



vGW Series

Event and Alert Messages Reference Guide

Release

5.0 r2



Published: 2012-01-25

Revision 1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

vGW Series Series Event and Alert Messages Reference Guide

Revision History
January 2012—R1

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

	About This Guide	xiii
Part 1	vGW Series Event and Alert Reference Messages	
Chapter 1	vGW Series Event and Alert Messages Overview	3
Chapter 2	vGW Series Management Messages	5
Chapter 3	vGW Series Multi-Center Messages	9
Chapter 4	vGW Series Firewall Messages	15
Chapter 5	vGW Series Firewall Logs Messages	21
Chapter 6	vGW Series Settings Messages	23
Chapter 7	vGW Series SRX Messages	29
Chapter 8	vGW Series Database Messages	31
Chapter 9	vGW Series IDS Messages	33
Chapter 10	vGW Series Licenses Messages	35
Chapter 11	vGW Series Compliance Messages	37
Chapter 12	vGW Series Introspection Messages	39
Chapter 13	vGW Series High Availability Messages	41
Chapter 14	vGW Series AntiVirus Messages	45
Chapter 15	vGW Series ESP and VMware vCenter Messages	47
Chapter 16	vGW Series Reports Messages	49
Chapter 17	vGW Series Inventory Messages	51
Chapter 18	vGW Series System Backup Messages	55
Part 2	Index	
	Index	59

Table of Contents

	About This Guide	xiii
	Objectives	xiii
	Audience	xiii
	Documentation Conventions	xiv
	Obtaining Documentation	xiv
	Documentation Feedback	xiv
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xv
Part 1	vGW Series Event and Alert Reference Messages	
Chapter 1	vGW Series Event and Alert Messages Overview	3
Chapter 2	vGW Series Management Messages	5
Chapter 3	vGW Series Multi-Center Messages	9
Chapter 4	vGW Series Firewall Messages	15
Chapter 5	vGW Series Firewall Logs Messages	21
Chapter 6	vGW Series Settings Messages	23
Chapter 7	vGW Series SRX Messages	29
Chapter 8	vGW Series Database Messages	31
Chapter 9	vGW Series IDS Messages	33
Chapter 10	vGW Series Licenses Messages	35
Chapter 11	vGW Series Compliance Messages	37
Chapter 12	vGW Series Introspection Messages	39
Chapter 13	vGW Series High Availability Messages	41
Chapter 14	vGW Series AntiVirus Messages	45
Chapter 15	vGW Series ESP and VMware vCenter Messages	47
Chapter 16	vGW Series Reports Messages	49
Chapter 17	vGW Series Inventory Messages	51
Chapter 18	vGW Series System Backup Messages	55
Part 2	Index	
	Index	59

List of Tables

Part 1	vGW Series Event and Alert Reference Messages	
Chapter 2	vGW Series Management Messages	5
	Table 1: Management Event and Alert Messages	5
Chapter 3	vGW Series Multi-Center Messages	9
	Table 2: Multi-Center Event and Alert Messages	9
Chapter 4	vGW Series Firewall Messages	15
	Table 3: Firewall Event and Alert Messages	15
Chapter 5	vGW Series Firewall Logs Messages	21
	Table 4: Firewall Logs Event and Alert Messages	21
Chapter 6	vGW Series Settings Messages	23
	Table 5: Settings Event and Alert Messages	23
Chapter 7	vGW Series SRX Messages	29
	Table 6: SRX Event and Alert Messages	29
Chapter 8	vGW Series Database Messages	31
	Table 7: Database Event and Alert Messages	31
Chapter 9	vGW Series IDS Messages	33
	Table 8: IDS Event and Alert Error Messages	33
Chapter 10	vGW Series Licenses Messages	35
	Table 9: License Event and Alert Messages	35
Chapter 11	vGW Series Compliance Messages	37
	Table 10: Compliance Event and Alert Messages	37
Chapter 12	vGW Series Introspection Messages	39
	Table 11: Introspection Event and Alert Messages	39
Chapter 13	vGW Series High Availability Messages	41
	Table 12: High Availability Event and Alert Messages	41
Chapter 14	vGW Series AntiVirus Messages	45
	Table 13: AntiVirus Event and Alert Messages	45
Chapter 15	vGW Series ESP and VMware vCenter Messages	47
	Table 14: ESP and VMware vCenter Event and Alert Messages	47
Chapter 16	vGW Series Reports Messages	49
	Table 15: Reports Event and Alert Messages	49

Chapter 17	vGW Series Inventory Messages	51
	Table 16: Inventory Event and Alert Messages	51
Chapter 18	vGW Series System Backup Messages	55
	Table 17: System Backup Event and Alert Messages	55

About This Guide

- [Objectives on page xiii](#)
- [Audience on page xiii](#)
- [Documentation Conventions on page xiv](#)
- [Obtaining Documentation on page xiv](#)
- [Documentation Feedback on page xiv](#)
- [Requesting Technical Support on page xiv](#)

Objectives

The Juniper Networks vGW Series for virtualized environments runs as integrated software on VMware ESXi hosts. This guide covers the messages that the vGW Series issues to inform you that certain events have occurred and to alert you to conditions that warrant your attention.

Audience

This guide is intended for the following audiences:

- Virtual infrastructure administrators

This group includes cloud service providers who offer virtual machines and other virtualized resources to enterprises and other business organizations.

These administrators manage virtualized servers, hypervisors, virtual machines, and other virtualized infrastructure. In the cloud deployment, the administrator also manages the physical resources on which virtualized servers and virtual machines run.

- Enterprise network and security administrators

This group includes enterprise personnel who are responsible for network and security infrastructure.

These administrators might manage a virtualized data center presently, or they might be consolidating and rearchitecting their data center for virtualization. They might deploy virtualized services and products within their data center using a private cloud or a hybrid cloud.

Documentation Conventions

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks web site at <http://www.juniper.net/techpubs>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

PART 1

vGW Series Event and Alert Reference Messages

- [vGW Series Event and Alert Messages Overview on page 3](#)
- [vGW Series Management Messages on page 5](#)
- [vGW Series Multi-Center Messages on page 9](#)
- [vGW Series Firewall Messages on page 15](#)
- [vGW Series Firewall Logs Messages on page 21](#)
- [vGW Series Settings Messages on page 23](#)
- [vGW Series SRX Messages on page 29](#)
- [vGW Series Database Messages on page 31](#)
- [vGW Series IDS Messages on page 33](#)
- [vGW Series Licenses Messages on page 35](#)
- [vGW Series Compliance Messages on page 37](#)
- [vGW Series Introspection Messages on page 39](#)
- [vGW Series High Availability Messages on page 41](#)
- [vGW Series AntiVirus Messages on page 45](#)
- [vGW Series ESP and VMware vCenter Messages on page 47](#)
- [vGW Series Reports Messages on page 49](#)
- [vGW Series Inventory Messages on page 51](#)
- [vGW Series System Backup Messages on page 55](#)

CHAPTER 1

vGW Series Event and Alert Messages Overview

The vGW Series Event and Alert Messages book is comprised of chapters each of which is dedicated to a category of event and alert conditions. Each chapter contains a table that provides the following information.

