Description** field, type a description for this group.  
For example, `BIG-IP devices located in Seattle`.  
You can change this name at any time, after you save this group.
6. For the **Group Type** setting, select **Static Group**.
7. From the **Parent Group** list, select the source for the group you are creating.
8. Click the **Save** button.

The associated managed devices now display in the Device panel, within the group you created.

If you want to further filter specific devices from within this group, you can create a dynamic group.

### Creating a dynamic group of managed devices

You must license, discover devices, and create a static group before you can create a dynamic group.

To filter a static group on specific parameters, you can create a dynamic group. For example, if you have a static group for all devices located in a particular city, you might want to view only those running a specific version of software.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Devices header, click the + icon when it appears, and then select **New Group**.
4. In the **Display Name** field, type the name you want to use to identify this group.  
This name is displayed in the Devices panel. You can change this name at any time, after you save this group.
5. In the **Description** field, type a description for this group.  
For example, `BIG-IP devices located in Seattle`.  
You can change this name at any time, after you save this group.
6. For the **Group Type** setting, select **Dynamic Group**.
7. For the **Source Group** setting, select the static group on which you want to query for results.
8. In the **Search Filter** field, type a term on which you want to filter the group.  
You can filter on a single term or, if you want to filter on more than one parameter, use the standard Open Data Protocol (OData) format.
9. Click the **Save** button.

This dynamic group displays in the Device panel as a child of the associated static group.



---

# Chapter

# 4

---

## Upgrading BIG-IP System Software

---

- *About upgrading BIG-IP system software* |

### About upgrading BIG-IP system software

---

A key feature of BIG-IQ<sup>®</sup> Device is the ability to centrally upgrade your managed BIG-IP<sup>®</sup> devices. Central management of software images means that you can perform upgrades without having to log in to each individual device. Software images can contain new software, upgrades, or hot fixes.

Upgrades are installed to a new volume, retaining the existing configuration so that if the upgrade does not go as planned, you can boot to the current volume and restore the current configuration. While the software image runs, you can continue to perform other administrative tasks.

---

**Important:** Before you can apply a hot fix, you must have installed the base software image to which the hotfix is associated.

---

### 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.

### Upgrading a device

Before you can upgrade a device, you must first download the software image from the F5 Downloads site, <https://downloads.f5.com> to the Images panel.

After you download a new software image, you can upgrade a managed BIG-IP device from version 11.3.0 or later.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Click the arrow next to the device group that contains the device you want to upgrade to expand the group.
4. Click the gear icon next to the device you want to upgrade, and then click **Upgrade Software**.
5. From the **Software Version** list, select the software image to which you want to upgrade this device.
6. Click the **Check** button.  
This initiates a check to ensure that the device is available for upgrade by verifying connectivity.
7. Click the **Upgrade** button to upgrade the device.

## Upgrading a legacy device

Before you can upgrade a device, you must first download the software image from the F5 Downloads site, <https://downloads.f5.com>, to the Images panel.

Before you can manage a legacy device, you must first upgrade it. Legacy devices are BIG-IP® devices running software versions 10.2.0 - 11.2.x.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover on the Devices panel header, click the + sign when it appears, and then click **Upgrade Legacy Device**.
4. In the **IP Address** field, type the IP address for the legacy device that you want to upgrade from a version prior to 11.3.0.
5. In the **Admin User Name** and **Admin Password** fields, type the administrator's user name and password.
6. In the **Root User Name** and **Root Password** fields, type the user name and password for the root user.
7. From the **Software Version** list, select the software image to which you want to upgrade this device.
8. Click the **Check** button.  
This initiates a check to ensure that the device is available for upgrade by verifying connectivity.
9. Click the **Upgrade** button to upgrade the device.



---

# Chapter 5

---

## Templates for Configuration Management

---

- *About configuration templates*
-

## About configuration templates

---

BIG-IQ<sup>®</sup> Device can manage multiple devices simultaneously. These devices can be located in several data centers that may be located in many different locations. To help you easily manage required configuration changes (such as changes to DNS, default gateways, route domains, NTP, or SNMP) for a large number of devices, you can use configuration templates. You define changes once in the configuration template, then push the template out to specified devices. This can save a significant amount of time because you are not required to log in to each device individually.

