Enterprise Manager™ Getting Started Guide

Version 3.1.1

Table of Contents

Legal Notices

Publication Date

This document was published on March 20, 2015.

Publication Number

MAN-0384-03

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Gabriel Forté.

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

This product includes software with glib library utility functions, which is protected under the GNU Public License.

This product includes software with grub2 bootloader functions, which is protected under the GNU Public License.

This product includes software with the Intel Gigabit Linux driver, which is protected under the GNU Public License. Copyright ©1999 - 2012 Intel Corporation.

This product includes software with the Intel 10 Gigabit PCI Express Linux driver, which is protected under the GNU Public License. Copyright ©1999 - 2012 Intel Corporation.

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 software under license from Qosmos (www.qosmos.com).

This product includes software developed by Andrew Tridgell, which is protected under the GNU Public License, copyright ©1992-2000.

IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes GRand Unified Bootloader (GRUB) software developed under the GNU Public License, copyright ©2007.

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

This product includes gd-libgd library software developed by the following in accordance with the following copyrights:

- Portions copyright ©1994, 1995, 1996, 1997, 1998, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.
- Portions copyright ©1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.
- Portions relating to GD2 format copyright ©1999, 2000, 2001, 2002 Philip Warner.
- Portions relating to PNG copyright ©1999, 2000, 2001, 2002 Greg Roelofs.
- Portions relating to gdttf.c copyright ©1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).
- Portions relating to gdft.c copyright ©2001, 2002 John Ellson (ellson@lucent.com).
- Portions copyright ©2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 2008 Pierre-Alain Joye (pierre@libgd.org).
- Portions relating to JPEG and to color quantization copyright ©2000, 2001, 2002, Doug Becker and copyright ©1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group.
- Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande. Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

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

1. Java Technology Restrictions. Licensee shall not create, modify, change the behavior of, or authorize licensees of licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developer.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icon including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at http://www.oraclc.com/html/3party.html; (b) not do anything harmful to or inconsistent with Oracle's rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.
3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portion of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.
5. Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table I-I (Commercial Features In Java SE Product Editions) of tile Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

This product includes utilities developed by Linus Torvalds for inspecting devices connected to a USB bus.

This product includes perl-PHP-Serialization software, developed by Jesse Brown, copyright ©2003, and distributed under the Perl Development Artistic License (http://dev.perl.org/licenses/artistic.html).

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 software developed by Trent Richardson, distributed under the MIT License. Copyright ©2012 jQuery Foundation and other contributors (http://jquery.com/).

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 software developed by Allan Jardine, distributed under the MIT License. Copyright ©2008 - 2012, Allan Jardine, all rights reserved, jQuery Foundation and other contributors (http://jquery.com/).

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 software developed by Douglas Gilbert. Copyright ©1992 - 2012 The FreeBSD Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``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 FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,

DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

This product includes software developed as open source software. Copyright ©1994 - 2012 The FreeBSD Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. 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 WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Copyright ©1998 - 2011 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``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 THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(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 software developed by Sony Computer Science Laboratories Inc. Copyright © 1997-2003 Sony Computer Science Laboratories 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:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.

THIS SOFTWARE IS PROVIDED BY SONY CSL 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 SONY CSL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

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

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

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

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

This product includes software developed by McAfee®.

This product includes software developed by Ian Gulliver ©2006, which is protected under the GNU General Public License, as published by the Free Software Foundation.

This product contains software developed by the RE2 Authors. Copyright ©2009 The RE2 Authors. 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 Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

This product includes the Zend Engine, freely available at http://www.zend.com.

This product includes software developed by Digital Envoy, Inc.

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

This product contains software developed by Erik Arvidsson and Emil A Eklund.

This product contains software developed by Aditus Consulting.

This product contains software developed by Dynarch.com, which is protected under the GNU Lesser General Public License, version 2.1 or later.

This product contains software developed by InfoSoft Global (P) Limited.

This product includes software written by Steffen Beyer and licensed under the Perl Artistic License and the GPL.

This product includes software written by Makamaka Hannyaharamitu ©2007-2008.

Rsync was written by Andrew Tridgell and Paul Mackerras, and is available under the GNU Public License.

This product includes Malloc library software developed by Mark Moraes. (©1988, 1989, 1993, University of Toronto).

This product includes open SSH software developed by Tatu Ylonen (ylo@cs.hut.fi), Espoo, Finland (©1995).

This product includes open SSH software developed by Niels Provos (©1999).

This product includes SSH software developed by Mindbright Technology AB, Stockholm, Sweden, www.mindbright.se, info@mindbright.se (©1998-1999).

This product includes free SSL software developed by Object Oriented Concepts, Inc., St. John's, NF, Canada, (©2000).

This product includes software developed by Object Oriented Concepts, Inc., Billerica, MA, USA (©2000).

This product includes free software developed by ImageMagick Studio LLC (©1999-2011).

This product includes software developed by Bob Withers.

This product includes software developed by Jean-Loup Gaily and Mark Adler.

This product includes software developed by Markus FXJ Oberhumer.

This product includes software developed by Guillaume Fihon.

This product includes QPDF software, developed by Jay Berkenbilt, copyright ©2005-2010, and distributed under version 2 of the OSI Artistic License (http://www.opensource.org/licenses/artistic-license-2.0.php).

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 software developed by Douglas Crockford, douglas@crockford.com.

This product includes ec2-tools software, copyright © 2008, Amazon Web Services, and licensed under the Amazon Software License. A copy of the License is located at http://aws.amazon.com/asl/ .

This product includes the ixgbevf Intel Gigabit Linux driver, Copyright © 1999 - 2012 Intel Corporation, and distributed under the GPLv2 license, as published by the Free Software Foundation.

Chapter 1

Enterprise Manager Overview

Overview of Enterprise Manager

Enterprise Manager™ is an appliance that helps you streamline the administrative tasks associated with managing multiple network devices. These administrative tasks include: performance monitoring, software installation and upgrades, configuration archival and restoration, certificate monitoring, security policy management, software image storage, and user account management. Enterprise Manager works in many types of network topologies, including those in multi-tiered configurations containing multiple firewalls.

You can use Enterprise Manager to manage networks with devices running the following software.

- BIG-IP® system version 9.3 and later
- BIG-IP® Local Traffic Manager™ Virtual Edition (VE) version 10.2 and later
- BIG-IP® Secure Access Manager™ version 8.0 and later
- WANJet® version 5.0 and later
- Enterprise Manager™ version 1.0 and later

Note: *Although Enterprise Manager works with previous software releases, we recommend that you upgrade your managed devices to the current software version to ensure optimal performance.*

Additional resources and documentation for Enterprise Manager

You can access all of the following Enterprise Manager™ documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`. The procedures and examples described in all documentation and online help are written for administrator-level users with full access (non-restricted) privileges to Enterprise Manager.

Document	Description
Enterprise Manager™ Getting Started Guide	This guide provides you with the basic concepts and tasks required to set up your Enterprise Manager and start managing devices.
Enterprise Manager™: Monitoring Network Health and Activity	This guide contains information to help use iHealth® for diagnostics purposes, monitor log events using LogIQ, track certificates, create alerts for events, run reports, and manage statistics storage.
Enterprise Manager™: Working with Changesets and Templates	This guide provides information specific to working with changesets and templates.
Enterprise Manager™: Managing Configuration Files	This guide contains instructions about how to store configuration data (UCS), including how to create an archive schedule, as well as information about restoring a UCS archive and comparing configurations.
Platform Guide: Enterprise Manager™ 4000	This guide includes Enterprise Manager system hardware platform specifications, installation instructions, and important environmental warnings.
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, as well as installation and upgrade instructions.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

About incorporating Enterprise Manager into your network

You incorporate Enterprise Manager™ into your network as you would any F5 Networks device. However, because it requires bilateral communication with each device for successful management, Enterprise Manager must have open communication with your devices and be able to translate a device's IP address into an address it can use. The most common network configurations for address translation are:

Tiered network, BIG-IP® Local Traffic Manager™ performs address translation
Where a device manages load balance requests for multiple devices and translates the IP addresses for those devices through a firewall

Tiered network, a SNAT performs network translation
Where a device (located in front of Enterprise Manager) load balances requests for multiple devices, and a SNAT translates the IP addresses for those devices

Ports required for two-way communication

For Enterprise Manager™ to properly manage devices, the following ports are open by default to allow for the required two-way communication.