Message—The message text that is presented informing you of an event or alerting you to a condition. When a message is issued, any variables it might contain, as shown in the text, are substituted with literal values identifying entities that the message pertains to.

Meaning—A brief explanation or elaboration of the message.

Action—A recommended approach that you can take to resolve the problem or discover more information about the event.

Internal ID—The ID number assigned to the message internally.

User-Associated—Whether this event or condition is caused by the action of an administrator.

Issuing Module—The name of the vGW Series module that issued the message in response to the occurrence or condition.

Submodule—If it issued the message, the name of the vGW Series submodule within the main module identified as the issuing module.

Priority—For messages that have categorization, Priority is high, medium, or low.

CHAPTER 2

vGW Series Management Messages

Table 1 on page 5 identifies the messages that pertain to system management, including user administration and management and vGW Series management of the system. For example, user administration and configuration might include login and logout events and addition, modification, and deletion of an administrator configuration. vGW Series management might include reports on whether the vGW Security Design VM is having DNS problems, whether an update for the vGW Security Design VM is available, and whether the vGW Security Design VM is restored after problems have occurred.

Table 1: Management Event and Alert Messages

Message	Meaning	Action	User Associated	Event ID	Issuing Module	Submodule	Priority
Successful login	An administrator logged into Security Design vGW.	None	true	1	VGW_MANAGEMENT		None
Failed login attempt by user "%s"	An administrator attempt to log into the Security Design vGW failed.	Verify that a malicious attempt to break into the system did not occur.	true	2	VGW_MANAGEMENT		None
Restarted Security Design vGW application	Security Design vGW was restarted.	None	false	3	VGW_MANAGEMENT		None
User requested restart of Security Design vGW application	Security Design vGW was restarted by a user.	None	true	4	VGW_MANAGEMENT		None
Standby-related restart of Security Design vGW application: %s	Security Design vGW was restarted by for standby-related reasons.	None	false	5	VGW_MANAGEMENT		None
Added Admin %s	An administrator configuration was added.	None	true	6	VGW_MANAGEMENT		None

Table 1: Management Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Event ID	Issuing Module	Submodule	Priority
Deleted Admin %s	An administrator configuration was deleted.	None	true	7	VGW_MANAGEMENT		None
Modified Admin %s. %s	An administrator configuration was modified.	None	true	8	VGW_MANAGEMENT		None
Initiated %sSecurity Design vGW software %s	Initiated software update to Standby or Primary Security Design vGW management server VM. The alert message specifies the original version and the updated version.	None	true	9	VGW_MANAGEMENT		None
Finished %sSecurity Design vGW software %s	Software update to Standby or Primary Security Design vGW management server is completed. The alert message specifies the original version and the updated version.	None	true	10	VGW_MANAGEMENT		none
Log Collection on Security Design vGW was started	Log Collection on Security Design vGW was started	None	true	11	VGW_MANAGEMENT		None
Enabled "Automatically check for updates" for Security Design vGW	"Automatically check for updates" for Security Design vGW was enabled.	None	true	12	VGW_MANAGEMENT		None
Disabled "Automatically check for updates" for Security Design vGW	Disabled "Automatically check for updates" for Security Design vGW	None	true	13	VGW_MANAGEMENT		None
Modified debug flags	Debug flags were modified.	None	true	14	VGW_MANAGEMENT		None
Enabled all debug flags	All debug flags were enabled.	None	true	15	VGW_MANAGEMENT		None

Table 1: Management Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Event ID	Issuing Module	Submodule	Priority
Disabled all debug flags	All debug flags were disabled.	None	true	16	VGW_MANAGEMENT		None
User logout	A user logged out.	None	true	17	VGW_MANAGEMENT		None
%s network connection logs were dropped since %s	A number of network connection logs have been dropped.	Refer to product documentation.	false	18	VGW_MANAGEMENT		HIGH
An update for Security Design vGW management server is available %s	An update for Security Design vGW management server is available.	Verify that the server is in suitable state for update.	false	19	VGW_MANAGEMENT		HIGH
Security Design vGW seems to be having DNS problem.	Security Design vGW seems to be having DNS problem.	Verify DNS functionality.	false	20	VGW_MANAGEMENT		HIGH
Security Design vGW DNS server seem to be working.	Security Design vGW DNS server appears to be working.	None	false	21	VGW_MANAGEMENT		HIGH
Unsuccessful XML-RPC authentication by '%s' for method %s	XML-RPC authentication attempt was unsuccessful.	Assess server security.	false	22	VGW_MANAGEMENT		None
Unauthorized attempt to call %s	An unauthorized attempt to call a method was made.	Assess server security.	true	23	VGW_MANAGEMENT		None
Security Design vGW was restored successfully	Update VMs were called via XML-RPC.	None	false	24	VGW_MANAGEMENT		None
Update VMs called via XML-RPC	Update VMs were called via XML-RPC.	None	true	25	VGW_MANAGEMENT		None
IDS signature setting modified by XML-RPC	IDS signature setting was modified by XML-RPC.	None	true	26	VGW_MANAGEMENT		None

Table 1: Management Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Event ID	Issuing Module	Submodule	Priority
Changed key %s to value %s via XML_RPC	A key value was changed via XML_RPC.	None	true	27	VGW_MANAGEMENT		None
Failed to update %s	Software update of an appliance failed.	Check logs. Verify that there is connectivity to the update server and that there is a valid license.	false	28	VGW_MANAGEMENT		HIGH
Check logs. Verify that there is connectivity to the update server, and that there is a valid license	This high priority alert is from an outside source that was received using an API that enables adding alerts to the Security Design vGW.	Unknown	false	29	VGW_MANAGEMENT		HIGH
%s	This medium priority alert is from an outside source that was received using an API that enables adding alerts to the Security Design vGW.	Unknown	false	30	VGW_MANAGEMENT		MEDIUM
%s	This is a low priority alert from an outside source that was received using an API that enables adding alerts to the Security Design vGW.	Unknown	false	31	VGW_MANAGEMENT		LOW
%s	This event from an outside source was received using an API that enables adding alerts to the Security Design vGW.	Unknown	false	32	VGW_MANAGEMENT		None

CHAPTER 3

vGW Series Multi-Center Messages

Table 2 on page 9 identifies the messages that pertain to the vGW Series Multi-Center feature that allows you to synchronize policy across multiple vGW Series management centers to enable large scale virtualization. They might report on normal events such as when the vGW Security Design VM master center renames a local object at a delegate center because it has the same name as the object being synchronized to the master center. They might inform you of problems that have occurred such as whether a delegate center is unable to synchronize with the master center.

