



# Fabric OS

## System Error Message Reference Manual

**Supporting Fabric OS v4.4.0**

**Supporting SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, 24000**

Copyright © 2004, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

Publication Number: 53-0000515-09

Brocade, the Brocade B weave logo, Secure Fabric OS, and SilkWorm are registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON, IBM **@server** BladeCenter are registered trademarks of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade’s patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

## **Brocade Communications Systems, Incorporated**

### **Corporate Headquarters**

Brocade Communications Systems, Inc.  
1745 Technology Drive  
San Jose, CA 95110  
Tel: 1-408-333-8000  
Fax: 1-408-333-8101  
E-mail: [info@brocade.com](mailto:info@brocade.com)

### **Latin America Headquarters**

Brocade Communications System, Inc.  
5201 Blue Lagoon Drive  
Miami, FL 33126  
Tel: 1-305-716-4165  
E-mail: [latinam-sales@brocade.com](mailto:latinam-sales@brocade.com)

### **European Headquarters**

Brocade Communications Switzerland Sàrl  
Centre Swissair  
Tour A - 2ème étage  
29, Route de l'Aéroport  
Case Postale 105  
CH-1215 Genève 15  
Switzerland  
Tel: +41 22 799 56 40  
Fax: +41 22 799 56 41  
E-mail: [emea-info@brocade.com](mailto:emea-info@brocade.com)

### **Asia-Pacific Headquarters**

Brocade Communications Systems K.K.  
Shiroyama JT Trust Tower 36th FL.  
4-3-1 Toranomom, Minato-ku  
Tokyo, Japan 105-6036  
Tel: +81-3-5402-5300  
Fax: +81-3-5402-5399  
E-mail: [japan-info@brocade.com](mailto:japan-info@brocade.com)

## Document History

The following table lists all versions of the *Fabric OS System Error Message Reference Manual*.

Document Title	Publication Number	Summary of Changes	Publication Date
<i>Diagnostic and System Error Message Reference v3.0, v4.0</i>	53-0000210-02	First release.	March 2002
<i>Diagnostic and System Error Message Reference v3.1.0</i>	53-0000511-04	Major content reorganization.	June 2003
<i>Diagnostic and System Error Message Reference v4.1.0</i>	53-0000515-02	Major content reorganization.	June 2003
<i>Diagnostic and System Error Message Reference v4.1.2</i>	53-0000515-06	Minor editorial changes.	October 2003
<i>Diagnostic and System Error Message Reference v4.2.0</i>	53-0000515-07	Add FW and PLATFORM messages.	December 2003
<i>Diagnostic and System Error Message Reference v4.2.0</i>	53-0000515-08	Update software and hardware support.	March 2004
<i>Fabric OS System Error Message Reference Manual</i>	53-0000515-09	Updated for v4.4.0. First RASLog release.	August 2004



# Contents

---

## About This Document

How This Document Is Organized . . . . .	xxxv
Supported Hardware and Software . . . . .	xxxvi
Document Conventions . . . . .	xxxvii
Getting Technical Help . . . . .	xl
Document Feedback . . . . .	xl

## Chapter 1 Introduction to System Messages

Changes for This Release of the Fabric OS . . . . .	1-1
Message Severity Levels . . . . .	1-2
Overview of the System Messages . . . . .	1-2
System Message Log (RASLog) . . . . .	1-3
Security Audit Logging . . . . .	1-3
Dual-CP Systems . . . . .	1-4
System Logging Daemon . . . . .	1-4
Port Logs . . . . .	1-5
Panic Dump and Core Dump Files . . . . .	1-5
Trace Dumps . . . . .	1-5
supportSave Command . . . . .	1-6
System Console . . . . .	1-6
View or Configure the System Message Logs . . . . .	1-6
Reading a System Message . . . . .	1-8
Example System Message . . . . .	1-8
Viewing System Messages from Advanced Web Tools . . . . .	1-9
Dumping the System Messages . . . . .	1-9
Viewing the System Messages with Page Breaks . . . . .	1-10
Clearing the System Message Log . . . . .	1-10

Responding to a System Message . . . . .	1-11
Looking Up a System Message . . . . .	1-11
Gathering Information About the Problem . . . . .	1-11
System Module Descriptions . . . . .	1-12

## **Chapter 2 AUTH Error Messages**

AUTH-1001 . . . . .	2-1
AUTH-1002 . . . . .	2-1
AUTH-1003 . . . . .	2-1
AUTH-1004 . . . . .	2-2
AUTH-1005 . . . . .	2-2
AUTH-1006 . . . . .	2-2
AUTH-1007 . . . . .	2-3
AUTH-1008 . . . . .	2-3
AUTH-1010 . . . . .	2-3
AUTH-1011 . . . . .	2-4
AUTH-1012 . . . . .	2-4
AUTH-1013 . . . . .	2-5
AUTH-1014 . . . . .	2-5
AUTH-1017 . . . . .	2-5
AUTH-1018 . . . . .	2-6
AUTH-1020 . . . . .	2-6
AUTH-1022 . . . . .	2-7
AUTH-1023 . . . . .	2-7
AUTH-1025 . . . . .	2-8
AUTH-1027 . . . . .	2-8
AUTH-1028 . . . . .	2-8
AUTH-1029 . . . . .	2-9
AUTH-1030 . . . . .	2-9
AUTH-1031 . . . . .	2-10
AUTH-1032 . . . . .	2-10
AUTH-1033 . . . . .	2-11

AUTH-1034 .....	2-11
AUTH-1035 .....	2-11
AUTH-1036 .....	2-12
AUTH-1037 .....	2-12
AUTH-1038 .....	2-13

**Chapter 3 BL Error Messages**

BL-1000 .....	3-1
BL-1001 .....	3-1
BL-1002 .....	3-1
BL-1003 .....	3-2
BL-1004 .....	3-2
BL-1006 .....	3-3
BL-1007 .....	3-3
BL-1008 .....	3-3
BL-1009 .....	3-4
BL-1010 .....	3-4
BL-1011 .....	3-5
BL-1012 .....	3-5
BL-1013 .....	3-6
BL-1014 .....	3-6
BL-1015 .....	3-7
BL-1016 .....	3-7

**Chapter 4 BLL Error Messages**

BLL-1000 .....	4-1
----------------	-----

**Chapter 5 CER Error Messages**

CER-1001 .....	5-1
----------------	-----

**Chapter 6 EM Error Messages**

EM-1001 .....	6-1
---------------	-----

EM-1002	6-1
EM-1003	6-2
EM-1004	6-2
EM-1005	6-3
EM-1006	6-4
EM-1007	6-4
EM-1008	6-4
EM-1009	6-5
EM-1010	6-5
EM-1011	6-6
EM-1012	6-6
EM-1013	6-6
EM-1014	6-7
EM-1015	6-8
EM-1016	6-8
EM-1017	6-8
EM-1028	6-9
EM-1029	6-10
EM-1031	6-10
EM-1033	6-11
EM-1034	6-11
EM-1036	6-12
EM-1041	6-12
EM-1042	6-13
EM-1043	6-14
EM-1044	6-14
EM-1045	6-14
EM-1046	6-15
EM-1047	6-15
EM-1048	6-16
EM-1049	6-16