Open Port	Purpose
443	For communication between managed devices and the Enterprise Manager system, for the purpose of device management.
4353	For communication between Enterprise Manager and a managed device's `big3d` agent, for the purpose of statistics collection.
3306	For communication between Enterprise Manager and a remote statistics database, for the purpose of storing and reporting statistics.

About best practices for management network topology

Device communication and management is performed through the following interfaces.

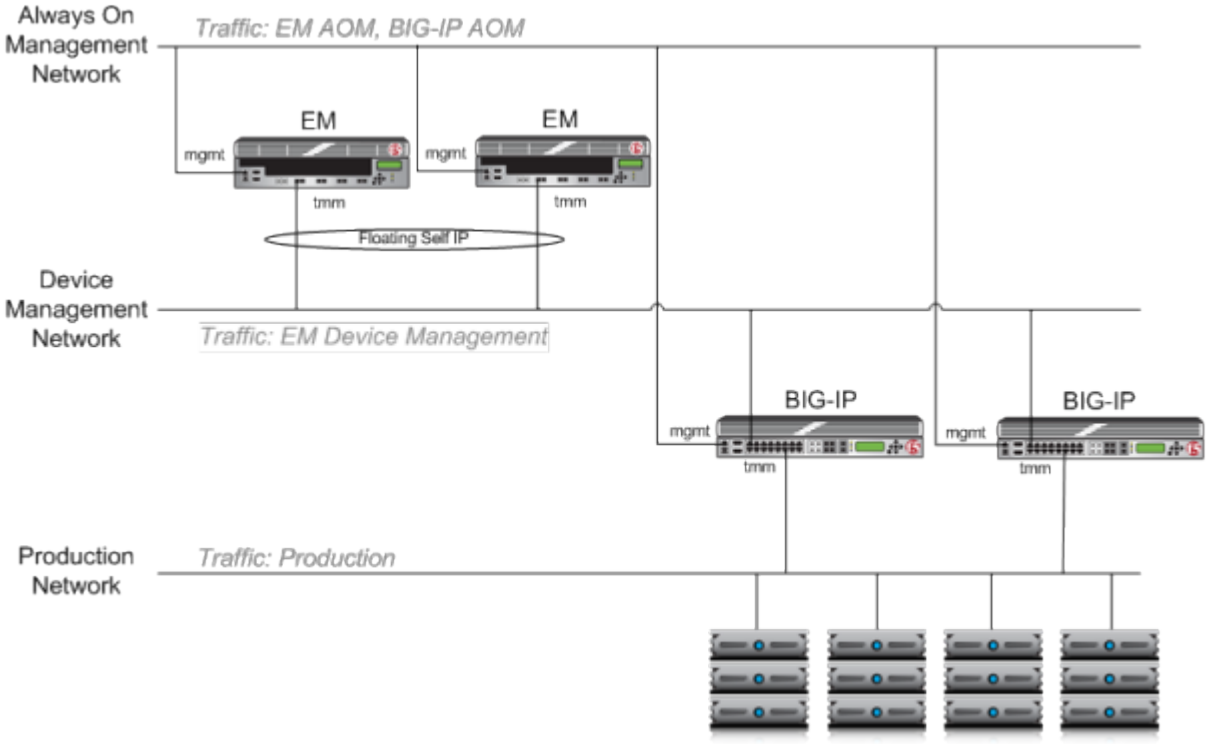
Traffic Management Microkernel (TMM) interfaces
For each of the following processes, you must dedicate a TMM interface to perform:

- Application traffic and load balancing
- Communication between Enterprise Manager™ and managed devices
- Communication between systems in a high availability configuration (for both static and floating self IP address support)

Management (MGMT) interface
Used by F5 devices for administrative traffic and for the Always-On Management (AOM) subsystem, which enables you to manage a system remotely using SSH or serial console, even if the host is powered down. Devices do not forward user application traffic, such as traffic slated for load balancing, through this interface.

Important: *The device's IP address is used for communication between Enterprise Manager and the device. F5 recommends that you use a self IP address for access to additional functionality that is not provided through the management port.*

Figure 1: Illustration of example management network topology



Tip: *Place the Enterprise Manager system on a management subnet that is separate from traffic management to keep device management and communication independent from traffic management activities.*

Chapter 2

Initial Setup and Configuration

Overview: Initial setup tasks and device discovery

After you configure one or more F5® devices in your network and determine how you want to incorporate Enterprise Manager™, you can perform specific tasks to complete the initial setup of the Enterprise Manager and discover devices in your network.

Task summary

Activating the Enterprise Manager license

To activate the system's license, you must have access to the command line and the base registration key. The base registration key is a character string that the license server uses to verify the type and number of F5 Networks products that you are entitled to license. If you do not have a base registration key, contact the F5 Networks sales group (`http://www.f5.com`).

You license the system from the License screen of the Setup Utility.

1. From a workstation attached to the network on which you configured the management interface, type the following URL syntax where `<management_IP_address>` is the address you configured for device management: `https://<management_IP_address>`.
2. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**.
   The Setup utility screen opens.
3. Click **Activate**.
   The License screen opens.
4. In the **Base Registration Key** field, paste the registration key.
5. Click **Next**.
   The End User License Agreement (EULA) displays.
6. Review the EULA.
   When you click **Accept**, the Platform screen opens.

Specifying initial configuration settings

You specify the initial configuration settings from the Setup Utility Platform screen.

1. For the **Management Port Configuration** setting, select **Manual**.
2. For the **Management Port** setting, type the IP address, network mask, and the management route.
3. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.

   The FQDN can consist of letters, numbers, and/or the characters underscore (_), dash (-), or period (.).
4. For the **Host IP Address** setting, retain the default value of **Use Management Port IP Address**.
5. For the **High Availability** setting, select an option.

   Keep in mind that this high availability functionality is different than this device service clustering configuration of a BIG-IP® system. Here, the high availability feature provides access to a current backup of the system's configuration. Review the considerations before selecting this option.
6. From the **Time Zone** list, select the time zone for this system.

7. For the **Root Account** setting, type and confirm a password for the `root` account.
   The `root` account provides console access only.
8. For the **Admin Account** setting, type and confirm a password.
9. For the **SSH Access** setting, select or clear the check box.
10. For the **SSH IP Allow** setting, specify a range of addresses.
11. Click **Next**.
    The system terminates your login session.
12. Log in to the system again using the new password that you specified.
    The Network screen opens.

Tip: *If you need to reconfigure any of the basic configuration settings, you can click the* ***Run the Setup Utility*** *link from the Configuration utility's Welcome screen. To access the Welcome screen, click the About tab.*

Configuring a standard network

After you specify the initial configuration settings and when you click **Next** from the Network screen, the Basic Network Configuration wizard screen opens.

You perform these steps to continue through the configurations screens, and specify the settings for the internal and external VLANs. For additional information about the settings on these screens, click the Help tab.