Table 2: Multi-Center Event and Alert Messages

Message	Meaning	Action	User Alert	Internal ID	Issuing Module	Submodule	Priority
There are problems with Multi-Center synchronization, please check Status screen.	One or more delegated centers have synchronization problems.	Check the status screen for Multi-Center synchronization problems.	false	201	MULTI_CENTER		HIGH
Policy "%s" is no longer mirrored from Master Center	The policy is no longer mirrored from the Master Center.	None	false	202	MULTI_CENTER		None
Added "%s" certificate to the Security Design vGW keystore	The certificate of the specified Security Design vGW was added to the keystore to enable secure communication.	None	false	203	MULTI_CENTER	HTTPS	None
Protocol "%s" was renamed to prevent name collision with global object	A protocol was renamed to prevent name collision with global object.	None	false	204	MULTI_CENTER		None
Protocol "%s" is no longer mirrored from Master Center	A protocol is no longer mirrored from the Master Center.	None	false	205	MULTI_CENTER		None

Table 2: Multi-Center Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Added "%s" to Multi-Center configuration	A host was added to the Multi-Center configuration.	None	true	206	MULTI_CENTER		None
Deleted Delegated center "%s"	A delegated center was deleted.	None	true	207	MULTI_CENTER		None
Compliance rule "%s" is no longer mirrored from Master Center	A compliance rule is no longer mirrored from Master Center.	None	false	208	MULTI_CENTER		None
Security Design vGW is now delegated a center of Master center (IP %s)	Security Design vGW is now delegated a center of Master center.	None	false	209	MULTI_CENTER		None
Security Design vGW is no longer part of Multi-Center configuration	Security Design vGW is no longer part of Multi-Center configuration.	None	false	210	MULTI_CENTER		None
Multi-Center event: Added external inspection device (%s, %s)	Multi-Center event: Added external inspection device.	None	false	211	MULTI_CENTER		None
Multi-Center event: Updated external inspection device (%s, %s)	Multi-Center event: Updated external inspection device.	None	false	212	MULTI_CENTER		None
Multi-Center event: Added external inspection device (%s, %s)	Multi-Center event: Added external inspection device	None	false	213	MULTI_CENTER		None

Table 2: Multi-Center Event and Alert Messages (*continued*)

Message	Meaning	Action	User Assigned	Internal ID	Issuing Module	Submodule	Priority
Cannot synchronize IDS Signatures to delegated Center %s because its IDS version is lower than the minimum version that is compatible with this Center's version	Cannot synchronize IDS signatures to specified delegated center because its IDS version is lower than the minimum version that is compatible with this center's version.	Check IDS versions.	false	214	MULTI_CENTER		HIGH
Cannot Synchronize IDS Signatures to %s since it has no IDS license	Cannot synchronize IDS signatures to the specified delegated center because it has no IDS license.	Check IDS licenses.	false	215	MULTI_CENTER		HIGH
Cannot synchronize IDS Signatures to delegated Center %s because its IDS version is lower than the minimum version that is compatible with this Center's version. Delegate Center Configuration changed for %s	Cannot synchronize IDS signatures to the specified delegated center because its IDS version is lower than the minimum version that is compatible with this center's version. The delegate center's configuration was changed.	Check IDS versions.	false	216	MULTI_CENTER		HIGH
Cannot Synchronize IDS Signatures to %s since it has no IDS license. Delegate Center Configuration changed for %s	Cannot synchronize IDS signatures to the specified delegated center because it has no IDS license. Delegate Center Configuration was changed	Check IDS licenses.	false	217	MULTI_CENTER		HIGH
Delegate Center %s IP changed to %s	Delegate center changed IP.	None	false	218	MULTI_CENTER		HIGH
Delegate Center %s IP changed to %s. Failed to update Multi-Center configuration	Delegate Center changed IP. Failed to update Multi-Center configuration.	Check logs for details.	false	219	MULTI_CENTER		HIGH

Table 2: Multi-Center Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Delegated Center	This object is no longer synchronized with the Master Security Design vGW object by the same name. It is now a local object of the Delegated Center.	None	false	220	MULTI_CENTER	Delegated Center	None
%s "%s" was renamed to "%s" in order to prevent name collision with global %s	The specified object was renamed to prevent name collision between a global synchronized object and a local, delegated center object.	None	false	221	MULTI_CENTER	Delegated Center	None
Failed to communicate with Master Center.	The delegated center is unable to communicate with the Master Security Design vGW.	Verify that the Master is working properly. Check for network problems that could prevent communication between the Master and the delegated center. If the problem does not resolve, after some time, contact support.	false	222	MULTI_CENTER	Master Security Design vGW	HIGH
Failed to synchronize IDS Signatures with Master Center.	There was an error while trying to synchronize IDS signatures with the master Security Design vGW.	Go to the Master Security Design vGW Settings → MULTI_CENTER. Open the dialog for the delegated center and click Synchronize. If the situation persists, check the error logs and contact support.	false	223	MULTI_CENTER	IDS Signatures	HIGH

Table 2: Multi-Center Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Configuration Synchronization	There was an error while trying to synchronize configuration with the master Security Design vGW.	Go to the Master Security Design vGW Settings → MULTI_CENTER. Open the dialog for the delegated center and click Synchronize. If the situation persists, check the error logs and contact support.	false	224	MULTI_CENTER	Configuration Synchronization	HIGH
Modified Multi-Center configuration for "%s". %s	The delegated center configuration was changed.	None	true	225	MULTI_CENTER	Configuration	None

CHAPTER 4

vGW Series Firewall Messages

The vGW Series Firewall module allows you to define, apply, and monitor security policies. [Table 3 on page 15](#) identifies the messages that are issued in response to certain events and the occurrence of error conditions or problems that pertain to the Firewall module. For example, messages might inform you of policy configuration problems, initiation of policy updates, and log collection.

Table 3: Firewall Event and Alert Messages

Message	Meaning	Action	User Affected	Internal ID	Issuing Module	Submodule	Priority
failed to install policy for %s	Could not apply policy on the specified VM.	Check FW → Apply Policy screen.	true	401	FIREWALL	Install Policy	HIGH
failed to install policy for %s	Could not apply policy on the specified VMs.	Check FW → Apply Policy screen.	false	402	FIREWALL	Install Policy	HIGH
Default Policy does not have any inbound rules	The default policy does not have any inbound rules.	Check Default Policy to verify validity.	false	403	FIREWALL	Default Policy	MEDIUM
Default Policy does not have any outbound rules	The default policy does not have any outbound rules.	Check Default Policy to verify validity.	false	404	FIREWALL	Default Policy	MEDIUM
Default policy was installed with missing rules: %s	The default policy was installed with rules missing.	Check that all Default policy rules have valid source / destination and protocol / protocol groups.	false	405	FIREWALL	Default Policy	MEDIUM
firewall failed to respond while installing policies for %d VM(s). Affected: %s	Could not apply policy on the specified VMs.	Check FW → Apply Policy screen.	false	406	FIREWALL	Install Policy	LOW

Table 3: Firewall Event and Alert Messages (*continued*)