EM-1050 .....	6-17
EM-1051 .....	6-18
EM-1052 .....	6-18
EM-1053 .....	6-19
EM-1055 .....	6-19
EM-1056 .....	6-20

**Chapter 7 EVMD Error Messages**

EVMD-1001 .....	7-1
-----------------	-----

**Chapter 8 FABR Error Messages**

FABR-1001 .....	8-1
FABR-1002 .....	8-1
FABR-1003 .....	8-2
FABR-1004 .....	8-2
FABR-1005 .....	8-3
FABR-1006 .....	8-3
FABR-1007 .....	8-3
FABR-1008 .....	8-4
FABR-1009 .....	8-4
FABR-1010 .....	8-4
FABR-1011 .....	8-5
FABR-1012 .....	8-5
FABR-1013 .....	8-5
FABR-1014 .....	8-6
FABR-1015 .....	8-6
FABR-1016 .....	8-7
FABR-1017 .....	8-7
FABR-1018 .....	8-7
FABR-1019 .....	8-8
FABR-1020 .....	8-8
FABR-1021 .....	8-8

	FABR-1022 .....	8-9
	FABR-1023 .....	8-9
	FABR-1024 .....	8-10
	FABR-1029 .....	8-10
<b>Chapter 9</b>	<b>FABS Error Messages</b>	
	FABS-1001 .....	9-1
	FABS-1002 .....	9-1
	FABS-1004 .....	9-1
	FABS-1005 .....	9-2
	FABS-1006 .....	9-2
	FABS-1007 .....	9-3
	FABS-1008 .....	9-3
	FABS-1009 .....	9-3
	FABS-1010 .....	9-4
<b>Chapter 10</b>	<b>FCMC Error Messages</b>	
	FCMC-1001 .....	10-1
<b>Chapter 11</b>	<b>FCPD Error Messages</b>	
	FCPD-1001 .....	11-1
	FCPD-1002 .....	11-1
	FCPD-1003 .....	11-2
<b>Chapter 12</b>	<b>FCPH Error Messages</b>	
	FCPH-1001 .....	12-1
<b>Chapter 13</b>	<b>FICU Error Messages</b>	
	FICU-1001 .....	13-1
	FICU-1002 .....	13-1
	FICU-1003 .....	13-2
	FICU-1004 .....	13-2

	FICU-1005 .....	13-2
	FICU-1006 .....	13-3
	FICU-1007 .....	13-3
	FICU-1008 .....	13-3
	FICU-1009 .....	13-4
<b>Chapter 14</b>	<b>FKLB Error Messages</b>	
	FKLB-1001.....	14-1
<b>Chapter 15</b>	<b>FLOD Error Messages</b>	
	FLOD-1001.....	15-1
	FLOD-1003.....	15-1
	FLOD-1004.....	15-1
	FLOD-1005.....	15-2
	FLOD-1006.....	15-2
<b>Chapter 16</b>	<b>FSPF Error Messages</b>	
	FSPF-1001 .....	16-1
	FSPF-1002 .....	16-1
	FSPF-1003 .....	16-1
	FSPF-1005 .....	16-2
	FSPF-1006 .....	16-2
<b>Chapter 17</b>	<b>FSS Error Messages</b>	
	FSS-1001 .....	17-1
	FSS-1002 .....	17-1
	FSS-1003 .....	17-2
	FSS-1004 .....	17-2
	FSS-1005 .....	17-2
	FSS-1006 .....	17-3

## **Chapter 18 FSSM Error Messages**

FSSM-1002.....	18-1
FSSM-1003.....	18-1
FSSM-1004.....	18-2

## **Chapter 19 FW Error Messages**

FW-1001 .....	19-1
FW-1002 .....	19-1
FW-1003 .....	19-2
FW-1004 .....	19-2
FW-1005 .....	19-2
FW-1006 .....	19-3
FW-1007 .....	19-3
FW-1008 .....	19-3
FW-1009 .....	19-4
FW-1010 .....	19-4
FW-1011 .....	19-4
FW-1012 .....	19-5
FW-1033 .....	19-5
FW-1034 .....	19-5
FW-1035 .....	19-6
FW-1036 .....	19-6
FW-1037 .....	19-6
FW-1038 .....	19-7
FW-1039 .....	19-7
FW-1040 .....	19-7
FW-1041 .....	19-8
FW-1042 .....	19-8
FW-1043 .....	19-8
FW-1044 .....	19-9
FW-1045 .....	19-9

FW-1046 .....	19-10
FW-1047 .....	19-10
FW-1048 .....	19-10
FW-1049 .....	19-11
FW-1050 .....	19-11
FW-1051 .....	19-11
FW-1052 .....	19-12
FW-1113 .....	19-12
FW-1114 .....	19-12
FW-1115 .....	19-13
FW-1116 .....	19-13
FW-1117 .....	19-13
FW-1118 .....	19-14
FW-1119 .....	19-14
FW-1120 .....	19-15
FW-1121 .....	19-15
FW-1122 .....	19-15
FW-1123 .....	19-16
FW-1124 .....	19-16
FW-1125 .....	19-17
FW-1126 .....	19-17
FW-1127 .....	19-18
FW-1128 .....	19-18
FW-1129 .....	19-19
FW-1130 .....	19-19
FW-1131 .....	19-19
FW-1132 .....	19-20
FW-1133 .....	19-20
FW-1134 .....	19-20
FW-1135 .....	19-21
FW-1136 .....	19-21

FW-1137 .....	19-21
FW-1138 .....	19-22
FW-1139 .....	19-22
FW-1140 .....	19-22
FW-1141 .....	19-23
FW-1142 .....	19-23
FW-1143 .....	19-23
FW-1144 .....	19-24
FW-1160 .....	19-24
FW-1161 .....	19-24
FW-1162 .....	19-25
FW-1163 .....	19-25
FW-1164 .....	19-26
FW-1165 .....	19-26
FW-1166 .....	19-26
FW-1167 .....	19-27
FW-1168 .....	19-27
FW-1169 .....	19-27
FW-1170 .....	19-28
FW-1171 .....	19-28
FW-1172 .....	19-29
FW-1173 .....	19-29
FW-1174 .....	19-29
FW-1175 .....	19-30
FW-1176 .....	19-30
FW-1177 .....	19-30
FW-1178 .....	19-31
FW-1179 .....	19-31
FW-1180 .....	19-31
FW-1181 .....	19-32
FW-1182 .....	19-32

FW-1183 .....	19-32
FW-1184 .....	19-33
FW-1185 .....	19-33
FW-1186 .....	19-33
FW-1187 .....	19-34
FW-1188 .....	19-34
FW-1189 .....	19-34
FW-1190 .....	19-35
FW-1191 .....	19-35
FW-1192 .....	19-35
FW-1193 .....	19-36
FW-1194 .....	19-36
FW-1195 .....	19-36
FW-1216 .....	19-37
FW-1217 .....	19-37
FW-1218 .....	19-38
FW-1219 .....	19-38
FW-1240 .....	19-38
FW-1241 .....	19-39
FW-1242 .....	19-39
FW-1243 .....	19-40
FW-1244 .....	19-40
FW-1245 .....	19-40
FW-1246 .....	19-41
FW-1247 .....	19-41
FW-1248 .....	19-41
FW-1249 .....	19-42
FW-1250 .....	19-42
FW-1251 .....	19-42
FW-1272 .....	19-43
FW-1273 .....	19-43

FW-1274 .....	19-44
FW-1275 .....	19-44
FW-1296 .....	19-44
FW-1297 .....	19-45
FW-1298 .....	19-45
FW-1299 .....	19-46
FW-1300 .....	19-46
FW-1301 .....	19-46
FW-1302 .....	19-47
FW-1303 .....	19-47
FW-1304 .....	19-48
FW-1305 .....	19-48
FW-1306 .....	19-48
FW-1307 .....	19-49
FW-1308 .....	19-49
FW-1309 .....	19-50
FW-1310 .....	19-50
FW-1311 .....	19-50
FW-1312 .....	19-51
FW-1313 .....	19-51
FW-1314 .....	19-51
FW-1315 .....	19-52
FW-1316 .....	19-52
FW-1317 .....	19-52
FW-1318 .....	19-53
FW-1319 .....	19-53
FW-1320 .....	19-54
FW-1321 .....	19-54
FW-1322 .....	19-54
FW-1323 .....	19-55
FW-1324 .....	19-55