1. Select an option for high availability:

Option	Description
To use Enterprise Manager in a high availability configuration	Select the **Config Sync** and **High Availability** check boxes, and select an option for the **Failover Method** setting
If you are not using Enterprise Manager in a high availability configuration	Clear the **Config Sync** and **High Availability** check boxes

   If you choose to use Enterprise Manager™ in a high availability configuration, you must review the considerations and prepare your network for a high availability configuration.
2. Click **Next**.
   This displays the screen for configuring the default VLAN **internal**.
3. For the **Self IP** setting, in the **Address** and **Netmask** fields, type the IP addresses specific to the Enterprise Manager system.
4. For the **Port Lockdown** setting, retain the default **Allow Default** to ensure that the required ports are open for communication between the Enterprise Manager and the managed devices.
5. For the **VLAN Interfaces** settings, you can specify the interfaces you want this VLAN to use for traffic management.
6. Click **Next**.
   The external VLAN screen opens.
7. For the **Self IP** setting, in the **Address** and **Netmask** fields, type the IP addresses specific to the Enterprise Manager system.
8. For the **Port Lockdown** setting, retain the default **Allow Default** to ensure that the required ports are open for communication between the Enterprise Manager and the managed devices.

9. For the **VLAN Tag ID** option, retain the default **auto** to allow Enterprise Manager to select one for you, or type a value in the field between 1 and 4094.
10. In the **Default Gateway** field, type the IP address or route of the default gateway.
11. For the **VLAN Interfaces** settings, you can specify the interfaces you want this VLAN to use for traffic management.
12. If you are configuring a high availability system, click **Next**. Otherwise, click **Finished** to save this configuration.

About using Enterprise Manager in a high availability configuration

Using Enterprise Manager™ in a high availability configuration (optional) is different than a BIG-IP®device service clustering configuration. The main function of Enterprise Manager in a high availability configuration is to provide a warm backup of an active system. A *warm backup* is a standby peer system on which you duplicate the configuration information of the active Enterprise Manager, and can perform all of the functions of its peer, but requires manual intervention to maintain the integrity of the backup configuration information.

When Enterprise Manager is configured for high availability, you back up the Enterprise Manager configuration (including device, alert, archive, certificate, and software repository information) to a standby system. In the event that the active system becomes unavailable, you can fail over to that system.

Important: *You must perform regular backups of the active system to the standby system to maintain the integrity of its configuration.*

Considerations for Enterprise Manager in a high availability configuration

The high availability features for Enterprise Manager™ are not the same as the device service clustering feature associated with a BIG-IP® system. Before using Enterprise Manager in a high availability configuration, it is important to review these considerations and details.

Consideration	Details
You must use Enterprise Manager only in active-standby mode for high availability.	When you specify the high availability settings during the initial configuration, use the active-standby configuration and not the active-active configuration.
The high availability system for Enterprise Manager works differently than the device service clustering feature for the BIG-IP system. Enterprise Manager does not automatically synchronize, in real time, user-configured or scheduled tasks (such as a software installation or archiving tasks). After a failover, the newly active system maintains the last known configuration before any user-initiated or scheduled task if the systems were properly synchronized.	For a successful failover, you must run a ConfigSync operation after each major configuration change.
Enterprise Manager contains all of the configuration details for managed devices in your networks, so there is more information to synchronize with its peer. Therefore, the ConfigSync process for an Enterprise Manager high availability configuration	To verify synchronization after you start a ConfigSync task, check the status of the target device to which you are copying the configuration. If a maintenance task appears in the task list, the ConfigSync task is not complete.

Consideration	Details
is considerably longer than a similar synchronization process on a BIG-IP device. The ConfigSync task might display as complete before the process has finished.	
If a task is running during a failover, the task does not continue when the standby peer becomes the active peer.	If you discover a task was running at the time you ran the ConfigSync task, you must re-start that task on the peer when it becomes active.
You cannot make configuration changes to Enterprise Manager when it is in standby mode, such as adding devices, importing software, or configuring alerts on the standby device. If you attempt to make a configuration change to Enterprise Manager when it is in standby mode, you will receive an error.	To ensure that you do not initiate tasks on a standby system, check for an `Active` or `Standby` status message in the upper left corner of the screen.

Preparing your network for a high availability Enterprise Manager system configuration

For two peer systems to properly communicate information about managed devices, you must complete these preparation steps before you start configuring initial settings for the high availability system.

1. Configure at least one static self IP address (instead of using the MGMT interface) to connect to devices.

   This is required because a TMM port can support both static and floating self IP addresses. A floating self IP address is necessary to ensure that the managed devices can communicate with the active device of the Enterprise Manager™ high availability system configuration.
2. Create at least one floating (shared) self IP address on the same network.
3. Configure a default gateway (or route) on the same network as each of the two self IP addresses that you configured.

Your network is now prepared for you to configure Enterprise Manager in a high availability configuration.

Specifying high availability configuration options

Before configuring Enterprise Manager™ as a high availability system, you must license the system and then, on the same network, configure self IP addresses and a gateway or route. You must also be aware of the differences between a high availability configuration for Enterprise Manager and the device service clustering configuration for BIG-IP®.

Use the following steps to specify the options for the each system in a high availability pair.

1. From the High Availability Wizard Options screen, for the **High Availability** setting, select an option.

   The high availability options and screens apply only if you selected to use Enterprise Manager in a high availability network configuration on the first screen of the Setup Utility, and after you have specified the settings for your VLAN configurations. If you have already run the Setup utility previously, you can re-access the High Availability Wizard screen from the About tab, by clicking **Run the Setup Utility** and select the Standard Configuration option.
2. Click **Next**.
3. For the **Self IP** setting, in the **Address** and **Netmask** fields, type the internal IP addresses specific to the Enterprise Manager system.

4. For the **VLAN Tag ID** setting, retain the default **auto** to allow Enterprise Manager to select one for you, or type a value in the field between 1 and 4094.
5. For the **VLAN Interfaces** setting, specify the interfaces you want this VLAN to use for configuration synchronization.
6. Click the **Next** button.
7. For the **Self IP** setting, in the **Address** and **Netmask** fields, type the external IP addresses specific to the Enterprise Manager system.
8. For the **VLAN Tag ID** setting, retain the default **auto** to allow Enterprise Manager to select one for you, or type a value in the field between 1 and 4094.
9. For the **VLAN Interfaces** setting, specify the interfaces you want this VLAN to use for management.
10. Click the **Next** button.
11. For the Self IP setting, in the **Address** and **Netmask** fields, type the IP addresses specific for the high availability VLAN.
12. For the **VLAN Tag ID** setting, retain the default **auto** to allow Enterprise Manager to select one for you, or type a value in the field between 1 and 4094.
13. For the **VLAN Interfaces** setting, specify the interfaces you want this VLAN to use for high availability.
14. From the **Local Address** list, select the local IP address that you want the system to use for ConfigSync operations.
15. Click the **Next** button.
16. Select the check box for the system that you want to use for ConfigSync or failover.
17. To send multicast messages associated with configuration synchronization:
    a) Select the **Use Failover Multicast Address** check box.
    b) Review the multicast address settings and click the **Next** button.

    The Mirroring configuration screen opens.
18. Review the settings and click the **Next** button.
19. Click the **Next** button, then log in to the peer Enterprise Manager system and run the Setup Utility to specify the configuration options for the peer system.

After you run the Setup Utility for the second system in the high availability pair, click the **Finished** button. When you perform the discovery task, the peer systems in the high availability pair will become associated with each other.

Automatically synchronizing configurations for a high availability pair

When you have Enterprise Manager™ configured in a high availability pair, it is important to perform regular synchronization. An effective way to do this is to schedule a configuration synchronization to occur on a regular basis, at a time that will not impact device management activities.

1. On the Main tab, click **Device Groups** > .

   The Device Groups screen opens.
2. Click the name of the device group.
3. To include the local statistics database in the configuration synchronization, select the **Enabled** check box.

   If you have a remote database configured, you cannot synchronize the database with the peer Enterprise Manager.
4. From the **Scheduled ConfigSync** list, select an option to specify the interval at which you want to synchronize the configuration with the peer Enterprise Manager.

5. For the **Start Time** options, select the time you want the configuration synchronization to occur.
6. Depending on whether you selected an option to synchronize the configurations as weekly or monthly, select an option from the **Day of the Week** or the **Day of the Month** list.
7. Click the **Update** button.