Message	Meaning	Action	User Alert	Internal ID	Issuing Module	Submodule	Priority
Installed policies for %d VM(s). Affected: %s	Policies were installed on the specified VMs.	None	false	407	FIREWALL	Install Policy	None
Expected %d VM(s) not found while installing policy. Missing: %s	The specified VMs were not found when the policy was being installed. They might have been migrated to other hosts.	Verify location of VMs and retry policy install.	false	408	FIREWALL	Install Policy	None
Batch firewall update scheduled to start immediately	Batch firewall update is scheduled to begin immediately.	None	true	409	FIREWALL	Batch Update	None
Batch firewall update scheduled to start on %s at %s	Batch firewall update is scheduled to begin later.	None	true	410	FIREWALL	Batch Update	None
Batch firewall update cancelled	Batch firewall update is cancelled.	None	true	411	FIREWALL	Batch Update	None
Initiated software %s to Security VM "%s"	Software update to Security VM was initiated.	None	true	412	FIREWALL		None
Finished software %s to Security VM "%s"	Software update to Security VM is completed.	None	true	413	FIREWALL		None
Log Collection on %s was started	Log collection on Security VM was started.	None	true	414	FIREWALL		None
Enabled "Automatically check for updates" for %s	"Automatically check for updates" was initiated for the specified Security VM.	None	true	415	FIREWALL		None
Disabled "Automatically check for updates" for %s	"Automatically check for updates" was disabled for the specified Security VM.	None	true	416	FIREWALL		None
User requested reboot of Security VM "%s"	User requested reboot of Security VM.	None	true	417	FIREWALL		None

Table 3: Firewall Event and Alert Messages (*continued*)

Message	Meaning	Action	User Alert	Internal ID	Issuing Module	Submodule	Priority
Could not auto-secure %s since it is poweredOn and has FaultTolerance? enabled	Could not auto-secure VM since it is poweredOn and has FaultTolerance? enabled.	Disable FaultTolerance? or suspend/powerOff the VM to have it secured.	false	418	FIREWALL		MEDIUM
Reconnected vNICs of VM "%s" after setting its vmsafe options	Reconnected vNICs of the specified VM after setting its VMsafe options.	None	true	419	FIREWALL		None
Suspending/restarting VM "%s" after reconfiguring its VMsafe options	After reconfiguring its VMsafe options, the specified VM is either suspended or restarted.	None	true	420	FIREWALL		None
Modified policy %s	Modified the specified policy.	None	true	421	FIREWALL		None
Dropped %s firewall events since %s (%s received)	Dropped firewall events.	Refer to product documentation.	false	422	FIREWALL		HIGH
Dropped %s connection events since %s (%s received)	Dropped connection events.	Refer to product documentation.	false	423	FIREWALL		HIGH
%s	Security VM changed status.	None	false	424	FIREWALL		HIGH
VM %s appears to be a possible Firewall on Host %s but it is not recognized by the Security Design vGW	This message warns that there might be an unmanaged firewall.	Go to Settings → Security VM Configuration to import the Firewall into the Security Design vGW.	false	425	FIREWALL		HIGH
%s %s %s %s	The indicated task was completed while installing, uninstalling, or updating a firewall.	None	true	426	FIREWALL		None
%s to %s %s %s	The indicated task failed while installing, uninstalling or updating a firewall.	None	true	427	FIREWALL		HIGH

Table 3: Firewall Event and Alert Messages (*continued*)

Message	Meaning	Action	User Alert	Internal ID	Issuing Module	Submodule	Priority
Automatic Securing of VMs was set to: %s	Auto Secure options are saved.	None	true	428	FIREWALL		None
Failed to set Automatic Securing of VMs options	Saving of Auto Secure options failed	None	true	429	FIREWALL		None
The policy for VM %s has been saved skipping the following rules because they are invalid: %s	The policy for a VM has been saved, skipping some rules because they are invalid.	Check policy rules.	false	430	FIREWALL		MEDIUM
AutoStart? option is turned off on some hosts. Host(s): %s. This will prevent firewalls on the listed ESX host(s) to be powered on automatically upon host reboot.	The AutoStart? option is turned off on some hosts. This will prevent firewalls on the ESX host(s) to be powered on automatically upon host reboot.	Check ESX autostart options.	false	431	FIREWALL		MEDIUM
The Firewall %s appears misconfigured. It does not have a sufficient number of vNICs	The firewall appears to be misconfigured. It does not have a sufficient number of vNICs.	Check Firewall configuration.	false	432	FIREWALL		HIGH
firewall '%s' sent: %s	This event is sent by the firewall.	None	false	433	FIREWALL	Fastpath Module	None
firewall '%s' sent: %s	This alert is sent by the firewall.	Unknown	false	434	FIREWALL	Fastpath Module	MEDIUM
firewall '%s' sent: %s	This is alert is sent by the firewall.	Unknown	false	435	FIREWALL	Fastpath Module	HIGH
%s	This is an event sent by the firewall when it protects VMs.	None	false	436	FIREWALL		None
%s	This event is sent by the firewall when it stops protecting VMs.	None	false	437	FIREWALL		None

Table 3: Firewall Event and Alert Messages (*continued*)

Message	Meaning	Action	User Alert	Internal ID	Issuing Module	Submodule	Priority
%s	This event is sent by the firewall when it is started.	None	false	438	FIREWALL		None
%s	This event is sent by the firewall when its administrator password is changed.	None	false	439	FIREWALL		None
%s	This alert is sent by the firewall when it detects a loop.	None	false	440	FIREWALL		HIGH
firewall rule alert: %s connection: %s	This alert is associated with policy rule.	None	false	441	FIREWALL	Policy	HIGH
secured VMs	There are VMs that should be secured but that are not in a secured zone or that do not have the VMsafe module applied to them.	Go to Settings → FW_INSTALL, and identify the VM(s) in the tree. If there is an alert sign near the VM node, follow the directions in the tooltip. Alternatively, try securing the VM or un-securing and then re-securing it.	false	442	FIREWALL	secured VMs	HIGH
%s was connected to the VMsafe Network, cannot disconnect Ethernet Card due to %s	This alert is associated with a possible security breach.	None	false	443	FIREWALL	Security Breach	HIGH
%s was connected to the VMsafe Network, cannot disconnect Ethernet Card due to %s	This alert is associated with the inability to disconnect a VM, causing a security breach.	None	false	444	FIREWALL	Security Breach	HIGH

CHAPTER 5

vGW Series Firewall Logs Messages

Table 4 on page 21 identifies messages issued pertaining to handling of firewall logs, such as the ability of the server to process them.