### Creating a configuration template

You can create a configuration template to deploy a specific configuration to one or more managed devices. Centrally managing these deployments from BIG-IQ Device eliminates the need to log in to each device individually to specify or update a configuration.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Config Templates panel, click the + icon when it appears, and then click **Create Config Template**.
4. In the **Name** and **Description** fields, type a name and a short description to identify this template.
5. From the **Add New Object** list, select the object you want to add to this template, and then click the **Add** button.  
The screen refreshes to display the property fields for the object.
6. In each property field, define the new object property's values.  
You can add additional values for some properties by clicking the + sign next to the property field.  
For specific information about the configuration options for BIG-IP, refer to the BIG-IP system documentation.
7. For each property, select one of the following:

<b>Option</b>	<b>Description</b>
<b>Fixed</b>	The value you define for this option is fixed. A user cannot change this value when deploying the template.
<b>Optional</b>	The value you define for this option is the default. A user can leave this default or specify their own value when deploying the template.
<b>Required</b>	You do not define a value for this option. The user must specify a value when they deploy the template.

You provide specific self IP addresses when you deploy this template.

8. After you add all of the objects you want to this template, click the **Save** button located on the panel header.

This template is now available for deployment to managed BIG-IP<sup>®</sup> devices.

### Applying a configuration template to a managed device

You must create a configuration template before you can apply it to a discovered device.

Applying a configuration template saves time when you want to make a similar change to several managed BIG-IP® devices.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device to which you want to apply a configuration template by clicking the arrow next to it.
4. Click the gear icon next to the device you want to apply this template, and then click **Apply Config Template**.
5. From the **Name** field, select the name for this configuration template deployment.
6. Click the **Deploy** button.

BIG-IQ® Device applies this configuration to the specified BIG-IP devices.



---

# Chapter

# 6

---

## UCS File Backup and Restoration

---

- *About UCS files*
-

## About UCS files

---

The configuration details of managed devices (including the BIG-IQ<sup>®</sup> 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<sup>®</sup> 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. You can create backup UCS archives for managed devices on demand, or at scheduled intervals.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Backups panel, click the + icon when it appears, and then click **Add Backup**.
4. In the **Description** field, type a description to identify this UCS backup file.
5. From the **Device** list, select the device or device group 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, and type the password in the **Passphrase** and **Verify Passphrase** fields.
8. To retain scheduled backups, for the **Archiving** setting, select the preferred method.
  - a) If you select **Local**, specify a valid BIG-IQ Device directory on which to save the file.
  - b) If you select **SCP** or **SFTP**, specify the server's user name, IP address, valid directory to which to save the file, and the user's password.
9. To delete archived backups, in the **Delete backups** field, specify the number of days to keep the backup before deleting it.
10. To archive scheduled backups indefinitely, select the **Never Delete** check box.
11. To immediately create a backup the UCS file for the selected device, for the **Schedule Backup** setting, select **Backup Now**.
12. To schedule a backup of the UCS file at regular intervals, select **Daily**, **Weekly**, or **Monthly** for the **Schedule Backup** setting.
  - a) If you selected **Weekly**, select the check box next to the day of the week you want BIG-IQ Device to create the backup.
  - b) If you selected **Monthly**, specify the day of the month you want BIG-IQ Device to create the backup.
13. For scheduled backups, place the cursor in the **Start Date** field, click the left mouse button, and click a day on the calendar on which you want to start this schedule.  
Alternatively, you can click the **Today** button located at the bottom of the calendar.

14. In the associated field, type the time you want BIG-IQ Device to start this scheduled backup.
15. To specify an end date for the scheduled backup, click the cursor in the **End Date** field, and then click a date on the calendar.
16. To run scheduled backups indefinitely, select the **No End Date** check box.
17. Click the **Create** button
18. To view the status of a scheduled backup or change its description, click the gear icon.

This UCS backup file is now available for restoration.

## Restoring a UCS file backup

You must create a backup of a device's UCS file before you can restore it.

In the event of a system failure or a requirement to roll back to a previous configuration, you can easily restore a backed up UCS file without having to recreate all of a device's content.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover on the Backups panel, click the gear icon next to the backup that you want to restore, and then click **Properties**.
4. To change the target device, click the **Change Device** button and select a device from the **Device** list.
5. Click the **Restore** button.