Enterprise Manager will synchronize with the peer in the high availability configuration at the specified interval.

About device discovery and communication

Before you can use Enterprise Manager™ to manage devices in your network, you must add the devices to the device list. For BIG-IP® devices in your network, you can use the discovery process to search specific IP addresses or IP subnets in your network, and add those devices to Enterprise Manager. *Discovery* is the process by which Enterprise Manager successfully logs on to available devices with an administrator user name and password that you supply. If Enterprise Manager succeeds in logging on to devices that it discovers, it adds those devices to the list on the Device List screen.

You can discover devices either by scanning your network for specific IP addresses, or importing a file that contains a list of all of the IP addresses, user names, and passwords for the devices you want to discover.

Important: *To perform discovery, you must have administrator privileges with root access for the Configuration utility. To successfully discover devices and receive the user name and password combination, the device must have an active SSL server listening for traffic on port* `443`.

Discovering devices by scanning your network

After you license and perform initial configuration for the system, you can scan your network to discover F5® devices.

When you discover devices, you establish a secure communication between the system and managed devices by exchanging public keys.

Important: *To have full access to the functionality of the analytics and iControl® proxy features, you must use the device´s self IP address for device discovery.*

1. On the Main tab, click **Enterprise Management** > **Devices** > **Device List**.
2. Click the **Discover** button.
3. For the **Scan Type** setting, select one of the following options:

Option	Description
Address List	Select this option if you know the IP addresses specific of the devices that you want to discover.
Subnet	Select this option if you want to use the IP address and netmask of the subnet to scan your network for devices to discover.

   The screen refreshes to display settings specific to the selected option.
4. If you selected the **Address List** option, perform the following steps:

a) In the **User Name** and **Password** fields, type a user name and password to use to log on to the discovered device.
b) Click **Add**.

5. If you selected the **Subnet**, option perform the following steps:
   a) In the **IP Address** field, type the device IP address.
   b) In the **Network Mask** field, type the netmask that you want to use when searching the network.
      You can search by class B or C network.
   c) In the **User Name** and **Password** fields, type a user name and password to use to log on to each device discovered in the subnet.

6. Click the **Discover** button.
   The Task Properties screen opens and discovered devices appear below the Properties area. The list refreshes until all specified devices are discovered, or until you click **Cancel Pending Items**.

The list of devices should include the BIG-IP system and its internal IP address. This indicates that keys have been exchanged and trust has been established.

Discovering devices through importation

After you license and perform initial configuration for Enterprise Manager™, you can discover F5® devices.

If you have a large number of devices, instead of typing the information required to scan your network, you can import a file in comma-separated values format (CSV) from your local system that contains the IP addresses, user names, and passwords of the devices that you want to discover.

Important: *To have full access to the functionality of the analytics and iControl® proxy features, you must use the device's self IP address for device discovery.*

---

1. Create a CSV file that contains, for each device that you want to discover, the following information:
   `<device IP address>,<username><password>`
   Use one line per device entry.
   For example:

```
10.10.10.1,admin,pass001
10.10.10.2,admin,pass002
10.10.10.3,admin,pass003
10.10.10.4,admin,pass004
10.10.10.5,admin,pass005
```

2. Save the file you created with a `.csv` extension.
3. On the Main tab, click **Enterprise Management** > **Devices** > **Device List**.
   The Device List screen opens.
4. Click the **Discover** button.
5. Click the **Import from File** button.
6. Click the **Browse** button and locate the `.csv` file that you created and saved.
7. Click the **Open** button.
8. Click the **Import** button.
   Enterprise Manager begins importing the specified devices.

The Task Properties screen opens and discovered devices appear below the Properties area. The list refreshes until all specified devices are discovered, or until you click **Cancel Pending Items**.

Troubleshooting communication from Enterprise Manager to a device

If a managed device cannot communicate with Enterprise Manager™, the Device List page displays the message, `Device cannot contact EM`, in the **Details** column next to a device name. If this occurs, you can troubleshoot potential issues from the command line of the managed device.

1. Log on to the managed device command line as the `root` user.
2. Type the following command where *<EM_address>* is the IP address of the Enterprise Manager system: `telnet <EM_address> 443`.

   This command tests the ability of the managed device to communicate with Enterprise Manager on port `443`.

Review the message returned, and take corrective measures to establish communication.

Changing the Enterprise Manager IP address on a device

For proper device management communication, the IP address for the Enterprise Manager™ must be correct on the managed device.

If you have determined that the IP address is not properly configured on a managed device, you can correct it and establish communication.

1. On the Main tab, click **Enterprise Management** > **Devices** > **Device List**.
2. In the Device list, click the device name of the device for which you want to verify communication.
   The Device Properties screen opens.
3. From the **Device Properties** list, select **Advanced**.
   The screen refreshes to display additional device properties.
4. In the **EM Address** field, type the correct IP address of the Enterprise Manager system.
5. Click the **Save Changes** button.

Remotely linking to a managed device's interface

From Enterprise Manager™, you can remotely link directly to a managed device's user interface. This saves you time, because you do not have to physically go to the managed device to change its configuration.

1. On the Main tab, click **Enterprise Management** > **Devices** > **Device List**.
2. Click the name of device that you want to access remotely.
   The device properties screen opens.
3. On the menu bar, click **Launch Pad**.
4. Click the **Launch** link adjacent to the access control type that you want to access.

You now have direct access to the managed device's interface.

Chapter 3

Software Management

Overview: Downloading, importing, and installing software images

Using Enterprise Manager™ to centrally manage your software images saves you time, because you do not have to log in to each individual device to download, install, or roll back to a previous version of a software image.

Files available for download

You can download and store several versions of software images for any number of different devices. The following file image types are hosted on the F5 Networks Download site located at `http://downloads.f5.com`.

File class	Description and purpose	File extension
Software image file	A software image contains all of the packages necessary and is not specific to a local or remote installation. Use a software image to perform a full software upgrade to the most recent version.	.iso
Hotfix image file	Legacy hotfix packages are IM files, which update a portion of the existing software without requiring a full installation. All other hotfix packages are ISO files, which require that you install the base software image with the hotfix. Use hotfix packages to install fixes developed since the last release.	`.im` or `.iso`
BIG-IP® Application Security Manager™ signature file	The attack signature files protects your network against attacks and threats. Download attack signature files to update the files shipped with BIG-IP Application Security Manager to ensure that you are protected against the most recent threats.	`.im`
Checksum file	A checksum file verifies the integrity of a software image that you downloaded. Use the checksum file to confirm that data errors were not introduced when you downloaded an image.	`.md5`
Documentation file	Some software images include a text or readme file. Use this file to supplement the documentation provided with the release.	`.txt` or `.readme`

Downloading software images and files

To access the F5® Downloads site you must have an F5 Networks Technical Support single sign-on account, which you can obtain from `https://downloads.f5.com`.

From the F5 Networks Downloads site, you can acquire the software images and other files you need to assist you in device management.

1. Using a web browser, browse to `https://downloads.f5.com`.
   The single sign-on screen opens.
2. In the **User Email** field, type the email address for your F5 Technical Support account.
3. In the **Password** field, type your password.
4. Click **Login**
   The Downloads Overview screen opens and displays notes about using the F5 Networks Downloads site.

5. Click the **Find a Download** button.
   The Select a Product Line screen opens listing all F5 product families.
6. Click the product version located next to the product family and that you want to download.
   The Product Version and Container screen opens, listing the available software images for the current product version.
7. Click the name of the container that corresponds to the software image that you want to download.
   The Software Terms and Conditions screen opens, displaying the End User License Agreement (EULA) screen.
8. Read the EULA and click the **I Accept** button.
   The Select a Download screen opens.
9. Click the name of the file that you want to download.
   The Select a Download Method screen opens.
10. Click the download icon next to the protocol that you want to use.
    A dialog box opens, prompting you to save the file to your local system.

When the download is complete, the file is available to import.