Table 4: Firewall Logs Event and Alert Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Unwanted %s %s	Alert on the given protocol had been defined.	None	false	3601	FW_LOGS		HIGH
Autoconfig address (%s) %s	Autoconfig address accord	None	false	3602	FW_LOGS		MEDIUM
multicast (%s) %s	multicast protocol	None	false	3603	FW_LOGS		LOW
%s	The server is overloaded and it is unable to insert firewall logs into the database.	Verify that polic the aes defined logs correctly.	false	3604	FW_LOGS		HIGH
%s	The server is overloaded and it is unable to process firewall logs.	Verify that the policies defined logs correctly.	false	3605	FW_LOGS		HIGH

CHAPTER 6

vGW Series Settings Messages

The vGW Series Settings module controls core operations. It covers a wide range of information. It contains application, security, and appliance sections that allow you to configure settings for various parts

of the systems. [Table 5 on page 23](#) identifies messages associated with the Settings module. For example, these messages might inform you that Network Traffic Monitoring, AntiVirus, and other features were enabled or disabled for a specific vGW Security VM, that VMs added to VMware's vCenter are now shown in the vGW Security Design VM tree, and that SSH was enabled or disabled.

Table 5: Settings Event and Alert Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Successful login to vCenter %s (Settings)	A successful connection to vCenter was made in Settings page.	None	true	601	SETTINGS		None
Failed login to vCenter %s (Settings)	An unsuccessful connection to vCenter was made in the Settings page.	Verify vCenter status and login/password and try again at Settings → vCenter Integration.	true	602	SETTINGS		None
Saved email settings (SMTP server: %s, port: %d, auth: %s, TLS auth: %s, SMTP user: %s)	Email settings were saved.	None	true	603	SETTINGS		None
Saved report settings (from: %s, subject: %s, content: %s)	Report settings were saved.	None	true	604	SETTINGS		None

Table 5: Settings Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Network Traffic Monitoring was enabled for Security VM "%s"	Network Traffic Monitoring was enabled.	None	true	605	SETTINGS		None
Network Traffic Monitoring was disabled for Security VM "%s"	Network Traffic Monitoring was disabled.	None	true	606	SETTINGS		None
Anti Virus Engine was enabled for Security VM "%s"	The vGW AntiVirus Engine was enabled.	None	true	607	SETTINGS		None
Anti Virus Engine was disabled for Security VM "%s"	The vGW AntiVirus Engine was disabled.	None	true	608	SETTINGS		None
Modified time zone to %s	Modified time zone.	None	true	609	SETTINGS		None
Modified NTP settings to %s	Modified NTP settings.	None	true	610	SETTINGS		None
Enabled automatic startup of the Security Design vGW and Security VM upon reboot of the host hardware.	Enabled automatic startup of the Security Design vGW and Security VM upon reboot of the host hardware.	None	true	611	SETTINGS		None
Disabled automatic startup of the Security Design vGW and Security VM upon reboot of the host hardware.	Disabled automatic startup of the Security Design vGW and Security VM upon reboot of the host hardware.	None	True	612	SETTINGS		None
Machine names in the Security Design vGW are updated when VMs are renamed in the vCenter	Machine names in the Security Design vGW are updated when VMs are renamed in the vCenter.	None	true	613	SETTINGS		None
NetFlow? enabled. Configuration: collector %s, port: %s	NetFlow? enabled.	None	true	614	SETTINGS		None

Table 5: Settings Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
NetFlow? enabled. Configuration: collector %s, port: %s	NetFlow? enabled.	None	true	615	SETTINGS	netflow	None
NetFlow? disabled	NetFlow? disabled.	None	true	616	SETTINGS	netflow	None
Modified NetFlow? config for Security VM"%s": enabled: %s, override global network config: %s, collector: %s,address: %s, collector port: %s	Modified NetFlow? config for Security VM.	None	true	617	SETTINGS	netflow	None
External logging (syslog) disabled	External logging (syslog) disabled.	None	true	618	SETTINGS	syslog	None
External logging (syslog) enabled from Security Design vGW, server: %s, port: %s	External logging (syslog) enabled from Security Design vGW.	None	true	619	SETTINGS	syslog	None
External logging (syslog) enabled from Security VM, server: %s, port: %s	External logging (syslog) enabled from Security VM.	None	true	620	SETTINGS	syslog	None
Modified syslog config for Security VM"%s": override global syslog config: %s, server: %s, server port: %s	Modified syslog config for Security VM.	None	true	621	SETTINGS	syslog	None
VMs which are deleted within vCenter will now be shown in inventory tree	VMs which are deleted within vCenter will now be shown in inventory tree.	None	true	622	SETTINGS		None
VMs which are deleted within vCenter will now be hidden in inventory tree	VMs which are deleted within vCenter will now be hidden in inventory tree.	None	true	623	SETTINGS		None
SSH mode was enabled	SSH mode was enabled.	None	true	624	SETTINGS		None

Table 5: Settings Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
SSH mode was disabled	SSH mode was disabled.	None	true	625	SETTINGS		None
Saved Active Directory settings for %s	Saved Active Directory settings.	None	true	626	SETTINGS		None
Modified Network Configuration with these details: hostname: %s, primary DNS: %s, secondary DNS: %s, DNS search: %s, default gateway: %s	Modified network configuration.	None	true	627	SETTINGS		None
Modified Proxy Settings with these details: http proxy: %s, http proxy port: %s, http proxy user: %s, https proxy: %s, https proxy port: %s, https proxy user: %s, NTLM Authentication: %s, NT domain: %s, Same settings for all proxy types: %s	Modified proxy settings.	None	true	628	SETTINGS		None
Infrastructure Configuration Enforcement changed to: disconnect the VM's vNIC	Infrastructure Configuration Enforcement changed to: Disconnect the VM's vNIC.	None	true	629	SETTINGS		None
Infrastructure Configuration Enforcement changed to: generate an alert	Infrastructure Configuration Enforcement changed to: Generate an alert.	None	true	630	SETTINGS		None
Canceled purging of vCenter deleted VMs within Security Design vGW	Canceled purging of vCenter deleted VMs within Security Design vGW.	None	true	631	SETTINGS		None

Table 5: Settings Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Canceled purging of vCenter deleted VMs within Security Design vGW	Canceled purging of vCenter deleted VMs within Security Design vGW.	None	true	632	SETTINGS		None
Delay before purging vCenter deleted VMs within Security Design vGW set to %s days	Set Delay before purging vCenter deleted VMs within Security Design vGW.	None	true	633	SETTINGS		None

CHAPTER 7

vGW Series SRX Messages

The vGW Series inter-operates with Junos OS SRX Series devices to provide support for zone synchronization and SRX Series IDP. [Table 6 on page 29](#) identifies the messages that are issued for events and conditions that pertain to SRX interoperability. For example, they might inform you that an SRX device configuration was created, removed, or updated, and that SRX zones were uploaded.

Table 6: SRX Event and Alert Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Created SRX %s device	Created SRX device.	None	true	1401	SRX_INTEGRATION		None
Updated SRX %s device	Updated SRX device.	None	true	1402	SRX_INTEGRATION		None
Removed SRX %s device	Removed SRX device.	None	true	1403	SRX_INTEGRATION		None
Saved SRX %s cert hash	Saved the certificate hash for SRX device.	None	true	1404	SRX_INTEGRATION		None
Imported group %s from SRX %s	One or more groups were imported from an SRX device configuration.	None	true	1405	SRX_INTEGRATION		None
Uploaded zones %s to SRX %s	Updated zone config on an SRX device from Security Design vGW group(s).	None	true	1406	SRX_INTEGRATION		None
Created task for SRX device %s	Created task for SRX device.	None	true	1407	SRX_INTEGRATION		None
Updated task for SRX device %s	Updated task for SRX device.	None	true	1408	SRX_INTEGRATION		None

CHAPTER 8

vGW Series Database Messages

The vGW Series writes network connection records and firewall logs to a database. [Table 7 on page 31](#) informs you of conditions pertaining to the database such as when the system begins to write logs of it and when it stops writing them.