FW-1325 .....	19-56
FW-1326 .....	19-56
FW-1327 .....	19-56
FW-1328 .....	19-57
FW-1329 .....	19-57
FW-1330 .....	19-57
FW-1331 .....	19-58
FW-1332 .....	19-58
FW-1333 .....	19-59
FW-1334 .....	19-59
FW-1335 .....	19-59
FW-1336 .....	19-60
FW-1337 .....	19-60
FW-1338 .....	19-61
FW-1339 .....	19-61
FW-1340 .....	19-61
FW-1341 .....	19-62
FW-1342 .....	19-62
FW-1343 .....	19-63
FW-1344 .....	19-63
FW-1345 .....	19-63
FW-1346 .....	19-64
FW-1347 .....	19-64
FW-1348 .....	19-65
FW-1349 .....	19-65
FW-1350 .....	19-66
FW-1351 .....	19-66
FW-1352 .....	19-66
FW-1353 .....	19-67
FW-1354 .....	19-67
FW-1355 .....	19-68

FW-1356 .....	19-68
FW-1357 .....	19-68
FW-1358 .....	19-69
FW-1359 .....	19-69
FW-1360 .....	19-70
FW-1361 .....	19-70
FW-1362 .....	19-70
FW-1363 .....	19-71
FW-1364 .....	19-71
FW-1365 .....	19-71
FW-1366 .....	19-72
FW-1367 .....	19-72
FW-1368 .....	19-72
FW-1369 .....	19-73
FW-1370 .....	19-73
FW-1371 .....	19-73
FW-1372 .....	19-74
FW-1373 .....	19-74
FW-1374 .....	19-75
FW-1375 .....	19-75
FW-1376 .....	19-75
FW-1377 .....	19-76
FW-1378 .....	19-76
FW-1379 .....	19-77
FW-1400 .....	19-77
FW-1401 .....	19-77
FW-1402 .....	19-78
FW-1403 .....	19-78
FW-1424 .....	19-78
FW-1425 .....	19-79
FW-1426 .....	19-79

FW-1427 .....	19-79
FW-1428 .....	19-80
FW-1429 .....	19-80
FW-1430 .....	19-80
FW-1431 .....	19-81
FW-1432 .....	19-81
FW-1433 .....	19-81
FW-1434 .....	19-82
FW-1435 .....	19-82
FW-1436 .....	19-82
FW-1437 .....	19-83
FW-1438 .....	19-83
FW-1439 .....	19-83
FW-1440 .....	19-84
FW-1441 .....	19-84
FW-1442 .....	19-84
FW-1443 .....	19-85
FW-1444 .....	19-85

**Chapter 20 HAM Error Messages**

HAM-1001 .....	20-1
HAM-1002 .....	20-1
HAM-1004 .....	20-2
HAM-1005 .....	20-2

**Chapter 21 HAMK Error Messages**

HAMK-1001 .....	21-1
HAMK-1002 .....	21-1
HAMK-1003 .....	21-2

**Chapter 22 HIL Error Messages**

HIL-1101 .....	22-1
----------------	------

HIL-1102.....	22-1
HIL-1103.....	22-2
HIL-1104.....	22-2
HIL-1105.....	22-2
HIL-1106.....	22-3
HIL-1107.....	22-3
HIL-1108.....	22-4
HIL-1201 .....	22-4
HIL-1202 .....	22-5
HIL-1203 .....	22-5
HIL-1204 .....	22-5
HIL-1205 .....	22-6
HIL-1206 .....	22-6
HIL-1301 .....	22-7
HIL-1302 .....	22-7
HIL-1303 .....	22-7
HIL-1304 .....	22-8
HIL-1305 .....	22-8
HIL-1306 .....	22-8
HIL-1307 .....	22-9
HIL-1308 .....	22-9
HIL-1309 .....	22-9
HIL-1401 .....	22-10
HIL-1402 .....	22-10
HIL-1403 .....	22-10
HIL-1404 .....	22-11
HIL-1501 .....	22-11
HIL-1502 .....	22-11
HIL-1503 .....	22-12
HIL-1504 .....	22-12
HIL-1505 .....	22-13

	HIL-1506 .....	22-13
	HIL-1507 .....	22-13
	HIL-1508 .....	22-14
	HIL-1509 .....	22-14
	HIL-1601 .....	22-15
	HIL-1602 .....	22-15
<b>Chapter 23</b>	<b>HLO Error Messages</b>	
	HLO-1001 .....	23-1
	HLO-1002 .....	23-1
	HLO-1003 .....	23-2
<b>Chapter 24</b>	<b>HMON Error Messages</b>	
	HMON-1001 .....	24-1
<b>Chapter 25</b>	<b>HTTP Error Messages</b>	
	HTTP-1001 .....	25-1
<b>Chapter 26</b>	<b>KSWD Error Messages</b>	
	KSWD-1003 .....	26-1
<b>Chapter 27</b>	<b>KTRC Error Messages</b>	
	KTRC-1001 .....	27-1
	KTRC-1002 .....	27-1
	KTRC-1003 .....	27-1
	KTRC-1004 .....	27-2
<b>Chapter 28</b>	<b>LOG Error Messages</b>	
	LOG-1000 .....	28-1
	LOG-1001 .....	28-1
	LOG-1002 .....	28-1

<b>Chapter 29</b>	<b>LSDB Error Messages</b>	
	LSDB-1001 .....	29-1
	LSDB-1002 .....	29-1
	LSDB-1003 .....	29-1
	LSDB-1004 .....	29-2
<b>Chapter 30</b>	<b>MFIC Error Messages</b>	
	MFIC-1001 .....	30-1
	MFIC-1002 .....	30-1
	MFIC-1003 .....	30-2
<b>Chapter 31</b>	<b>MPTH Error Messages</b>	
	MPTH-1001 .....	31-1
	MPTH-1002 .....	31-1
	MPTH-1003 .....	31-1
<b>Chapter 32</b>	<b>MQ Error Messages</b>	
	MQ-1004 .....	32-1
<b>Chapter 33</b>	<b>MS Error Messages</b>	
	MS-1001 .....	33-1
	MS-1002 .....	33-1
	MS-1003 .....	33-2
	MS-1004 .....	33-2
	MS-1005 .....	33-3
	MS-1006 .....	33-3
	MS-1007 .....	33-4
	MS-1008 .....	33-4
	MS-1021 .....	33-4
<b>Chapter 34</b>	<b>NBFS Error Messages</b>	
	NBFS-1001 .....	34-1

NBFS-1002 .....	34-1
NBFS-1003 .....	34-2

**Chapter 35 NS Error Messages**

NS-1001 .....	35-1
NS-1002 .....	35-1
NS-1003 .....	35-2
NS-1004 .....	35-2

**Chapter 36 PDM Error Messages**

PDM-1001 .....	36-1
PDM-1002 .....	36-1
PDM-1003 .....	36-1
PDM-1004 .....	36-2
PDM-1005 .....	36-2
PDM-1006 .....	36-2
PDM-1007 .....	36-3
PDM-1008 .....	36-3
PDM-1009 .....	36-3
PDM-1010 .....	36-4
PDM-1011 .....	36-4
PDM-1012 .....	36-4
PDM-1013 .....	36-5
PDM-1014 .....	36-5
PDM-1017 .....	36-5
PDM-1019 .....	36-6
PDM-1020 .....	36-6
PDM-1021 .....	36-6