Importing software images to the software repository

You must download software images and files from the `https://downloads.f5.com` site before you can import them to the Enterprise Manager™ software repository.

Software images imported to the software repository are available for distribution to managed devices.

1. On the Main tab, click **Enterprise Management** > **Repository**.
2. Select the list associated with the software that you downloaded and saved, and that you want to add to the repository. The options include:
   - Hotfix Image List
   - Signature List
   - Software Image List

   The associated image list screen opens.
3. Click the **Import** button located above the image list.
   The Import screen opens.
4. Click the **Choose File** button and browse to the location that you saved the downloaded file.
5. Select the file and click the **Import** button.
   The Repository list screen opens and the image name appears with the status of `Importing`.

When the importation is complete, the software image displays in the associated repository list screen with the status of `Imported`.

About software installation

Starting in BIG-IP® version 10.0 and Enterprise Manager™ version 2.0, devices use the *Logical Volume Management* (LVM) disk-formatting scheme that dynamically adds virtual storage space for software through the use of volumes. A *volume* is a specific section of the hard drive that can hold a complete version of software.

The LVM scheme allows you to install software images in a separate volume of a currently running system, without impacting the system or application traffic to the device. You can also install software to another boot location while continuing to use the active boot location with the current software installation. During a normal maintenance window, you can boot the system to the new boot location, at which time you can

test application traffic and verify that the new image is working as expected. have the option of formatting the device's hard drive, for the purpose of software installation, in volumes.

For software releases after version 10.x or Enterprise Manager version 2.x, you use the Software Image Copy and Installation wizard to guide you through the steps to copy and install downloaded software and hotfix images to a particular volume on the managed devices in your network. If you have legacy devices in your network that are running software version prior to version 10.x or Enterprise Manager version 2.x, you use the Legacy Software Image Installation wizard.

Using the Software Image Copy and Installation wizard

Before you start a software image copy and installation task, you must first download the software image and import it into the software repository.

Important: *You cannot install software to a Compact Flash boot location using the Software Image Copy and Installation wizard.*

You use the Software Image Copy and Installation wizard to copy a software image and install it to one or more specified devices. This task applies only to managed devices running versions later than 10.x or Enterprise Manager version 2.x.

1. On the Main tab, click **Enterprise Management** > **Tasks**.
2. For the **Software Installation** setting, select **Copy and Install Software and Hotfix Images**.
3. Click **Next**.
   The Software Image Copy and Installation screen opens.
4. From the **Software Image** list, select the software image that you want to copy to one or more devices.
   The Compatible Devices list refreshes to display the devices available for this installation.
5. From the **Hotfix Image** select an optional hotfix to apply to the software image.
6. From the **Task Type** list, select **Copy Install Image(s) copies and installs the software image to the selected devices, in one task**.
7. Use the **Device List** and **Device Filter** settings to specify which devices you want displayed.
8. Select the check box next to one or more devices on which you want to install this software image and click the **Next** button.
9. Specify settings for the following options.

Option	Description
Post-Install Run Location	Select the location to which you want the device to reboot after software is installed.
Configuration Archive	Specify whether to include or exclude private keys in the configuration archive.
Device Error Behavior	Select the action that you want the system to take if an error is encountered during the software installation task.

10. Click the **Start Task** button.

The screen refreshes to display the software installation task progress.

Using the Legacy Software Image Installation wizard

Before you start a software image copy and installation task, you must first download the software image and import it into the software repository.

You use the Legacy Software Image Installation wizard to select a software image and install it to one or more specified devices. This task applies only to managed devices running versions prior to 10.x or Enterprise Manager™ version 2.x.

1. On the Main tab, click **Enterprise Management** > **Tasks**.
2. For the **Software Installation Setting**, select **Install Legacy Software Image** and click the **Next** button.
   The Legacy Software Image Installation wizard opens.
3. From the **Software Image** list, select the Legacy Software Image you want to install.
   The Compatible Devices table refreshes to display only devices that are compatible with the software image you selected.
4. From the **Software Image** list, select the software image that you want to copy to one or more devices.
   The Compatible Devices list refreshes to display the devices available for this installation.
5. Select the check box next to one or more devices on which you want to install this software image and click the **Next** button.
6. From the **Hotfix Image** list, select an optional hotfix to include with the software installation and click the **Next** button.
7. Specify settings for the following options.

Option	Description
Install Location	Select the location to install the software image.
Configuration Options	Specify whether to install the full or essential configuration.
Post-Install Run Location	Select the location to which you want the device to reboot after software is installed.
Configuration Archive	Specify whether to include or exclude private keys in the configuration archive.
Device Error Behavior	Select the action that you want the system to take if an error is encountered during the software installation task.

8. Click the **Next** button.
   The Task Review screen opens
9. Review the options and click the **Start Task** button.
   The screen refreshes to display the software installation task progress.

Chapter 4

Managing User Roles and User Accounts

About authentication and permissions for Enterprise Manager user roles

A user role specifies the type of management tasks that an Enterprise Manager™ user can perform on managed devices in your network. Permissions for user roles are classified as either non-restricted or restricted. The user roles are defined as:

Administrator
This (non-restricted) role can perform all management functions available to Enterprise Manager, including managing other user accounts and roles.

Operator and Application Editor
By default, these (restricted) roles perform fewer management tasks than the Administrator. You can customize each role by specifying the tasks that the role is allowed to perform.

Users are authenticated through Enterprise Manager's local database.

User role permissions and management tasks

There are eight different types of permissions that you can specify for each restricted user role. You can specify any of these management task permissions to the Operator and Application Editor user roles.

Permission	Management task
Manage Device Configuration Archives	Create and manage UCS archives for all managed devices
Browse Device Configurations	View configurations from the Enterprise Manager™ configuration browser
Compare Device Configuration Archives	Compare UCS configuration files between two devices
Stage Changesets for Deployment from Published Templates	Create a new staged changeset from a published template
Deploy Staged Changesets	Deploy a staged changeset created by a user
Administer Device Lists	Manage device list members
Synchronize Device Configuration with Peer	Synchronize peer device configurations
Failover Devices	Initiate a failover to a peer managed device

Adding new users to perform management tasks on Enterprise Manager

All users and their privileges are displayed on the User list screen.

Important: *When you add users, you must use the same administrator-level user name that you currently use for managing BIG-IP® devices in your network. This ensures that you can successfully manage devices as soon as Enterprise Manager™ discovers them and adds them to the Device List screen.*

1. In the navigation pane, click **System** > **Users**.
   The Users list screen opens.
2. Click the **Create** button.
   The New User screen opens.

3. In the **User Name** field, type the administrative-level user name that you are currently using to manage the BIG-IP devices in your network.
4. In the **New** and **Confirm** fields, type the password for the user.
5. From the **Role** list, select one of the following roles.

Option	Description
Administrator	Grants user complete access to all objects on the system and permission to perform configuration synchronization for a BIG-IP device service clustering configuration.
Operator	Grants user permission to enable or disable existing nodes and pool members.
Application Editor	Grants user permission to modify existing nodes, pools, pool members, and monitors.

   If you select another user role, managed devices cannot authorize the user to perform management tasks, and the user cannot initiate tasks using the Enterprise Manager system.
6. From the **Partition Access** list, select an option to specify which administrative partitions the new user can access.
7. From the **Terminal Access** list, select **Enabled** to allow the user command-line access to Enterprise Manager.
8. Click the **Repeat** button to add another user, or click the **Finished** button to return to the User list screen.

Changing source for authenticating users

By default, Enterprise Manager™ uses a local database to authenticate users, but you can choose to use a remote LDAP, Active Directory, RADIUS, or TACACS+ authentication source.

1. In the navigation pane, click **System** > **Users**.
   The Users list screen opens.
2. On the menu bar, click **Authentication**.
   The Authentication screen opens.
3. Click the **Change** button.
4. From the **User Directory** list, select an option.
   The screen refreshes to display options specific to the authentication source you selected.
5. Specify the configuration settings for the remote authentication server.
   Refer to the online help for information specific to each authentication setting.
6. Click the **Finished** button to save your changes.