The BIG-IQ system restores the saved UCS backup file to the associated device.



---

# Chapter

# 7

---

## SSL Certificate Monitoring

---

- *About SSL certificate monitoring*
- *Monitoring SSL certificate expiration dates*

### About SSL certificate monitoring

---

When you manage BIG-IP® devices that load balance SSL traffic, you must monitor both their SSL traffic and SSL system certificates. *Traffic certificates* are server certificates that a device uses for traffic management tasks. *System certificates* are the web certificates that allow client systems to log in to the BIG-IP Configuration utility.

BIG-IQ® Device populates the Certificates panel with details about each certificate on every managed BIG-IP device you discover. This makes it easy to monitor the expiration dates all of your devices' SSL certificates from one location.

### Monitoring SSL certificate expiration dates

---

You must discover at least one device for the Certificates panel to display a device's SSL certificate properties before you can monitor the certificates.

SSL certificates have a set expiry date, and do not automatically renew. For this reason, it is important to monitor the SSL certificate's expiration dates for your managed devices.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Review the Certificates panel.

A yellow icon appears next to any SSL certificates that are either within 30 days of expiring, or have already expired.

4. Click the gear icon next to an SSL certificate to view its properties.

If an SSL certificate is about to expire, or has expired, immediately contact the owner of the device.

---

# Chapter 8

---

## 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<sup>®</sup> 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<sup>®</sup> 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.

### Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ<sup>®</sup> 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<sup>®</sup> 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.

## Adding a remotely-authenticated LDAP 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 **Remote LDAP**.
5. For the **Auth Provider** setting, select the remote LDAP server to use for authorization.
6. In the **Distinguished Name** field, type a name to identify this user.  
The full name can contain a combination of symbols, letters, numbers and spaces.
7. Click the **Add** button.

You can now associate this user with a role.

## Adding a remotely-authenticated RADIUS 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 **Remote RADIUS**.
5. For the **Auth Provider** setting, select the remote RADIUS server to use for authorization.
6. Click the **Add** button.

You can now associate this user with a role.

## Creating a user group

Create a user group to offer individual users access to the same 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 on the User Groups header, click the + icon when it appears, then click **New User Group**.

4. In the **Name** field, type a name for this new user group.
5. For the **Auth Provider Type** setting, select the type of authorization provider for this user group.
6. Click the **Add** button.

You can now associate users with this user group, and the group 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.
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.

Role	Description
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

# 9

---

## BIG-IQ High Availability

---

- *About a high availability active-active cluster*
- *Implementing an active-active high availability configuration*

## 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.*

---

## Implementing an active-active high availability configuration

---

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 10

---

## License Management

---

- *Overview: Licensing options*
  - *About pool licenses*
  - *About utility licenses*
  - *About volume licenses*
-

## Overview: Licensing options

---

You can centrally manage BIG-IP® virtual edition (VE) licenses for a specific set of F5 offerings (for example, BIG-IP LTM® 25M, BIG-IP LTM 200G, and BIG-IP LTM 1G). When a device is no longer needed, you can revoke the license instance and assign it to another BIG-IP VE device. This flexibility keeps operating costs fixed, and allows for a variety of provisioning options. There are three types of options:

- *Pool licenses* are purchased once, and you assign them to a number of concurrent BIG-IP VE devices, as defined by the license. These licenses do not expire.
- *Utility licenses* are purchased as you need them, and billed at a specific interval (hourly, daily, monthly, or yearly).
- *Volume licenses* are prepaid for a fixed number of concurrent devices, for a set period of time.

## About pool licenses

---

Pool licenses are purchased for a particular product offering for a fixed number of devices, but are not permanently tied to a specific device. As resource demands change, you can use BIG-IQ® Device to revoke and reassign those licenses to other BIG-IP® VE devices as required. Pool licenses do not expire.

## Automatically activating a pool license

You must have a base registration key before you can activate a pool license.

Activating a license make it available for assignment to BIG-IP® devices in your network. If the BIG-IQ® system on which you are activating licensing is connected to the public internet, you can automatically activate the pool license.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Pool License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. In the **Add-on Keys** field, paste any additional license key you have.
7. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.  
The License Agreement displays.
8. To accept the License Agreement, click the **Agree** button.
9. Click the **Activate** button.