**Chapter 37 PDTR Error Messages**

PDTR-1001 .....	37-1
PDTR-1002 .....	37-1

<b>Chapter 38</b>	<b>PLAT Error Messages</b>	
	PLAT-1000 .....	38-1
<b>Chapter 39</b>	<b>PORT Error Messages</b>	
	PORT-1003 .....	39-1
	PORT-1004 .....	39-1
<b>Chapter 40</b>	<b>PS Error Messages</b>	
	PS-1000.....	40-1
	PS-1001.....	40-1
	PS-1002.....	40-1
	PS-1003.....	40-2
	PS-1004.....	40-2
	PS-1005.....	40-2
<b>Chapter 41</b>	<b>PSWP Error Messages</b>	
	PSWP-1001.....	41-1
	PSWP-1002.....	41-1
	PSWP-1003.....	41-2
	PSWP-1004.....	41-2
<b>Chapter 42</b>	<b>RCS Error Messages</b>	
	RCS-1001 .....	42-1
	RCS-1002 .....	42-1
	RCS-1003 .....	42-2
	RCS-1004 .....	42-2
	RCS-1005 .....	42-2
	RCS-1006 .....	42-3
<b>Chapter 43</b>	<b>RPCD Error Messages</b>	
	RPCD-1001.....	43-1
	RPCD-1002.....	43-1



RPCD-1003.....	43-1
RPCD-1004.....	43-2
RPCD-1005.....	43-2
RPCD-1006.....	43-2
RPCD-1007.....	43-3

**Chapter 44 RTWR Error Messages**

RTWR-1001 .....	44-1
RTWR-1002 .....	44-1

**Chapter 45 SCN Error Messages**

SCN-1001 .....	45-1
----------------	------

**Chapter 46 SEC Error Messages**

SEC-1001 .....	46-1
SEC-1002 .....	46-1
SEC-1003 .....	46-2
SEC-1005 .....	46-2
SEC-1006 .....	46-2
SEC-1007 .....	46-3
SEC-1008 .....	46-3
SEC-1009 .....	46-3
SEC-1016 .....	46-4
SEC-1022 .....	46-4
SEC-1024 .....	46-4
SEC-1025 .....	46-5
SEC-1026 .....	46-5
SEC-1028 .....	46-5
SEC-1029 .....	46-6
SEC-1030 .....	46-6
SEC-1031 .....	46-6
SEC-1032 .....	46-7

SEC-1033	46-7
SEC-1034	46-7
SEC-1035	46-8
SEC-1036	46-8
SEC-1037	46-8
SEC-1038	46-9
SEC-1040	46-9
SEC-1041	46-10
SEC-1042	46-10
SEC-1043	46-10
SEC-1044	46-11
SEC-1045	46-11
SEC-1046	46-11
SEC-1049	46-12
SEC-1050	46-12
SEC-1051	46-12
SEC-1052	46-13
SEC-1053	46-13
SEC-1054	46-13
SEC-1055	46-14
SEC-1056	46-14
SEC-1057	46-14
SEC-1059	46-15
SEC-1062	46-15
SEC-1063	46-15
SEC-1064	46-16
SEC-1065	46-16
SEC-1069	46-16
SEC-1071	46-17
SEC-1072	46-17
SEC-1073	46-17

SEC-1074	46-18
SEC-1075	46-18
SEC-1076	46-18
SEC-1077	46-19
SEC-1078	46-19
SEC-1079	46-19
SEC-1080	46-20
SEC-1081	46-20
SEC-1082	46-20
SEC-1083	46-21
SEC-1084	46-21
SEC-1085	46-21
SEC-1086	46-22
SEC-1088	46-22
SEC-1089	46-22
SEC-1090	46-23
SEC-1091	46-23
SEC-1092	46-23
SEC-1093	46-24
SEC-1094	46-24
SEC-1095	46-24
SEC-1096	46-25
SEC-1097	46-25
SEC-1098	46-25
SEC-1099	46-26
SEC-1100	46-26
SEC-1101	46-26
SEC-1102	46-27
SEC-1104	46-27
SEC-1105	46-27
SEC-1106	46-28

SEC-1107	46-28
SEC-1108	46-28
SEC-1110	46-29
SEC-1111	46-29
SEC-1112	46-30
SEC-1115	46-30
SEC-1116	46-30
SEC-1117	46-31
SEC-1118	46-31
SEC-1119	46-31
SEC-1121	46-32
SEC-1122	46-32
SEC-1123	46-32
SEC-1124	46-33
SEC-1126	46-33
SEC-1130	46-33
SEC-1135	46-34
SEC-1136	46-34
SEC-1137	46-34
SEC-1138	46-35
SEC-1139	46-35
SEC-1142	46-35
SEC-1145	46-36
SEC-1146	46-36
SEC-1153	46-37
SEC-1154	46-37
SEC-1155	46-37
SEC-1156	46-38
SEC-1157	46-38
SEC-1158	46-38
SEC-1159	46-39

SEC-1160 .....	46-39
SEC-1163 .....	46-39
SEC-1164 .....	46-40
SEC-1165 .....	46-40
SEC-1166 .....	46-40
SEC-1167 .....	46-41
SEC-1168 .....	46-41
SEC-1170 .....	46-41
SEC-1171 .....	46-42
SEC-1172 .....	46-42
SEC-1173 .....	46-42
SEC-1174 .....	46-43
SEC-1175 .....	46-43
SEC-1176 .....	46-43
SEC-1180 .....	46-44
SEC-1181 .....	46-44
SEC-1182 .....	46-44
SEC-1183 .....	46-45
SEC-1184 .....	46-45
SEC-1185 .....	46-45
SEC-1186 .....	46-46
SEC-1187 .....	46-46
SEC-1188 .....	46-46
SEC-1189 .....	46-47
SEC-1190 .....	46-47
SEC-1191 .....	46-47
SEC-1192 .....	46-48
SEC-1193 .....	46-48
SEC-1194 .....	46-48
SEC-1195 .....	46-49
SEC-1196 .....	46-49

SEC-1197	46-49
SEC-1198	46-50
SEC-1199	46-50
SEC-1200	46-50
SEC-1201	46-51
SEC-1202	46-51
SEC-1250	46-52
SEC-1251	46-52
SEC-1253	46-52
SEC-1300	46-53
SEC-1301	46-53
SEC-1302	46-53
SEC-1303	46-54
SEC-1304	46-54
SEC-1305	46-54
SEC-1306	46-55
SEC-1307	46-55
SEC-1308	46-55
SEC-3001	46-56
SEC-3002	46-56
SEC-3003	46-56
SEC-3004	46-57
SEC-3005	46-57
SEC-3006	46-58
SEC-3007	46-58
SEC-3008	46-58
SEC-3009	46-59
SEC-3010	46-59
SEC-3011	46-59
SEC-3012	46-60
SEC-3013	46-60

SEC-3014 .....	46-60
SEC-3015 .....	46-61
SEC-3016 .....	46-61
SEC-3017 .....	46-61

**Chapter 47 SNMP Error Messages**

SNMP-1001 .....	47-1
SNMP-1002 .....	47-1
SNMP-1003 .....	47-1
SNMP-1004 .....	47-2

**Chapter 48 SS Error Messages**

SS-1000.....	48-1
SS-1001.....	48-1

**Chapter 49 SULB Error Messages**

SULB-1001.....	49-1
SULB-1002.....	49-1
SULB-1003.....	49-1
SULB-1005.....	49-2
SULB-1006.....	49-2
SULB-1007.....	49-2
SULB-1008.....	49-3
SULB-1009.....	49-3
SULB-1010.....	49-8