Customizing user role permissions

When you complete the initial setup tasks for Enterprise Manager™, you specify a default administrator-level user account that permits you to configure and start working with the system through the web interface. You can use this procedure to customize permissions for users, defining which user role (Operator or Application Editor) can perform specific device management tasks.

1. On the Main tab, click **Enterprise Management** > **Access Control** > **Role Permissions**.
2. For each restricted user role, select or clear the check box next to the permission you want to modify.

3. Click **Apply** to save your changes.

About user accounts for managed devices

Managed BIG-IP® systems contain accounts that specify the authorization (level of access) for users. When you configure user account information on a BIG-IP system, you set parameters such as user names and passwords, shell access information, web interface and root access privileges, and an authentication source. You can use Enterprise Manager™ to view and copy account parameters from managed devices to other managed devices, as well as to modify passwords.

Viewing user accounts for managed devices

You must first discover a device before Enterprise Manager™ displays its user account information.

Using Enterprise Manager, you can view all managed device users and their access privileges from one central location. This eliminates the need to log on to each individual managed device for user account information.

1. On the Main tab, click **Enterprise Management** > **Access Control** > **User List**.
2. To search for a specific user, in the **Search** field, type all or part of the name and click **Search**.
3. Click the name of a user to view the devices to which this user has access privileges.

   The screen displays the devices associated with the selected user.

Replicating user account information for managed devices

Once you configure a user account on a BIG-IP® system, and Enterprise Manager™ has discovered that device, you can copy that configuration to other managed devices.

With the Copy User Access Configuration wizard, you can distribute a common user account configuration, or specific elements of configuration data, simultaneously to multiple devices.

1. On the Main tab, click **Enterprise Management** > **Tasks**.
2. Click the **New Task** button.
3. For the **User Access** setting, select **Copy User Access Configuration**.
4. Click **Next**.
5. From the **Source Device** list, select the device from which you want to replicate user account information.
6. For the **Configuration Data** setting, select the type of configuration data you want to replicate from the source device.
   - **Users**
   - **Shell Access**
   - **Authentication**
7. From the **Device List**, you can select a group of devices to narrow the number of devices displayed.
8. Select the check box next to each compatible device to which you want to copy the source device's configuration.
9. Click the **Next** button.

10. From the **Device Users** list, select an option.

Option	Description
Add users not already present on device	Adds user accounts to the destination device instead of replacing the users with those on the source device.
Replace users on device	Deletes all user accounts on the destination device and replaces them with the user accounts from the source device.

11. From the **Device Error Behavior** list, select the action you want Enterprise Manager to take in the event that the task fails on one of the devices.
    - **Continue task on remaining devices**
    - **Cancel task on remaining devices**
12. Click **Next**.
    The Task Review screen opens, and you can confirm the task details.
13. Click the **Start Task** button.
    The Task Properties page displays the progress for the task.

Enterprise Manager copies the configuration from the source device to the selected target devices.

Changing user passwords for managed devices

Enterprise Manager™ increases the efficiency of managing user passwords by centralizing the password change process for your devices. This saves you time, while ensuring that when you change a password, the new password is the same for each selected device.

1. On the Main tab, click **Enterprise Management** > **Tasks**.
2. Click the **New Task** button.
3. For the **User Access** setting, select **Change User Password**.
4. Click **Next**.
5. From the **User Name** list, select the user for which you want to change the password.
6. From the **Device List**, you can select a group of devices to narrow the number of devices displayed.
7. Select the check box next to each device for which you want to change the password.
8. In the **Password** field, type a new password.
9. In the **Confirm** field, re-type the password.
10. Click **Next**.
11. From the **Device Error Behavior** list, select the action you want Enterprise Manager to take in the event that the task fails on one of the devices.
    - **Continue task on remaining devices**
    - **Cancel task on remaining devices**
12. Click **Next**.
13. Click the **Start Task** button.
    The Task Properties page displays the progress for the task.

The new password you specified is now associated with the selected user.

Chapter 5

Health and Performance Monitoring Statistics Overview

Overview: Health and performance monitoring statistics

When statistics data collection is enabled, Enterprise Manager™ stores the following information in its statistics database for each managed device on which the Data Collection Agent is installed:

- Specifics about the managed devices, such as host name, IP address, and software version
- Details, such as object type and name, about any enabled network objects associated with a managed device
- Performance and health data for managed devices and associated network objects

You can use collected statistics to display standardized reports about the health and performance of managed devices in your network. This helps you identify any systems that are not performing at full capacity and assists you in determining when you should add new devices.

Important: *Enterprise Manager collects statistics only from devices that have BIG-IP® Local Traffic Manager™ licensed and provisioned. Starting with Enterprise Manager version 2.3, Enterprise Manager can also collect statistics from devices licensed and provisioned for BIG-IP Global Traffic Manager™.*

To start collecting statistics, you must enable the collect statistics data feature and install the Data Collection Agent.

Enabling statistics data collection

To collect statistics you must enable data collection, which is disabled by default.

Important: *Due to the processing power required to collect and store statistics data, only Enterprise Manager™ 4000 platform and Enterprise Manager Virtual Edition (VE) support statistics data collection. If you are upgrading from a version of Enterprise Manager that is earlier than 1.7, you must re-license the system before enabling data collection.*

Tip: *If Enterprise Manager is managing devices that are part of a BIG-IP® Global Traffic Manager™ (GTM™) synchronization group, Enterprise Manager temporarily disrupts communication between GTM and remote BIG-IP objects while it verifies the version of the* `big3d` *agent on GTM. To reduce the impact to production traffic relying on the BIG-IP GTM infrastructure, we recommend that you enable statistics data collection during a maintenance window. Alternatively, you can configure the BIG-IP GTM system to maintain an available status for the virtual servers on each managed device while communication is briefly disrupted.*

---

1. On the Main tab, click **Statistics** > **Options** > **Data Collection**.
2. For the **Collect Statistics Data** setting, select **Enabled**.
3. Click the **Save Changes** button.

When you enable statistics collection, Enterprise Manager verifies that each managed device has a compatible version of the Data Collection Agent installed.

Installing the Data Collection Agent

When data collection is enabled, Enterprise Manager™ collects health and performance monitoring statistics data for each managed device in your network on which the most current version of the Data Collection

Agent is installed. If a device on which statistics is enabled requires a more recent version of the Data Collection Agent, Enterprise Manager displays that device as `Impaired` in the device list, and indicates that an upgrade is required.

You can use the Data Collection Agent Installation wizard to update and install the Data Collection Agent.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Task List**.
2. Click the **New Task** button.
3. For the **Software Installation** setting, click **Install Data Collection Agent**, and then click **Next**.
   The Data Collection Agent Installation screen opens.
4. For the **Device Filter** setting, click the **Devices with data collection enabled requiring update** option.
   The screen refreshes to display the devices that require an update.
5. Select the check box next to each device on which you want to install the most recent version of the Data Collection Agent, and click **Next**.
   The Task Options screen opens.
6. From the **Configuration Archive** list, select an option to include or exclude private SSL keys in the configuration archive.
7. From the **Device Error Behavior** list, select an option to specify how you want the system to proceed if an error occurs during the Data Collection Agent installation task.
8. Click **Next**.
   The Task Review screen opens.
9. In the **Task Name** field, you can type a new name to customize the name that displays in the task list.
10. Click the **Start Task** button.
    The Task Properties screen opens, displaying the progress of the task. The task progress displays as Finished when the Data Collection Agent is installed.

Enterprise Manager starts collecting and storing health and performance monitoring statistics for the devices on which data collection is enabled and the Data Collection Agent is installed.

Specifying defaults for alert options

Setting the default behavior for alerts ensures consistent alert actions and the ability to quickly add new alerts based on these standardized options. It is important to specify default behavior for alerts before you enable the alert options.