Table 7: Database Event and Alert Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Severity	Priority
A Log Collection was automatically started due to a severe DB error.	A Log Collection was automatically started due to a severe DB error.	Go to Settings → Log Collection to view or upload the collection.	false	1601	DATABASE	Warning	HIGH
Start connection logs and idp alerts writing, disk usage: %s	Start connection logs and IDP alerts writing.	None	false	1602	DATABASE	Info	HIGH
Stop connection logs and idp alerts writing, disk usage: %s	Stop connection logs and IDP alerts writing.	None	false	1603	DATABASE	Info	HIGH

CHAPTER 9

vGW Series IDS Messages

The vGW Series includes a fully integrated IDS engine that allows you to monitor all virtual network traffic. You can monitor all traffic or traffic for a subset of VMs or protocols used.

[Table 8 on page 33](#) identifies the messages that pertain to the IDS module. For example, these messages provide information about the IDS signatures file, such as when it was updated successfully, automatically updated, or when update to it was disabled.

Table 8: IDS Event and Alert Error Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Severity	Priority
IDS signatures updated successfully	IDS signatures were updated successfully.	None	true	1801	IDS		None
IDS signatures failed to update	IDS signatures failed to update.	Check errors for details.	true	1802	IDS		None
Parsed file "%s", rules: new: %s, modified: %s, same: %s	Parsed new file.	None	false	1803	IDS		None
IDS Settings modified: EnableIDS=%s, HTTP ports=%s, SSL ports=%s	IDS Settings were modified.	None	true	1804	IDS		None
IDS Auto Update Disabled	IDS Auto Update Disabled.	None	true	1805	IDS		None
IDS Auto Update changed to: Download and Apply Update Automatically	IDS Auto Update changed to: Download and Apply Update Automatically.	None	true	1806	IDS		None
IDS Auto Update changed to: Download Automatically, Manually Apply Updates	IDS Auto Update changed to: Download Automatically, Manually Apply Updates.	None	true	1807	IDS		

Table 8: IDS Event and Alert Error Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Severity	Priority
Deleted IDS signature file %s	Deleted IDS signature file.	None	true	1808	IDS		None
Signature file %s uploaded	Signature file uploaded.	None	true	1809	IDS		None
The IDS sensor on %s dropped more than %s% of network packets	An IDS sensor has dropped more packets than the predefined limit.	Check IDS.	false	1810	IDS		MEDIUM
The IDS sensor on %s generated more than %s alerts per second	An IDS sensor is generating alerts faster than the predefined limit.	Check IDS.	false	1811	IDS		HIGH
Added external inspection device (%s, %s)	An external inspection device was added.	None	true	1812	IDS		None
Updated external inspection device (%s, %s)	An external inspection device was updated.	None	true	1813	IDS		None
Removed external inspection device (%s, %s)	An external inspection device was removed.	None	true	1814	IDS		None
IDS Signature configuration changed: %s	The IDS signature configuration was modified by an administrator.	None	true	1815	IDS		None

CHAPTER 10

vGW Series Licenses Messages

To use the vGW Series product, you must meet the license requirements. For each component and feature that you want to use that requires a license, you must install an entitlement license key using the vGW Security Design VM.

The following table identifies messages that pertain to licensing conditions and issues. For example, these messages might inform you that one or more licenses have been added, that licenses are missing, or that licenses were removed.

Table 9: License Event and Alert Messages

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
No license, starting 30 days of full function evaluation mode	There is no license installed. Starting 30 days of full function evaluation mode.	None	true	2601	LICENSE		None
Successfully added one or more licenses.	Successfully added one or more licenses.	None	true	2602	LICENSE		None
Successfully added one or more licenses, but with issues. %s	Successfully added one or more licenses, but with issues.	Investigate issues and try again.	true	2603	LICENSE		None
Unable to add licenses. %s	Unable to add licenses.	Investigate issues and try again.	true	2604	LICENSE		None
Removed license "%s..."	Removed license.	None	true	2605	LICENSE		None
Successfully uploaded %s license(s).	Successfully uploaded one or more licenses	None	true	2606	LICENSE		None
Successfully uploaded %slicense(s). %s	Successfully uploaded one or more licenses.	Check error for details.	true	2607	LICENSE		None

Table 9: License Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Hard ID	Issuing Module	Submodule	Priority
Error installing policy: no valid license.	Error installing policy. There is no valid license.	Add valid license before installing policy.	false	2608	LICENSE		None
Error installing AV policy: no valid license.	An error occurred while installing vGW AntiVirus policy: no valid license exists.	Add valid license before installing vGW AntiVirus policy.	false	2609	LICENSE		None

CHAPTER 11

vGW Series Compliance Messages

The vGW Series Compliance module allows you to monitor the overall compliance of your system with regard to industry standards and best practices as well as your own organizations.

The following table identifies the messages that pertain to Compliance module conditions and events. For example, these messages might inform you that certain VMs comply or do not comply with a compliance rule that you created.

Table 10: Compliance Event and Alert Messages

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Created compliance rule "%s" with weight %s, quarantine is %s	A compliance rule was created.	None	true	2401	COMPLIANCE		None
Modified compliance rule "%s" with weight %s, quarantine is %s	A compliance rule was modified.	None	true	2402	COMPLIANCE		None
Deleted compliance rule "%s"	A compliance rule was deleted compliance rule.	None	true	2403	COMPLIANCE		None
Compliance rule "%s" was renamed to "%s" in order to prevent name collision with global compliance rule	A compliance rule was renamed in order to prevent name collision with the global compliance rule.	None	false	2404	COMPLIANCE		None

Table 10: Compliance Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Alert for Compliance Rule "%s": %s compliance state changed from Comply to Non-Comply	Alert for Compliance Rule: The compliance state of some VMs was changed from Comply to Non-Comply	Check VM(s) against compliance rules.	false	2405	COMPLIANCE		HIGH
Rule "%s": %s compliance state changed from Non-Comply to Comply	Alert for Compliance Rule: The compliance state of some VMs was changed from Non-Comply to Comply.	Check VM(s) against compliance rules.	false	2406	COMPLIANCE		HIGH
Alert for Compliance Rule "%s": rule does not apply to %s anymore	Alert for Compliance Rule: Rule no longer applies to one or more VMs.	Check VM(s) against compliance rules.	false	2407	COMPLIANCE		HIGH
Alert for Compliance Rule "%s": %s were deleted	Alert for Compliance Rule: One or more VMs was deleted	None	false	2408	COMPLIANCE		HIGH
Alert for Compliance Rule "%s": %s added to complying VMs	Alert for Compliance Rule: One or more VMs were added to complying VMs.	None	false	2409	COMPLIANCE		HIGH
Alert for Compliance Rule "%s": %s added to non-complying VMs	Alert for Compliance Rule: One or more VMs were added to non-complying VMs.	None		2410	COMPLIANCE		HIGH

CHAPTER 12

vGW Series Introspection Messages

The vGW Series Introspection module lets you monitor software within the virtualized infrastructure that is installed in all MS Windows VMs and Linux VMs that support the RPM package manager. Using it, you can determine which applications are installed, the OS type, registry values, and hot fixes applied. It also includes a component called the Image Enforcer that allows you to create a template or VM that has a desirable configuration and compare the configurations of guest VMs against it, enforcing compliance to varying degrees.