**Chapter 50 SWCH Error Messages**

SWCH-1001 .....	50-1
SWCH-1002 .....	50-1
SWCH-1003 .....	50-2
SWCH-1004 .....	50-2
SWCH-1005 .....	50-2

## **Chapter 51 SYSC Error Messages**

SYSC-1001 .....	51-1
SYSC-1002 .....	51-1

## **Chapter 52 SYSM Error Messages**

SYSM-1001 .....	52-1
SYSM-1002 .....	52-1
SYSM-1003 .....	52-1
SYSM-1004 .....	52-2

## **Chapter 53 TRCE Error Messages**

TRCE-1001 .....	53-1
TRCE-1002 .....	53-1
TRCE-1003 .....	53-2
TRCE-1004 .....	53-2
TRCE-1005 .....	53-2
TRCE-1006 .....	53-3
TRCE-1007 .....	53-3
TRCE-1008 .....	53-3
TRCE-1009 .....	53-4
TRCE-1010 .....	53-4
TRCE-1011 .....	53-4

## **Chapter 54 TRCK Error Messages**

TRCK-1001 .....	54-1
TRCK-1002 .....	54-1
TRCK-1003 .....	54-1
TRCK-1004 .....	54-2
TRCK-1005 .....	54-2
TRCK-1006 .....	54-2



<b>Chapter 55</b>	<b>TS Error Messages</b>	
	TS-1001 .....	55-1
	TS-1002 .....	55-1
	TS-1006 .....	55-2
<b>Chapter 56</b>	<b>UCST Error Messages</b>	
	UCST-1003 .....	56-1
	UCST-1007 .....	56-1
<b>Chapter 57</b>	<b>UPTH Error Messages</b>	
	UPTH-1001 .....	57-1
<b>Chapter 58</b>	<b>USWD Error Messages</b>	
	USWD-1006 .....	58-1
<b>Chapter 59</b>	<b>WEBD Error Messages</b>	
	WEBD-1001 .....	59-1
	WEBD-1002 .....	59-1
	WEBD-1003 .....	59-1
	WEBD-1004 .....	59-2
	WEBD-1005 .....	59-2
	WEBD-1006 .....	59-2
	WEBD-1007 .....	59-3
<b>Chapter 60</b>	<b>ZOLB Error Messages</b>	
	ZOLB-1001 .....	60-1
<b>Chapter 61</b>	<b>ZONE Error Messages</b>	
	ZONE-1002 .....	61-1
	ZONE-1003 .....	61-1
	ZONE-1004 .....	61-2
	ZONE-1005 .....	61-2

ZONE-1006 .....	61-3
ZONE-1007 .....	61-3
ZONE-1008 .....	61-3
ZONE-1010 .....	61-4
ZONE-1012 .....	61-4
ZONE-1013 .....	61-4
ZONE-1014 .....	61-5
ZONE-1015 .....	61-5
ZONE-1017 .....	61-5
ZONE-1018 .....	61-6
ZONE-1019 .....	61-6
ZONE-1022 .....	61-7
ZONE-1023 .....	61-7
ZONE-1024 .....	61-7
ZONE-1026 .....	61-8
ZONE-1027 .....	61-8
ZONE-1028 .....	61-8
ZONE-1029 .....	61-9
ZONE-1030 .....	61-9

## **Glossary**

## **Index**

# About This Document

---

This document is a reference guide written to help system administrators read and troubleshoot the system message logs to fix problems with the switch. There are several logs in the Fabric OS, including system messages, port logs, panic dump files, core files, and trace dumps. This book focuses on system messages: that is, the messages viewed using the **errShow** or **errDump** commands.

“About This Document” contains the following sections:

- [“How This Document Is Organized,”](#) next
- [“Supported Hardware and Software”](#) on page xxxvi
- [“What’s New in This Document”](#) on page xxxvi
- [“Document Conventions”](#) on page xxxvii
- [“Additional Information”](#) on page xxxviii
- [“Getting Technical Help”](#) on page xl
- [“Document Feedback”](#) on page xl

## How This Document Is Organized

This document is organized to help you find the particular information that you want as quickly and easily as possible. As a message reference, this document begins with a brief overview of messages and how they are stored on the system. It then provides details of each message, listed alphabetically.

The document contains the following components:

- [Chapter 1, “Introduction to System Messages,”](#) provides basic information on system messages.
- Chapters 2 through 61 provide message syntax, probable cause, recommended actions, and severity for the **errShow** and **errDump** messages.
- The glossary defines both terms specific to Brocade technology and common industry terms with uses specific to Brocade technology.
- The index points you to the exact pages on which specific information is located.

# Supported Hardware and Software

This document is specific to the Fabric OS version 4.4.0 and all switches running Fabric OS version 4.4.0, including:

- Brocade SilkWorm 3016 switch
- Brocade SilkWorm 3250 switch
- Brocade SilkWorm 3850 switch
- Brocade SilkWorm 3900 switch
- Brocade SilkWorm 4100 switch
- Brocade SilkWorm 12000 director
- Brocade SilkWorm 24000 director

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for the Fabric OS v4.4.0 release, documenting all possible configurations and scenarios is beyond the scope of this document.

This document does not support all 4.x Fabric OS versions. This document is specific to the Fabric OS v4.4.0 release.

## What's New in This Document

The following changes have been made since this document was last released:

Information that was added:

- A new security audit flag has been added so that messages reporting sensitive security changes are flagged “AUDIT” in the error log and provide additional information about security changes.

Information that was modified:

- The titles of all messages have changed. Messages are now named by the Fabric OS module and number.
- The number of severity levels has changed. Previous versions of the Fabric OS (v4.3 and earlier) had six levels of severity, Panic through Debug. The Panic and Debug severity levels have been merged into the other message levels.
- As a result of the change in number of severity levels, many messages have new severity levels.
- The format of messages has changed.
- Within the message log, the message sequence numbering behavior has changed.

Information that was removed:

- DIAG messages are now Brocade internal use only.
- PANIC messages are now Brocade internal use only.

# Document Conventions

This section describes text formatting conventions, important notices formats, and special term uses.

## Text Formatting

The narrative-text formatting conventions that are used in this document are as follows:

<b>bold text</b>	Identifies command names Identifies GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

## Notes, Cautions, and Warnings

The following notices appear in this document.



---

### Note

A note provides a tip, emphasizes important information, or provides a reference to related information.

---



---

### Caution

A caution alerts you to potential damage to hardware, firmware, software, or data.

---



---

### Warning

A warning alerts you to potential danger to personnel.

---

## Special Term Uses

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at <http://www.snia.org/education/dictionary>.

## Additional Information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

## Brocade Resources

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.



---

### Note

Go to <http://www.brocade.com> and click **Brocade Connect** to register at no cost for a user ID and password.