1. On the Main tab, click **Enterprise Management** > **Options** > **Alerts**.
2. If you want Enterprise Manager to send emails when an alert is triggered, in the **Email Recipient** field, type the email address of the user, or the alias, that you want as the default receiver for alerts.
3. If you want to log alert events to a `syslog` file:
   a) In the **Remote Syslog Server Address** field, type the IP address of the remote syslog server where you want to store alert event logs by default.
   b) In the **Maximum History Entries** field, type the maximum number of alerts that you want stored in the `syslog` file.

      If the alert history reaches the limit you set, Enterprise Manager deletes the oldest entries to create room for newer entries.

4. Click **Save Changes**.

Chapter 6

Network Object Lists

Overview: Custom lists for network objects

A *custom list* is a collection of selected network objects that can span multiple devices in your network. Creating custom lists allows you to monitor a group of objects from one screen, without restricting the view to an associated device.

There are two types of custom network object lists that you can create: static lists and dynamic lists. A *static list* is a fixed selection of network objects. A *dynamic list* is a selection of network objects, which match characteristics that you define in the list's rules.

Note: *Custom lists are available only for Enterprise Manager™ version 2.1 and later. Data collection must be enabled to use this feature. You have the opportunity to enable data collection as part of the process of creating a list. However, if you upgraded to the current version of Enterprise Manager from a version prior to 1.7, you must re-license the system before you can enable data collection. Due to the processing power required to collect and store statistical information, data collection is available only for the Enterprise Manager 4000 platform.*

About custom static lists

Custom static lists that you create retain the network objects that you selected until you remove the objects from the list, or you delete the list.

Creating a static list

If you want to simultaneously view a collection of network objects, or change the status of certain nodes and pool members from one screen, you can create a custom static list that contains those objects. For example, you could create a custom static list of devices managed by a particular department, or containing all of the network objects specific to a certain office location.

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. Click the **Create List** button.
   The Create a Custom List pop-up opens.
3. In the **List Name** field, type a name for the custom list.
4. From the **List Type** list, select **Static List** and click **OK**.
   The screen refreshes to displays the custom static list that you created (as part of the **Custom Lists**) on the left of the screen.
5. At left of the screen, below **Custom Lists**, click the name of the object type (devices, nodes, pool members, pools, or virtual servers) that you want to add to the list.
   The screen refreshes to display (in the center of the screen) a summary list of all the objects in your network for that object type.
6. Select the check box next to each object that you want to add to the list.
7. Place your cursor over one of the items you selected, click the left-mouse button, and drag the selected items onto the name of the list that you created.
   The screen refreshes, displaying the details of the list with all of the selected objects.
8. Repeat steps 5-7 for each object type that you want to add to the list.

Removing network objects from a custom static list

Custom static lists retain the same selected network objects until you remove the objects from the list.

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. At left of the screen, below **Custom Lists**, click the name of the custom static list that you want to modify.
   The screen refreshes to display (in the center of the screen) a summary list of all the objects in the custom list.
3. Select the check box next to the network object that you want to remove from the custom static list, and click the **Remove From List** button.
   The screen refreshes to display the custom static list without the objects you removed.

Deleting a custom static list

Custom static lists remain active until you delete them.

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. Click the name of the custom static list that you want to delete.
3. Select the check box next to the custom static list that you want to delete and click **Confirm**.
   The screen refreshes and the list displays without the custom network object list that you deleted.

About custom dynamic network object lists

You can create a custom dynamic list to contain network objects that have specific characteristics. After you create this list, you can use it to view (from one page) all of the network objects that match the rules you specify, and to change the status of nodes and pool members. Enterprise Manager™ removes an object from a custom dynamic list when the object's characteristics have changed, and adds an object to the list when it detects that the object matches the defined rules.

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. Click the **Create List** button.
   The Create a Custom List pop-up opens.
3. In the **List Name** field, type a name for the custom list.
4. From the **List Type** list, select **Dynamic List** and click **OK**.
   The Specify a rule for your dynamic list popup screen opens.
5. In the **Name or address should contain** field, type all or part of an object's name or IP address.
6. Specify one or more of the following elements to prompt Enterprise Manager to add a matching network object to this custom dynamic list.

Perform this action:	To:
Select a network object type from the Object Type list	Limit the list to a specific of network object type
Select a status from Object Status list	Limit the list to network objects with a particular status

Perform this action:	To:
Select the Objects that have reached one or more thresholds check box	Limit the list to network objects that have reached a defined threshold
Select the Objects that currently have no connections check box	Limit the list to network objects with no current connections

7. Click the **Add Another** button to specify additional rules, or click the **Done** button to save your changes. The list you created displays at left of the screen, under **Custom Lists** and below the **Advanced Search** field, as well as in the custom lists summary section in the center of the screen.

About managing network objects using custom lists

With Enterprise Manager™, you can view the following details for devices, nodes, pools, pool members, and virtual servers (collectively called *network objects*) for every managed device in your network.

- Current connections
- Object name or IP address
- Object state (for nodes and pool members only)
- Object status

Using custom lists, you can narrow the type of object displayed, then select specific objects and change the status for those objects without having to log in to each device individually.

Viewing network object details

When you have data collection enabled, you can view information about objects associated with managed devices in your network from the Custom Lists screen.

Note: *You can view only the objects for which you have administrative partition rights. For information about administrative partitions, see the TMOS® Management Guide for BIG-IP® Systems.*

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. Left of the screen, below the **Advanced Search** field and under **Custom Lists**, click the name of the network object type (nodes, pool members, pools, or virtual servers) that you want to view.
   The screen refreshes to display the associated details for every object of the selected type.

Modifying the status of a network object

When you have statistics enabled, you can enable, disable, or force offline, any network object without having to log in to each associated device.

Note: *You can modify the status of network objects only if you have administrative partition rights to that object. For information about administrative partitions, see the TMOS® Management Guide for BIG-IP® Systems.*

1. On the Main tab, click **Enterprise Management** > **Custom Lists**.
   The Custom Lists screen opens.
2. Below the Advanced Search field, click the object type that you want to change.

The screen displays a list and associated details for every object of the selected type.

3. Select the check box next to the object for which you want to change the status.
4. Below the list, select an option.

Select this option:	To:
Enable	Allow traffic to the selected objects.
Disable	Allow only persistent or active connections to the selected objects.
Force Offline	Allow only active connections to the selected objects.

The Task List Properties screen opens, displaying the status of the task.

Chapter 7

Customizing Settings

Overview: Customizing settings

After you activate the license, complete the initial setup, and specify your network configuration options, you can customize settings for other Enterprise Manager™ features.

About storing configuration data

The configuration details of managed devices (including Enterprise Manager™ itself) are contained in a compressed *user configuration set* (*UCS*) file with the extension of `.ucs`. This file contains all of the information required to restore a device's configuration, and consists of these elements:

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

Enterprise Manager saves UCS files to a *UCS archive*. You can create a task to save UCS archives for devices at regularly scheduled intervals. Archives that are created and saved on a schedule are called, *rotating archives*. When the system creates rotating archives, it compares the most recently stored UCS archive file to the current configuration on the device at the specified interval. If there are any differences, Enterprise Manager stores a copy of the current configuration in a UCS archive. If there are no differences, Enterprise Manager does not store an additional copy of the current configuration, which leaves you room to store a higher number of unique historical UCS archives. When Enterprise Manager reaches the maximum number of archives specified to store, it deletes the oldest archive in the rotating archive list. By default, Enterprise Manager stores up to 10 rotating archives each, for itself and every managed device.

Another option for archive storage is to create an archive of a specific UCS for a device, referred to as a *pinning* an archive. Enterprise Manager also creates a pinned archive of a device's current configuration before it installs new software. Pinned archives are stored until you delete them.

Creating a rotating UCS archive schedule

A device must be listed on the Device List screen before you can create a rotating archive schedule for it.