If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this license to another BIG-IP® device.

## Manually activating a pool license

You must have a base registration key before you can activate the pool license.

Activating a license make it available for assignment to BIG-IP® devices in your network. If the BIG-IQ® system on which you are activating licensing is not connected to the public internet, you can activate the pool license manually.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Pool License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. In the **Add-on Keys** field, paste any additional license key you have.
7. 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.
8. 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/>.

9. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
10. To accept the License Agreement, click the **Agree** button.
11. Click the **Activate** button.

If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this license to another BIG-IP® device.

## Assigning a pool license to a BIG-IP VE

Before you can assign a pool license to a BIG-IP® VE device, you must activate the license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign the license.

Pool licenses provide you with the flexibility to easily manage resources and operating costs. Use this procedure if you have activated a pool license, but have not yet assigned it to a BIG-IP VE.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device you want to license by clicking the arrow next to it. The panel expands to display the list of devices contained in this group.
4. Click the gear icon next to the device you want to license, and then click **License Device**.
5. In the **Name** field, type a name for this license.
6. From the **Licensing** list, select **Use a Pool License**.
7. From the **Pool License** list, select the pool license you want to assign to this device.
8. Click the **Deploy** button.

9. To confirm that the license was successfully deployed, click the gear icon next to the license you deployed, click **Properties**, and then click **Assignments**.  
The device you licensed displays with the license status and the last contact from the BIG-IQ system.

### Revoking a pool license from a BIG-IP VE

If traffic decreases to the applications on some of your managed BIG-IP® devices, you can use BIG-IQ® Device to revoke those licenses and assign them to other resources as needed.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device for which you want to revoke a license by clicking the arrow next to it.
4. Click the gear icon next to the device for which you want to revoke a license, and then click **License Device**.
5. From the **Licensing** list, select **Revoke a License**.
6. Click the **Deploy** button.

You can now assign this license to another BIG-IP® device.

### About utility licenses

---

You are charged for utility licenses only for the duration that the license is activated. You can activate any number of licenses as you need them, specifying the interval (an hour, a day, a month, or a year) at which you want to be billed for each. BIG-IQ® Device tracks license usage in each billing period, and sends that data directly to F5. When a resource is no longer required, you revoke its license and are no longer charged for that instance until you reassign it to another BIG-IP VE device. Utility licenses can be particularly useful when traffic to certain applications increases for a short period of time, for example, during fiscal year end.

### Automatically activating a utility license

You must have a base registration key before you can activate the utility license.

If the resources you are licensing are connected to the public internet, you can automatically activate the utility license.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Utility License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.  
The License Agreement displays.
7. To accept the License Agreement, click the **Agree** button.
8. Click the **Activate** button.

If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this utility license to a BIG-IP® device.

## Manually activating a utility license

You must have a base registration key before you can activate the utility license.

Activating a utility license is the first step to making it available for assignment to BIG-IP® devices in your network. If the BIG-IQ® system on which you are activating licensing is not connected to the public internet, you can activate the utility license manually.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Utility License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. 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.
7. 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/>.
8. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
9. Select the check box next to the Accept User Legal Agreement to agree to the license terms, and then click the **Next** button.  
The license key displays
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Apply** button at the top of the panel.

You must now activate each individual utility license offering.

## Manually activating offering licenses

Before you can activate the individual offering licenses, you must first activate the license itself.

Activating the offering licenses makes them available for assignment.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the arrow next to the license you previously activated. The list expands to display the license offerings associated with this license.
4. Hover over an offering license and click the gear icon when it appears.
5. 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/>.

6. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
7. Copy the license key.
8. On BIG-IQ Device, into the **License Text** field, paste the license key.
9. Click the **Apply** button at the top of the panel.

You can now assign this offering license to a BIG-IP® VE device.

### Assigning a utility license to a BIG-IP device

Before you can assign a utility pool to a BIG-IP® VE device, you must activate the utility license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign a pool license.

Using a utility license for a BIG-IP VE device provides you with the flexibility to easily manage resources and operating costs by choosing a specific billing term for licenses.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device you want to license by clicking the arrow next to it.  
The panel expands to display the list of devices contained in this group.
4. Click the gear icon next to the device you want to license, and then click **License Device**.
5. In the **Name** field, type a name for this license.
6. From the **Licensing** list, select **Use a Utility License**.
7. From the **Utility License** list, select the license you want to assign to this device.
8. From the **Offering License** list, select the specific product offering you want to assign to this device.
9. From the **Unit Of Measure** list, select the interval at which you want to be billed for this license.
10. Click the **Deploy** button.