---

### Fabric OS

- *Brocade Fabric OS Features Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Command Reference Manual*
- *Brocade Fabric OS MIB Reference Manual*

### Fabric OS Optional Features

- *Brocade Advanced Web Tools Administrator's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Secure Fabric OS QuickStart Guide*

### SilkWorm 24000

- *SilkWorm 24000 Hardware Reference Manual*
- *SilkWorm 24000 QuickStart Guide*

### SilkWorm 12000

- *SilkWorm 12000 Hardware Reference Manual*
- *SilkWorm 12000 QuickStart Guide*

### SilkWorm 4100

- *SilkWorm 4100 Hardware Reference Manual*
- *SilkWorm 4100 QuickStart Guide*

### **SilkWorm 3900**

- *SilkWorm 3900 Hardware Reference Manual*
- *SilkWorm 3900 QuickStart Guide*

### **SilkWorm 3250/3850**

- *SilkWorm 3250/3850 Hardware Reference Manual*
- *SilkWorm 3250/3850 QuickStart Guide*

### **SilkWorm 3016**

- *SilkWorm 3016 Hardware Reference Manual*
- *SilkWorm 3016 QuickStart Guide*
- *Brocade Enterprise and Entry SAN Switch Modules for IBM eServer BladeCenter Design, Deployment and Management Guide (DDM)*

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

*<http://www.amazon.com>*

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

*<http://www.brocade.com>*

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

## **Other Industry Resources**

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, as well as other applications:

*<http://www.t11.org>*

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

*<http://www.fibrechannel.org>*

# Getting Technical Help

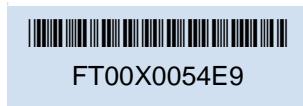
Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

## 1. General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- **supportSave** command output
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results

## 2. Switch Serial Number

The switch serial number and corresponding bar code are provided on the serial number label, as shown here:



The serial number label is located as follows:

- *SilkWorm 3016 switch*: Side of switch module.
- *SilkWorm 3200 and 3800 switches*: Back of chassis.
- *SilkWorm 3250, 3850, and 3900 switches*: Bottom of chassis.
- *SilkWorm 4100 switches*: On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side).
- *SilkWorm 12000 and 24000 directors*: Inside the front of the chassis, on the wall to the left of the ports.

## 3. World Wide Name (WWN)

- *SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and SilkWorm 12000 and 24000 directors*: Provide the license ID. Use the **licenseIDShow** command to display the license ID.
- *All other SilkWorm switches*: Provide the switch WWN. Use the **wwn** command to display the switch WWN.

# Document Feedback

Because quality is our first concern at Brocade, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to [documentation@brocade.com](mailto:documentation@brocade.com). Provide the title and version number and as much detail as possible about your issue, including the topic heading and page number and your suggestions for improvement.







# Introduction to System Messages

---

This guide supports Fabric OS v4.4.0 and contains system messages that you can use to diagnose and fix problems with the switch or fabric. The messages are organized alphabetically by module name. A *module* is a subsystem in the Fabric OS. Each module generates a set of numbered messages. For each message, this book provides message text, probable cause, recommended action, and severity level. There can be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

This chapter provides an introduction to the system messages. The following topics are discussed:

- [“Changes for This Release of the Fabric OS,”](#) next
- [“Message Severity Levels”](#) on page 1-2
- [“Overview of the System Messages”](#) on page 1-2
- [“View or Configure the System Message Logs”](#) on page 1-6
- [“Reading a System Message”](#) on page 1-8
- [“Responding to a System Message”](#) on page 1-11
- [“System Module Descriptions”](#) on page 1-12

## Changes for This Release of the Fabric OS

There are several major changes to error messages for this release of the Fabric OS. The changes are as follows:

- The titles of messages have changed. Previous versions of the Fabric OS (v4.2 and earlier) used the module name followed by an alpha description as the message name: for example, BLADE-FAULT. The new names for messages use the module name followed by a numeric identifier: for example, BL-1003. All messages appear in order, but not all message numbers are used.
- The number of severity levels has changed. Previous versions of the Fabric OS (v4.2 and earlier) had six levels of severity, Panic through Debug. The Panic and Debug severity levels have been merged with Critical and Info messages respectively. The current version of the Fabric OS (v4.4.0) has only four levels of severity:

- 1 = Critical
- 2 = Error
- 3 = Warning
- 4 = Info

For more information, refer to [“Message Severity Levels”](#) on page 1-2.

- As a result of the change in number of severity levels, many messages have new severity levels.

- A new security audit flag has been added so that messages reporting sensitive security changes are flagged “AUDIT” in the error log and provide more detailed information about what security commands were run, by which user, and whether the action was successful. For more information, refer to “[Security Audit Logging](#)” on page 1-3.
- The format of messages has changed. Previous versions of the Fabric OS used this format:
 

```
<severity>, <Module-alphaname>, <severity_number>, <message_text>
```

The current format of messages use this format:

```
<timestamp>, [Module-Number], <sequence-number>, <AUDIT>, <severity>, <switch-chassis-name>, <message-text>
```
- All messages are saved in persistent storage in this release. Previous releases normally saved only Panic and Critical levels persistently. All commands related to managing persistent storage are removed in this release.
- The sequence number of error messages within the error log has new behavior. Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.

## Message Severity Levels

There are four levels of severity for messages, ranging from Critical (1) to Info (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you should look at each specific error message description thoroughly before taking action. System messages have the following severity levels.

1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting online and offline status of a fabric port.

## Overview of the System Messages

This section provides information on the various logs saved by the system and how to view the information in the log files, including the following topics:

- [“System Message Log \(RASLog\),”](#) next
- [“Security Audit Logging”](#) on page 1-3
- [“Dual-CP Systems”](#) on page 1-4
- [“System Logging Daemon”](#) on page 1-4
- [“Port Logs”](#) on page 1-5
- [“Panic Dump and Core Dump Files”](#) on page 1-5
- [“Trace Dumps”](#) on page 1-5
- [“supportSave Command”](#) on page 1-6
- [“System Console”](#) on page 1-6

## System Message Log (RASLog)

The Fabric OS maintains an internal system message log of all messages. For Fabric OS v4.4.0, this log is saved as a RASLog. Features of the system message log include the following:

- The system message log by default saves all messages to nonvolatile storage.
- The system message log can save a maximum of 1024 messages in RAM.
- The system message log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are overwritten by new entries.
- By default, the **errDump** and **errShow** commands display all of the system messages.
- You should configure the syslogd facility as a management tool for error logs. This is particularly important for dual-domain switches, as the syslogd facility saves messages from two CPs as a single file and in sequential order. See [“System Logging Daemon”](#) on page 1-4 for more information.

## Security Audit Logging

Audit messages are enhanced to record more information, for security purposes. They are flagged AUDIT in the system message log. Currently, the only messages that have the audit flag set are SEC-3001 through SEC-3017.

They provide the following information:

- User Name: The name of the user who triggered the action.
- Role: The role of the user: for example, root or admin.
- Event Name: The name of the event that occurred.
- Status: The status of the event that occurred: success or failure.
- Event Info: Information about the event. If you are creating an SCC\_POLICY and use wildcards such as the asterisk (\*), meaning all the switches in the current fabric, these wildcards are displayed in the audit error message.

An example audit message is as follows:

```
2004/07/09-02:09:40, [SEC-3001], 181, AUDIT, INFO, User:rick, role: admin, Event:
secpolicy create, status:success, Info: Create SCC_POLICY policy, with * entries.
```

Only certain commands generate an AUDIT message in the system message log. The commands that generate AUDIT messages are as follows:

- **secModeEnable** and **secModeDisable**
- **secPolicyCreate**, **secPolicyDelete**, **secPolicyRemove**, **secPolicyActivate**, and **secPolicySave**
- **login** and **logout**
- **secFCSFailover**
- **secTransAbort**
- **secStatsReset**
- **secTempPasswdSet** and **secTempPasswdReset**
- **aaaConfig**
- **authUtil**

## Dual-CP Systems

For both the SilkWorm 12000 and the SilkWorm 24000, each CP has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging on the SilkWorm 12000 or the SilkWorm 24000, you should enable the system logging daemon because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For both the SilkWorm 12000 and the SilkWorm 24000, security violations such as telnet, HTTP, and serial connection violations are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

## System Logging Daemon

The system logging daemon (syslogd) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system.

The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogd functionality.

Configuring for syslogd involves configuring the host, enabling syslogd on the SilkWorm model, and, optionally, setting the facility level.