It is best practice to create a rotating archive schedule for each device in your network so that you always have a copy of a recent configuration. The UCS archive provides your network with added stability in the event that a configuration change results in a need for a system restore. You can create a customized schedule for a specific device, or create several schedules and assign any number of devices to each schedule.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Schedules** > **Archive Collection**.
   The Archive Collection screen opens.
2. Click the **Create** button.
   The New Scheduled Task screen opens.
3. In the **Archive File Name** field, type a name for the rotating archive schedule.
4. From the **Check for Changes** list, select the frequency that you want Enterprise Manager to check for configuration changes.
   Depending on your selection, the screen refreshes to display associated options.
5. Click **Finished** to save the settings.

The Archive Collection list screen opens and the new rotating archive schedule appears in the list. If a device in the **Assigned** list changes its configuration during the interval you specified, Enterprise Manager creates an archive of the device's configuration and adds it to the rotating archives on the Archives Collection screen.

Changing private key archive settings

When Enterprise Manager™ creates a UCS archive, it stores the private keys in the archive by default. If you would prefer not to have the system store the private keys in the UCS archive, you can change this default behavior.

Important: *If you choose not to have Enterprise Manager™ store the private keys in the UCS archive, you must manually restore the keys if you restore the archive.*

---

1. On the Main tab, click **Enterprise Management** > **Options** > **Certificates** > **SSL Private Keys**.
2. From the **Private Keys in Archives** list, select an option:

Option	Description
Include	Select this option if you want the system to store private key data when it creates a configuration archive. This is the default setting.
Exclude	Select this option if you do not want the system to store private key data when it creates a configuration archive. Note that if you select this option, you must manually restore the keys if you restore the archive.

3. Click **Save Changes**.

About refreshing device configurations

To ensure that the stored configuration for each managed device is up-to-date, Enterprise Manager™ compares it with the device's current configuration at regular intervals. If a configuration change has occurred, Enterprise Manager updates the stored configuration with those changes.

Changing the device refresh interval

By default, Enterprise Manager™ contacts its managed devices to check for configuration changes once every 60 minutes. You can reduce the amount of management traffic by increasing this interval or you can more closely monitor the state of devices by decreasing the interval.

Tip: *You can refresh device information immediately at any time, by selecting devices and clicking the* ***Update Status*** *button on the Device list screen or on the General Properties screen of a specific device.*

---

1. On the Main tab, click **Enterprise Management** > **Options** > **Devices** > **Communications**.
2. In the **Refresh Interval** field, type an interval value to specify the number of minutes that Enterprise Manager waits before requesting new information from each managed devices.

   This interval is superseded if a configuration change prompts an automatic refresh before the interval is reached, unless the **Send Event Notifications to EM** setting is disabled.
3. Select **Disable** for the setting in these circumstances:

Setting	Disable this option if:
Contact F5 During Refresh	Enterprise Manager is behind a firewall and cannot contact F5 licensing servers for updated license information
Send Event Notifications to EM	You want to reduce management traffic and refresh only at the interval defined in the **Refresh Interval** field
Check Connectivity From Device to EM	There is a firewall between Enterprise Manager and the managed device, and communication is only allowed unilaterally from Enterprise Manager to the device

4. Click **Save Changes**.

About proxy servers for Enterprise Manager

If you do not want to expose the IP address of the Enterprise Manager™ system or devices, you can use a proxy server specific to the type of communication.

Proxy server	Description
Internet proxy server	For outbound communication from the Enterprise Manager to F5 Networks® for download licensing information, support information, and Application Security Manager™ attack signature files
Device proxy server	For communication between Enterprise Manager and managed devices in your network
iControl® proxy server	For inbound communication to managed devices, required for authentication, pass-through, and device inventory
SMTP proxy server	For alert email notification

You can configure Enterprise Manager to use a single proxy for SSL and FTP connections, or to use a unique proxy for each protocol.

Specifying a device proxy server for communication between Enterprise Manager and devices

By default, Enterprise Manager™ communicates with devices through HTTPS. You have the option to specify a proxy server for communication between Enterprise Manager and your network devices.

1. On the Main tab, click **Enterprise Management** > **Options** > **Servers**.
2. In the Device Proxy Server area, select the **Use Proxy** check box.
   The screen refreshes, displaying additional options.
3. In the **EM-side SSL Proxy Address** field, type the SSL proxy server address that you want to use for Enterprise Manager.
4. If you want to use the same SSL proxy address for the device side, select the **Also use this proxy address for the device-side connections** check box.
5. To specify a separate device-side SSL proxy address, clear the **Also use this proxy address for the device-side connections** check box and type an IP address in the **Device-side SSL Proxy Address** field.
6. Click **Save Changes**.

Specifying a proxy for iControl communication

When you specify an iControl® proxy, Enterprise Manager™ acts as a proxy to support authentication, pass-through, and device inventory using iControl

1. On the Main tab, click **Enterprise Management** > **Options** > **Servers**.
2. In the iControl Proxy area, select the **Use Proxy** check box.
3. Click the **Save Changes** button.

Specifying a proxy server for downloading files and information

When you specify an Internet proxy, Enterprise Manager™ uses that proxy for tasks configured through its task wizards, such as the Licensing wizard.

For example, if you create a task to update the licensing information for a device, Enterprise Manager sends the licensing information through the specified proxy. Conversely, if instead of using the Licensing wizard, you select **License** option from the **System** menu on the Main tab to update the licensing information for a device, Enterprise Manager does not send the licensing information through the configured proxy.

1. On the Main tab, click **Enterprise Management** > **Options** > **Servers**.
2. On the menu bar, click **Options**.
3. In the Internet Proxy Server area, select the **Use Proxy** check box.
   The screen refreshes, displaying additional options.
4. In the **SSL Proxy Address** field, type the address of the SSL proxy server.
5. If you want to use the same SSL proxy address for FTP connections, select the **Always use this proxy address for the FTP protocol** check box.
6. To specify a separate SSL proxy for FTP connections, clear the **Always use this proxy address for the FTP protocol** check box and type an IP address in the **FTP Proxy Address field**.
7. Click **Save Changes**.

About using a web proxy for ASM IP Address Intelligence Service database updates

You can use Enterprise Manager™ to obtain updates to the IP Address Intelligence Service database for managed BIG-IP® Application Security Manager™ (ASM) devices, without requiring that those devices connect directly to the public internet.

To do this, you configure Enterprise Manager to communicate with a web proxy connected to the internet. The ASM™ devices request and receive IP Address Intelligence Service updates transparently, through the Enterprise Manager system.

Configuring Enterprise Manager to forward connections from ASM devices to a web proxy

Before you perform this configuration, you must first:

- Get the IP address, proxy port, and any required credentials for the web proxy.
- Configure BIG-IP® Application Security Manager™ devices to use either no authentication, or HTTP basic authentication.
- Verify that the Enterprise Manager™ system allows communication through port 3128.

Once all of the prerequisites are met, you can configure Enterprise Manager to act as an additional proxy between the internet and the managed Application Security Manager devices.

1. Log into the Enterprise Manager system's command line and edit the `/config/em/emforwardd.conf` file as follows:
   ```
   EMFORWARD_PROXY_IP=<web proxy IPv4 address>
   EMFORWARD_PROXY_PORT =<web proxy port>
   ```
2. Type the following command to restart the daemon.
   ```
   tmsh start sys service emforwardd
   ```
3. Log into the command line of each Application Security Manager device for which you want to provide this proxy service, and type the following commands:
   ```
   tmsh modify sys db proxy.username { value <web proxy-username> }
   tmsh modify sys db proxy.password { value <web proxy-password> }
   tmsh modify sys db proxy.host { <self-IP address that can reach Enterprise
   Manager> }
   tmsh modify sys db proxy.port { value 3128 }
   ```

The managed Application Security Manager devices now send requests for IP Address Intelligence Service database updates through Enterprise Manager.

Index

V

W