### Downloading a utility license usage report

You must assign a utility license to a device before you can create a utility usage report for that license.

You can use this report to augment your internal licensing management and budget planning. You also have the option to submit this report manually to F5 for billing purposes.

---

***Note:** If you would like to manually submit this report to F5 for billing purposes instead of automatically, contact F5 Support.*

---

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the gear icon for the utility license for which you want to download a usage report, and then click **Create Usage Report**.
4. For the **Period** setting, in the **From** and **To** fields, type the date range for the report. Alternatively, click the calendars and navigate to the dates.
5. Select a format option for the report.
6. Click the **Download** button and select an option to open the file, or save the file.

## Automatically submitting a utility license usage report to F5

You must assign a utility license to a device before you can submit and save a usage report.

You provide this report to F5 Networks for billing purposes, as per the terms and conditions of your contract.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the gear icon for the utility license that you want to submit for billing, and then click **Create Usage Report**.
4. For the usage submission method, select **Automatically submit report to F5**.
5. Click the **Submit** button.  
BIG-IQ Device sends a report directly to F5, and saves a copy on BIG-IQ Device.

## Revoking a utility license from BIG-IP VE

If traffic decreases to the applications on some of your managed BIG-IP® devices, you can use BIG-IQ® Device to revoke those licenses and assign them to other resources as needed.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device for which you want to revoke a license by clicking the arrow next to it.
4. Click the gear icon next to the device for which you want to revoke a license, and then click **License Device**.
5. From the **Licensing** list, select **Revoke a License**.
6. Click the **Deploy** button.

You can now assign this license to another BIG-IP® device.

## About volume licenses

---

With volume licenses, you can flexibly manage BIG-IP® VE devices by purchasing a number of prepaid, concurrent licenses. If your needs change throughout the year, you have the option of purchasing more prepaid licenses in increments of 50. BIG-IQ® Device helps you track and distribute these various licenses as required by the applications your customers are using, and notifies you when you reach your prepaid limit. When you revoke a license, you can then assign it to another BIG-IP VE device.

## Automatically activating a volume license

You must have a base registration key before you can activate the volume license.

If the resources you are licensing are connected to the public internet, you can automatically activate the volume license.

1. Log in to BIG-IQ Device with your administrator user name and password.

2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Volume License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button. The License Agreement displays.
7. To accept the License Agreement, click the **Agree** button.
8. Click the **Activate** button.  
If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this volume license to a BIG-IP® device.

### Manually activating a volume license

You must have a base registration key before you can activate the volume license.

If the resources you are licensing are not connected to the public internet, you can still activate the utility license manually.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses header, click the + icon when it appears, and then click **Add New Volume License**.
4. In the **License Name** field, type the name you want to use to identify this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. 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.
7. 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/>.
8. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
9. Select the check box next to the Accept User Legal Agreement to agree to the license terms, and then click the **Next** button.  
The license key displays
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Add** button.  
The unactivated volume license displays in the Licenses panel.
13. Click the arrow next to the volume license you created to expand the list of licenses.
14. Click the volume license you want to activate.
15. Copy the license key.
16. On BIG-IQ Device, into the **License Text** field, paste the license key.
17. To accept the License Agreement, click the **Agree** button.
18. Click the **Activate** button.

If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this volume license to a BIG-IP® VE device.

### Manually activating offering licenses

Before you can activate the individual offering licenses, you must first activate the license itself.

Activating the offering licenses makes them available for assignment.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the arrow next to the license you previously activated. The list expands to display the license offerings associated with this license.
4. Hover over an offering license and click the gear icon when it appears.
5. 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/>.
6. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
7. Copy the license key.
8. On BIG-IQ Device, into the **License Text** field, paste the license key.
9. Click the **Apply** button at the top of the panel.

You can now assign this offering license to a BIG-IP® VE device.

### Assigning a volume license to a BIG-IP VE

Before you can assign a volume license to a BIG-IP® VE device, you must activate the volume license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign a volume license.