For information on configuring syslogd functionality, refer to the *Fabric OS Procedures Guide*.

## Port Logs

The Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Run the **portLogShow** command to display the port logs for a particular port.

Run the **portLogEventShow** command to display the specific events reported for each port.

Refer to the *Fabric OS Procedures Guide* for information on interpreting results of the **portLogDump** command.

Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

## Panic Dump and Core Dump Files

The Fabric OS creates panic dump files and core files when there are problems in the Fabric OS kernel. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the **saveCore** command. In case of a panic dump, the files can be viewed with the **pdShow** command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon.

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, then the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Run the **pdShow** command to view these files or the **saveCore** command to send them to a host workstation using FTP. The panic dump files and core files are intended for support personnel use only.

## Trace Dumps

The Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. You can initiate the sending of trace dump files to support personnel using the **supportSave** or **traceFtp** command. The Fabric OS trace dumps files are intended for support personnel use only.

## supportSave Command

The **supportSave** command can be used to send by FTP the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to a support location. Prior to running the **supportSave** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *Fabric OS Command Reference Manual* for more information on these commands.

## System Console

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

The **errFilterSet** command can be used by administrators to filter messages that appear on the system console by severity. All messages are still sent to the system message log and syslog (if enabled).

The system console displays both system messages and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

# View or Configure the System Message Logs

The following commands are used to view or configure the system message logs. Many of these commands require admin login privileges in order to execute.

**Table 1-1** Commands Used to View or Configure the System Logs

Command	Description
<b>agtCfgDefault</b>	Resets the SNMP recipients to default values.
<b>agtCfgSet</b>	Configures the SNMP recipients.
<b>agtCfgShow</b>	Displays the current configuration of the SNMP recipients.
<b>errClear</b>	Clears the error log.
<b>errDelimiterSet</b>	Sets the error log start and end delimiter for messages pushed to the console.
<b>errDump</b>	Displays the entire error log, without page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
<b>errFilterSet</b>	Sets an error severity filter for the system console.
<b>errShow</b>	Displays the entire error log, with page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
<b>pdShow</b>	Displays the contents of the panic dump and core dump files.
<b>portErrShow</b>	Displays the port error summary.
<b>portLogClear</b>	Clears the port log. (If the port log is disabled, this commands enables it.)
<b>portLogDisable</b>	Disables the port log facility.



**Table 1-1** Commands Used to View or Configure the System Logs (Continued)

<b>Command</b>	<b>Description</b>
<b>portLogDump</b>	Displays the port log, without page breaks.
<b>portLogDumpPort</b>	Displays the port log of the specified port, without page breaks.
<b>portLogEventShow</b>	Displays which port log events are currently being reported.
<b>portLoginShow</b>	Displays port logins.
<b>portLogPdisc</b>	Sets or clear the debug pdisc_flag.
<b>portLogReset</b>	Enables the port log facility.
<b>portLogResize</b>	Resizes the port log to the specified number of entries.
<b>portLogShow</b>	Displays the port log, with page breaks.
<b>portLogShowPort</b>	Displays the port log of a port, with page breaks for a specific port.
<b>portLogTypeDisable</b>	Disables an event from reporting to the port log. Port log events are described by the <b>portLogEventShow</b> command.
<b>portLogTypeEnable</b>	Enables an event to report to the port log. Port log events are described by the <b>portLogEventShow</b> command.
<b>saveCore</b>	Saves or removes core files created by the kernel.
<b>setVerbose</b>	Sets the verbose level of a particular module within the Fabric OS.
<b>supportFtp</b>	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
<b>supportSave</b>	Collects RASLog, trace files, and <b>supportShow</b> (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
<b>supportShow</b>	Executes a list of diagnostic and error display commands. This output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long.
<b>syslogDIpAdd</b>	Adds an IP address as a recipient of system messages.
<b>syslogDIpRemove</b>	Removes an IP address as a recipient of system messages.
<b>syslogDIpShow</b>	Views the currently configured IP addresses that are recipients of system messages.
<b>syslogdFacility</b>	Changes the syslogd facility.
<b>traceDump</b>	Displays, initiates, or removes a Fabric OS module trace dump.
<b>traceFtp</b>	Displays, enables, or disables the trace auto-FTP or retrieves the trace dump file.
<b>traceTrig</b>	Sets, removes, or displays trace triggers.

# Reading a System Message

This section provides information about reading system messages.

## Example System Message

The following example shows a sample message from the error log:

```
2004/07/22-10:12:33, [EM-1031], 4,, ERROR, switchname, Slot 7 ejector not closed
```

The fields in the error message are described in table below.

**Table 1-2** Error Message Field Description

Example	Variable Name	Description
2004/07/22-10:12:33	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the “LOCAL” setting.
[EM-1031]	Message Module and Message Number	Displays the message module and number. These values uniquely identify each message in the Fabric OS and are used to reference the cause and actions in this manual.
4	Sequence Number	<p>This represents the error message position in the log. When any messages are added to the log, this number is incremented. When this message reaches the last position in the error log, and becomes the oldest message in the log, it is deleted when a new message is added.</p> <p>In Fabric OS v4.4.0, the message sequence number starts at 1 after a <b>firmwareDownload</b> and will increase up to a value of 2,147,483,647 (0x7ffffff).</p> <p>The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the <b>errClear</b> command. The sequence number is persistent across power cycles and switch reboots.</p>

**Table 1-2** Error Message Field Description (Continued)

Example	Variable Name	Description
, <AUDIT> , (not shown in the above example)	Audit Flag	Indicates that this message is an AUDIT message for a security issue. The only messages that have the audit flag set are SEC-3001 through SEC-3017. For all other messages, this field is blank; however, the commas still appear, so many messages have two commas separated by a blank space.
ERROR	Severity Level	Displays the severity of the error in alpha format: 1 = Critical 2 = Error 3 = Warning 4 = Info
switchname	Switch name or chassis name, depending on the action; for example, HA messages typically show the chassis name and login failures show the logical switch name.	This field displays the defined switch name or the chassis name of the switch. This value is truncated if it is over 16 characters in length. Run either the <b>chassisName</b> command to name the chassis or the <b>switchName</b> command to rename the logical switch.
Slot 7 ejector not closed	Error Description	This field displays a text string explaining the error encountered and providing parameters supplied by the software at runtime.

## Viewing System Messages from Advanced Web Tools

This procedure is valid for the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000.

To view the system message log for a switch from Advanced Web Tools:

1. Launch Advanced Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the **Switch Events** button. A Switch Events Report appears.
4. View the switch events and messages. In dual-domain switches, an Event button exists for each logical switch. Only messages relating to that switch (and chassis) will be displayed.

## Dumping the System Messages

This procedure is valid for the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000.

To display the system message log, with no page breaks:

1. Log in to the switch as admin.
2. Enter the **errDump** command at the command line:

```
switch:admin> errDump
Version: 4.4.0
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media
incompatible. Reason: Configured port speed.

2004/07/28-17:04:54, [FABR-1001], 4,, WARNING, switch, port 4, ELP rejected by the
other switch

2004/07/28-17:05:06, [FW-1050], 5,, WARNING, switch, Sfp Supply Voltage 0, is below
low boundary(High=3600, Low=3150). Current value is 0 mV.

switch:admin>
```

## Viewing the System Messages with Page Breaks

This procedure is valid for the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000.

To display the system message log, with page breaks:

1. Log in to the switch as admin.
2. At the command line, enter the **errShow** command:

```
switch:admin> errShow
Version: 4.4.0
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media incompatibl
e. Reason: Configured port speed.

Type <CR> to continue, Q<CR> to stop:
```

## Clearing the System Message Log

This procedure is valid for the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000.