[Table 11 on page 39](#) identifies the messages that pertain to the Introspection module and its Image Enforcer feature. For example, these messages might inform you that an Image Enforcer profile was created or deleted or that a disk scan was started.

Table 11: Introspection Event and Alert Messages

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Created Image Enforcer profile %s	Created Image Enforcer profile.	None	true	2201	IMAGE_ENFORCER		None
Updated Image Enforcer profile %s. %s	Updated Image Enforcer profile.	None	true	2202	IMAGE_ENFORCER		None
Removed Image Enforcer profile %s	Removed Image Enforcer profile.	None	true	2203	IMAGE_ENFORCER		None
Created %s schedule for %s	Created Schedule.	None	true	801	INTROSPECTION		None
Updated %s schedule for %s	Updated Schedule.	None	true	802	INTROSPECTION		None
Removed %s schedule for %s	Removed schedule.	None	true	803	INTROSPECTION		None

Table 11: Introspection Event and Alert Messages (*continued*)

Started %s disk scan for the following machine(s): %s	A disk scan process was started.	None	false	804	INTROSPECTION	None
Disk scan error for %s: %s	A disk scan error occurred.	None	false	805	INTROSPECTION	MEDIUM
Registry value (name: %s, key: %s, value: %s) has been created	A new Registry Value was added .	None	true	806	INTROSPECTION	None
Registry value (name: %s, key: %s, value: %s) has been modified	A Registry Value was deleted.	None	true	807	INTROSPECTION	None
Registry value (name: %s, key: %s, value: %s) has been deleted	An existing Registry Value was modified.	None	true	808	INTROSPECTION	None
	Snapshot of VM created for introspection has been removed	None	false	809	INTROSPECTION	MEDIUM

CHAPTER 13

vGW Series High Availability Messages

The vGW Series high availability feature allows for deployment of primary and secondary vGW Security VMs and vGW Security Design VMs.

Table 12 on page 41 identifies the messages that are issued pertaining to high availability events and conditions. For example, these message might inform you about problems with the standby appliance or recovery from those problems.

Table 12: High Availability Event and Alert Messages

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
lost communication with Standby Appliance.	For some reason, the Standby appliance is no longer communicating with the Security Design vGW.	Go to Settings → High Availability. Also verify that the standby appliance is turned on, and that it is connected to the network.	false	2801	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
It seems that machine with IP %s thinks it is a Standby Appliance, but there is no Standby Appliance configured, please turn off that machine.	A VM is trying to communicate with the Security Design vGW as if it is a Standby Appliance, but High Availability is not configured.	Find the VM with the specified IP and turn it off.	false	2802	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
Time is not synced with the Standby Appliance.	Time is not synchronized between Security Design vGW and the Standby Appliance.	Verify that Settings → Time Settings is configured correctly.	false	2803	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH

Table 12: High Availability Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Standby Appliance IP changed from %s to %s. Trying to recover from change.	Standby Appliance changed IP address, and the Security Design vGW is trying to accommodate automatically to the change.	None	false	2804	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
Recovered from Standby Appliance IP change.	Standby Appliance changed IP address, and the Security Design vGW was able to successfully accommodate the change.	None	false	2805	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
Failed to recover from IP change of the Standby Appliance.	Standby Appliance changed IP address, and the Security Design vGW could not recover automatically from that change.	Turn off the Standby Appliance VM. Go to Settings → High Availability and reconfigure it.	false	2806	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
Standby appliance Mirror Database error. %s	The standby appliance is not syncing properly with Security Design vGW.	If the problem persists, go to Settings → High Availability and reconfigure Standby appliance.	false	2807	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
restarted Standby application in %s mode	The standby appliance was restarted.	None	false	2808	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH
Standby Appliance Global Admin's Console administrator's password is not synced with the Primary Appliance	Global Admin's console password on the standby appliance was not synced with the Master Security Design vGW Global Admin's console password.	Check the error log. Try to restart the standby appliance.	false	2809	HIGH_AVAILABILITY	Standby Security Design vGW	HIGH

Table 12: High Availability Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Internal ID	Issuing Module	Submodule	Priority
Added Master center (IP %s) certificate to the center's keystore	Added Master center certificate to the center's keystore .	None	false	2810	HIGH_AVAILABILITY		None
Added delegated center "%s" certificate to the center's keystore	A delegated center certificate was added to the center's keystore.	None	false	2811	HIGH_AVAILABILITY		None

CHAPTER 14

vGW Series AntiVirus Messages

The vGW Series AntiVirus feature allows you to protect your provides two means of protecting your virtualized environment against malware and viruses in real time and through offline scans. [Table 13 on page 45](#) identifies the messages that pertain to AntiVirus events and conditions. For example, you might be informed that AntiVirus signatures are being downloaded or that there was a problem downloading them.

Table 13: AntiVirus Event and Alert Messages

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Antivirus global setting %s was changed to: %s.	Antivirus global setting was changed.	None	true	2001	ANTI_VIRUS		None
Virus %s was detected on %s %s	Either the on-demand or the on-access scan found a virus on the machine.	Check the machine.	false	2002	ANTI_VIRUS		HIGH
Error downloading AntiVirus signatures.	The process that runs automatically and checks for updates could not download the new signature file.	Check that Security Design vGW have an access to the web	false	2003	ANTI_VIRUS		HIGH
AntiVirus download signatures error resolved.	The process that runs automatically and checks for updates succeeded in downloading a new version.	None	false	2004	ANTI_VIRUS		HIGH
%s antivirus setting '%s' (id: %s)	A user modified, created, or deleted antivirus scan settings.	None	true	2005	ANTI_VIRUS		None

Table 13: AntiVirus Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Hard ID	Issuing Module	Submodule	Priority
Multi-Center event: %s antivirus setting %s (id: %s)	The Multi-Center master modified, created, or deleted antivirus scan settings.	None	true	2006	ANTI_VIRUS		None
Deleted schedule for %s %s		None	true	2007	ANTI_VIRUS	Schedule	HIGH

CHAPTER 15

vGW Series ESP and VMware vCenter Messages

Table 14 on page 47 identifies messages that pertain to the vGW Series interaction with VMware vCenter.