Using a volume license for a BIG-IP VE device provides you with the flexibility to easily manage resources and operating costs by choosing only those features you want to use on the managed BIG-IP VE device.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device you want to license by clicking the arrow next to it.  
The panel expands to display the list of devices contained in this group.
4. Click the gear icon next to the device you want to license, and then click **License Device**.
5. In the **Name** field, type a name for this license.
6. From the **Licensing** list, select **Use a Volume License**.
7. Click the **Deploy** button.

### Revoking a volume license from a BIG-IP VE

If traffic decreases to the applications on some of your managed BIG-IP® devices, you can use BIG-IQ® Device to revoke those licenses and assign them to other resources as needed.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device for which you want to revoke a license by clicking the arrow next to it.
4. Click the gear icon next to the device for which you want to revoke a license, and then click **License Device**.
5. From the **Licensing** list, select **Revoke a License**.
6. Click the **Deploy** button.

You can now assign this license to another BIG-IP® device.

# Index

## A

- active-active cluster
  - configuring for the BIG-IQ system [54](#)
- active-active pair
  - configuring for the BIG-IQ system [54](#)
- admin, *See* administrator
- administrator
  - specifying global user settings for [20](#)
- Administrator role
  - defined [50](#)
- administrator user
  - changing password for [48](#)
- administrator user password
  - changing [48](#)
- asset management
  - for devices [26](#)

## B

- backups
  - about [42](#)
  - for UCS files [42](#)
- backup schedule
  - creating [42](#)
- backup UCS files
  - restoring [43](#)
- BIG-IP devices
  - downloading software image for upgrades [34](#)
  - installing BIG-IQ system components [22](#)
  - viewing trust certificates BIG-IP in a device service clustering [28](#)
- BIG-IP device service clustering properties
  - viewing [28](#)
- BIG-IQ Cloud
  - finding documentation for [18](#)
- BIG-IQ Device
  - about [18](#)
  - finding documentation for [18](#)
- BIG-IQ Security
  - finding documentation for [18](#)
- BIG-IQ system
  - downloading software image for [34](#)
  - reordering panels [19](#)
- BIG-IQ system components
  - installing on BIG-IP devices [22](#)
- billing
  - for utility licenses [61](#)

## C

- certificate expiration dates
  - monitoring [46](#)
- clusters
  - for high availability [54](#)
- config template
  - creating [38](#)

- configurations
  - about changing for devices [38](#)
  - about creating backups [42](#)
  - backing up [42](#)
  - creating a template [38](#)
  - deploying with a template [38](#)
  - modifying for devices [27](#)
- configuration templates
  - about [38](#)
  - applying [38](#)
  - creating [38](#)
- CSV file
  - uploading for bulk device discovery [26](#)

## D

- default screen
  - specifying for BIG-IQ system administrator [20](#)
- device backup
  - about [42](#)
  - and USC files [42](#)
- device configurations
  - modifying [27](#)
- device discovery
  - using CSV a file for bulk discovery [26](#)
- device groups
  - about dynamic [29](#)
  - about static [29](#)
- device inventory
  - about [24](#)
  - viewing details [26](#)
- device management
  - about [24](#)
  - modifying configurations [27](#)
- Device Manager role
  - defined [50](#)
- devices
  - about discovering [24](#)
  - adding [24](#)
  - backing up [42](#)
  - discovering [24](#)
  - upgrading [34–35](#)
- Device Service Clustering [28](#)
- See also* DSC
  - defined [28](#)
  - See also* DSC
- device status
  - viewing for BIG-IP devices in a device service clustering [28](#)
- discovery
  - using a CSV file for bulk device discovery [26](#)
- documentation, finding [18](#)
- DSC [28](#)
- See also* Device Service Clustering
  - defined [28](#)
  - See also* Device Service Clustering
- DSC devices
  - synchronization options [29](#)

DSC devices (*continued*)

synchronizing 29

DSC groups

viewing configurations for 29

dynamic device groups

about 29

dynamic group

creating 30

## E

exportation of inventory details 26

## F

failover 54

filtering process

finding associated objects 19

## G

global user settings

specifying for administrator 20

groups

about dynamic device groups 29

about static device groups 29

creating dynamic 30

creating static 30

guides, finding 18

## H

HA, See high availability cluster

high availability cluster

configuring 54

high availability configuration

about 54

## I

installation

of required system components 22

inventory details

exporting to CSV file 26

viewing for devices 26

IP addresses

for managed devices 24

## L

LDAP authentication

configuring for new user 49

legacy devices

upgrading 35

license

activating pool license 56

adding pool license 56

manually activate a pool license 57

licenses

about managing for devices 56

about pool licenses 56

licenses (*continued*)

about utility licenses 58

about volume licenses 61

assigning a volume license 63

assigning utility 60

for pools 57

revoking a volume license for managed device 64

revoking for managed device 58, 61

licensing

activating a utility license automatically 58

activating a volume license automatically 61

activating a volume license manually 62

activating pool license automatically 56

activating utility license manually 59

assigning a volume license to BIG-IP devices 63

assigning utility license to BIG-IP devices 60

for managed devices 56, 58, 61

for pool license 56

for pools for BIG-IP devices 57

manually activating pool license manually 57

## M

managed devices

about discovering 24

about upgrading software 34

manual activation

for pool license 57

manuals, finding 18

## N

Network Security Deploy role

defined 50

Network Security Edit role

defined 50

Network Security Manager role

defined 50

Network Security View role

defined 50

## O

objects

finding associations 19

searching for 19

offering licenses

activating for a license 59, 63

## P

panels

reordering 19

password

changing for administrator user 48

pool license

activating automatically 56

activating manually 57

adding 56

revoking for a BIG-IP device 58, 61

- pool licenses
  - about [56](#)
  - assigning to a BIG-IP device [57](#)

## R

- RADIUS authentication
  - configuring for new user [49](#)
- release notes, finding [18](#)
- reports
  - for asset management [26](#)
  - for utility license [60](#)
  - for utility license billing [61](#)
- required system components
  - installing BIG-IQ components [22](#)
- roles
  - associating with users and user groups [51](#)
  - defined [48](#)
  - for users [48, 50](#)

## S

- search function
  - finding specific objects [19](#)
- Security Manager role
  - defined [50](#)
- software
  - upgrading [34](#)
  - upgrading for devices [34–35](#)
- software images
  - downloading [34](#)
- software upgrade
  - about managed devices [34](#)
- SSL certificates
  - about [46](#)
  - monitoring [46](#)
- static device groups
  - about [29](#)
- static group
  - creating [30](#)
- status
  - for BIG-IP devices in a device service clustering [28](#)
- synchronization
  - for devices in a DSC configuration [29](#)
- synchronization options
  - for devices in a DSC configuration [29](#)
- system certificate [46](#)
- system user
  - adding [48](#)
  - adding LDAP authenticated user [49](#)
  - adding RADIUS authenticated user [49](#)

## T

- templates
  - about configuration templates [38](#)
- timeout
  - specifying for BIG-IQ system administrator [20](#)
- traffic certificates
  - defined [46](#)

- trust certificates
  - verifying for BIG-IP in a device service clustering [28](#)
- trust domain details
  - viewing for BIG-IP in a device service clustering [28](#)

## U

- UCS file
  - about [42](#)
  - defined [42](#)
- UCS files
  - creating backup [42](#)
  - restoring from backup [43](#)
- Upgrade Advisor
  - about [34](#)
  - using [35](#)
- upgrades
  - downloading software image [34](#)
- user configuration set, See UCS file
- user groups
  - creating [49](#)
  - defined [48](#)
- user interface
  - and searching for specific objects [19](#)
  - customizing [19](#)
  - navigating [19](#)
- user roles
  - about [50](#)
  - associating with users and user groups [51](#)
- users
  - adding [48–49](#)
  - defined [48](#)
  - removing role from [51](#)
- utility license
  - activating an offering license for [59, 63](#)
  - activating automatically [58](#)
  - activating manually [59](#)
  - assigning to a BIG-IP device [60](#)
  - submitting usage report [61](#)
- utility license reports
  - downloading [60](#)
- utility licenses
  - about [58](#)

## V

- volume license
  - activating automatically [61](#)
  - activating manually [62](#)
  - assigning to a BIG-IP device [63](#)
  - revoking for a BIG-IP device [64](#)
- volume licenses
  - about [61](#)

## W

- Web App Security Manager role
  - defined [50](#)