Table 14: ESP and VMware vCenter Event and Alert Messages

Message	Meaning	Action	User Associated	Event ID	Issuing Module	Submodule	Priority
Found %s machines with same %s: %s	The uuid/vcUuid provided by the SVM is not unique.	None	false	3001	ESP		HIGH
Found no VM with %s : %s	The uuid/vcUuid provided by the SVM does not match any known VM.	None	false	3002	ESP		HIGH
ESX host %s has %s. Correct firewall functionality requires a unique and valid UUID.	Host has invalid or overlapping UUID.	Check the ESX host for a valid non-overlapping UUID.	false	1001	VC_GENERATED		HIGH
Updated vEthernet cards for %s - %s	The virtual Ethernet cards of the specified VMs were automatically reconfigured.	None	false	1201	VC_RELATED		HIGH
Error disconnecting non compliant VM %s	An error occurred while disconnecting the NICs of the specified non-compliant VMs.	None	false	1202	VC_RELATED		HIGH

Table 14: ESP and VMware vCenter Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Hard ID	Issuing Module	Submodule	Priority
vCenter on server "%s" unavailable: three consecutive failures to retrieve events using username "%s"	The Security Design vGW failed to retrieve events from the vCenter.	Check that the vCenter is up, and that the credentials in Settings → VIRTUAL_CENTER are correct.	false	1203	VC_RELATED		None
%s	The Security Design vGW reconfigured a VM. This may have been done for one of several reasons is described in the alert text.	None	false	1204	VC_RELATED		None

CHAPTER 16

vGW Series Reports Messages

The vGW Series Reports module allows you to create automated reports. [Table 15 on page 49](#) identifies the messages issued for conditions and events pertaining to reports, such as when a report was generated and when it failed to be generated.

Table 15: Reports Event and Alert Messages

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Deleted schedule for report %s		None	true	3201	REPORTS		HIGH
Report: '%s' was successfully generated	The report was successfully generated.	None	false	3202	REPORTS		None
Failed to generate report '%s'	Failed to generate report.	Check results and try again.	false	3203	REPORTS		HIGH
%s report "%s" of type "%s"	A report was edited or created.	None	true	3204	REPORTS		None

CHAPTER 17

vGW Series Inventory Messages

Table 16 on page 51 identifies the messages that the vGW Series issues pertaining to management of its object inventory occur. For example, these message might inform you that a protocol or a network has been added, updated, or deleted. They might report that a VM has been added or that one has been deleted.

Table 16: Inventory Event and Alert Messages

Message	Meaning	Action	User Associated	Hard ID	Issuing Module	Submodule	Priority
Added protocol %s	A user created the specified new protocol.	None	true	3401	INVENTORY		None
Updated protocol %s. %s	A user updated the specified protocol.	None	true	3402	INVENTORY		None
Deleted protocol %s	A user removed the specified protocol.	None	true	3403	INVENTORY		None
Added network %s	A user added the specified new network.	None	true	3404	INVENTORY		None
Updated network %s. %s	A user updated the specified network.	None	true	3405	INVENTORY		None
Deleted network %s	A user removed the specified network.	None	true	3406	INVENTORY		None
Added protocol group %s	A user created the new specified protocol group.	None	true	3407	INVENTORY		None
Updated protocol group %s. %s	A user updated the specified protocol group.	None	true	3408	INVENTORY		None
Deleted protocol group %s	A user removed the specified protocol group.	None	true	3409	INVENTORY		None

Table 16: Inventory Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Alert ID	Issuing Module	Submodule	Priority
Added machine %s	A user created the specified new machine.	None	true	3410	INVENTORY		None
Updated machine %s. %s	A user updated the specified machine.	None	true	3411	INVENTORY		None
Deleted machine %s	A user removed the specified machine.	None	true	3412	INVENTORY		None
Modified machine name from "%s" to "%s"	The specified machine name was modified.	None	false	3413	INVENTORY		None
Modified vCenter name from "%s" to "%s" for %s	The vCenter name was modified.	None	false	3414	INVENTORY		None
Error persisting machine name change from "%s" to "%s"	Failed to update the machine name.	None	false	3415	INVENTORY		None
Error persisting vCenter name change from "%s" to "%s" for %s	Failed to update the vCenter name.	None	false	3416	INVENTORY		None
Modified VM "%s": %s	The Machine IP addresses changed.	None	false	3417	INVENTORY		None
Modified VM "%s": %s	The Machine Mac addresses changed.	None	false	3418	INVENTORY		None
%s	This event provides information about group changes: group creation, group deletion, or changes in group members.	None	true	3419	INVENTORY	Groups	None
VMs updated from vCenter %s	The Security Design vGW inventory was updated from the vCenter. The specific changes are described in the alert message text.	None		3420	INVENTORY		None

Table 16: Inventory Event and Alert Messages (*continued*)

Message	Meaning	Action	User Associated	Hard ID	Issuing Module	Submodule	Priority
Added VM "%s"	The specified VM was added to the inventory.	None		3421	INVENTORY		None

CHAPTER 18

vGW Series System Backup Messages

vGW Series includes a feature that allows you to back up and restore the vGW Security Design VM. [Table 17 on page 55](#) identifies the messages that pertain to this feature, including messages that inform you about the backup schedule, the host used, and the path to that host.

Table 17: System Backup Event and Alert Messages

Message	Meaning	Action	User Associated	Host ID	Issuing Module	Submodule	Priority
Backup setting schedule changed, enable = %s	Backup setting schedule changed state.	None	true	3801	SYSTEM_BACKUP		None
Backup setting number of backups changed to: %s	Backup setting number of backups changed quantity.	None	true	3802	SYSTEM_BACKUP		None
Backup setting host changed to: %s	Backup setting host was changed.	None	true	3803	SYSTEM_BACKUP		None
Backup setting path changed to: %s	Backup setting path was changed to the specified value.	None	true	3804	SYSTEM_BACKUP		None
Backup setting user name changed to: %s	Backup setting user name was changed to the specified value.	None	true	3805	SYSTEM_BACKUP		None
Backup was scheduled for immediate execution	Backup was scheduled for immediate execution.	None	true	3806	SYSTEM_BACKUP		None
Restore backup.	Restore backup.	None	true	3807	SYSTEM_BACKUP		None

PART 2

Index

- [Index on page 59](#)

Index

A

AntiVirus messages.....45

C

compliance messages.....37

customer support.....xiv

 contacting JTAC.....xiv

D

documentation

 comments on.....xiv

E

ESP and vCenter messages.....47

F

firewall logs messages.....21

firewall messages.....15

H

high availability messages.....41

I

IDS messages.....33

Image Enforcer messages.....39

introspection messages.....39

inventory messages.....51

L

licenses messages.....35

M

management messages.....5

manuals

 comments on.....xiv

Multi-Center messages.....9

R

reports messages.....49

S

settings messages.....23

SRX messages.....29

support, technical See technical support

system backup messages.....55

T

technical support

 contacting JTAC.....xiv