To clear the system message log for a particular switch instance:

1. Log in to the switch as admin.
2. Enter the **errClear** command to clear all messages from memory

The following example shows how to clear the system message log:

```
switch:admin> errclear  
switch:admin>
```

## Responding to a System Message

This section provides procedures on gathering information on system messages.

### Looking Up a System Message

Error messages are arranged in this manual alphabetically. To look up an error message, copy down the module (see [Table 1-3 on page 1-12](#)) and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

Information provided by this book is as follows:

- Module and code name for the error
- Message text
- Probable cause
- Recommended action
- Message severity

### Gathering Information About the Problem

Common steps and questions to ask yourself when troubleshooting a system message are as follows:

1. What is the current Fabric OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. Assess impact and urgency:
  - Is the switch down?
  - Is it a standalone switch?
  - How large is the fabric?
  - Is the fabric redundant?
5. Run the **errDump** command on each logical switch.
6. Run **supportFtp** (as needed) to set up automatic FTP transfers, and then run the **supportSave** command.

7. Document the sequence of events by answering the following questions:
  - What happened just prior to the problem?
  - Is the problem repeatable?
  - If so, what are the steps to produce the problem?
  - What configuration was in place when the problem occurred?
8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP was master? (only applicable to the SilkWorm 12000 or 24000)
13. What and when were the last actions or changes made to the system?

## System Module Descriptions

[Table 1-3](#) provides a summary of the system modules for which messages are documented in this reference guide; the system modules are listed alphabetically by name.

**Table 1-3** System Module Descriptions

System Module	Description
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BL	Blade error messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between a blade and the EM (environment monitor) module.
BLL	Bloom is the name of the ASIC used as the building block for third-generation hardware platforms.
CER	This is the core edge routing module on the SilkWorm 24000 platform.
EM	The environmental monitor (EM) manages and monitors the various FRUs (field replaceable units), including the port cards, CP blades, blower assemblies, power supplies, and WWN (World Wide Name) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery.  EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by way of telnet commands, system LEDs, and status and alarm messages. EM also manages some component-related data.
EVMD	This is the event management module.

**Table 1-3** System Module Descriptions (Continued)

System Module	Description
FABR	FABRIC refers to a network of Fibre Channel switches. The FABRIC error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FICU	The FICON-CUP daemon handles communication with FICON on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core PID, and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOOD is a part of the FSPF (fabric shortest path first) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSR).
FSPF	Fabric shortest path first (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.
FSS	<p>The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation.</p> <p>FSS is defined both as a component and a service. A <i>component</i> is a module in the Fabric OS, implementing a related set of functionality. A <i>service</i> is a collection of components grouped together to achieve a modular software architecture.</p>
FSSM	The Fabric OS state synchronization management module is defined both as a component and a service. A component is a module in Fabric OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.
FW	FW is the Fabric Watch module. This module monitors thresholds for many switch subsystems: for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.

**Table 1-3** System Module Descriptions (Continued)

System Module	Description
HAM	HAM is a user space daemon responsible for high availability management.
HAMK	This is the kernel module for the HAM daemon.
HIL	Hardware independent layer.
HLO	HLO is a part of FSPF protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HTTP	HTTP error message.
KSWD	<p>The kernel software watchdog (KSWD) watches daemons for unexpected terminations and “hang” conditions and informs the HAM module to take corrective actions such as failover or reboot.</p> <p>The following daemons are monitored by KSWD:</p> <ul style="list-style-type: none"> <li>• Diagnostics daemon (DIAGD)</li> <li>• Environment monitor daemon (EMD)</li> <li>• EVM daemon (EVM D)</li> <li>• Fabric daemon (FABRICD)</li> <li>• FCPD daemon (FCPD)</li> <li>• FDMI daemon (FDMID)</li> <li>• FICON-CUP daemon (FICUD)</li> <li>• FSPF daemon (FSPFD)</li> <li>• Fabric watch daemon (FWD)</li> <li>• Management Server daemon (MSD)</li> <li>• Name Server daemon (NSD)</li> <li>• PDM daemon (PDMD)</li> <li>• PS daemon (PSD)</li> <li>• Reliable commit service daemon (RCSD)</li> <li>• FA-API RPC daemon (RPCD)</li> <li>• Security daemon (SECD)</li> <li>• SNMP daemon (SNMPD)</li> <li>• Track changes daemon (TRACK_CHANGES)</li> <li>• Time Service daemon (TSD)</li> <li>• Web Tools daemon (WEBD)</li> <li>• Zone daemon (ZONED)</li> </ul>
KTRC	Kernel RAS trace module.
LOG	RASLog subsystem.



**Table 1-3** System Module Descriptions (Continued)

System Module	Description
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MFIC	MS-FICON messages relate to FICON installations. FICON-CUP messages are displayed under the FICU module.
MPTH	Multicast path uses the shortest path first (SPF) algorithm to dynamically compute a broadcast tree.
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas:  <b>Fabric Configuration Server.</b> Provides for the configuration management of the fabric.  <b>Unzoned Name Server.</b> Provides access to Name Server information that is not subject to zone constraints.  <b>Fabric Zone Server.</b> Provides access to and control of zone information.
NBFSM	NBFSM is a part of the FSPF (fabric shortest path first) protocol that handles a neighboring or adjacent switch's finite state machine (FSM).  Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an ISL (interswitch link) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on.  NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the Simple Name Server module.
PDM	Parity data manager is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	These messages indicate panic dump trace files have been created.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users, to connect end devices or connect to other switches.
PS	The performance server daemon measures the amount of traffic between end points or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.

Table 1-3 System Module Descriptions (Continued)

System Module	Description
RCS	The reliable commit service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests RTWR (reliable transport write and read) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RPCD	The remote procedure call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS.
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SS	The <b>supportSave</b> command generates these error messages if problems are encountered.
SULB	The software upgrade library provides <b>firmwareDownload</b> command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all 4.x switches. These messages might display if there are any problems during the <b>firmwareDownload</b> procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the <i>Fabric OS Procedures Guide</i> .
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TRCE	RAS TRACE error messages.

**Table 1-3** System Module Descriptions (Continued)

System Module	Description
TRCK	<p>The track change feature tracks the following events:</p> <ul style="list-style-type: none"> <li>• Turning on or off the track change feature</li> <li>• CONFIG_CHANGE</li> <li>• LOGIN</li> <li>• LOGOUT</li> <li>• FAILED_LOGIN</li> </ul> <p>If any of these events occurs, a message is sent to the system message log. Additionally, if the SNMP trap option is enabled, an SNMP trap is also sent.</p> <p>For information on configuring the track change feature, refer to the <i>Fabric OS Command Reference Manual</i> or the <i>Fabric OS Procedures Guide</i>.</p>
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCST	UCAST is a part of the fabric shortest path first (FSPF) protocol that manages the Unicast routing table.
UPATH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.
USWD	The user-space software watchdog daemon informs the KSWD about which daemons the watchdog subsystem will monitor. Additionally, the USWD daemon helps the KSWD daemon to print debug information if a critical daemon has an unexpected termination.
WEBD	Indicates problems with the Web Tools module.
ZOLB	Indicates problems with the zone library module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.



# AUTH Error Messages

---

## AUTH-1001

### Message

```
<timestamp>, [AUTH-1001], <sequence-number>,, INFO, <system-name>,  
<Operation type> has been successfully done.
```

### Probable Cause

Indicates that the secret database operation has been updated using the **secAuthSecret** command. The values for *Operation type* can be “set” or “remove”.

### Recommended Action

No action is required.

### Severity

INFO

## AUTH-1002

### Message

```
<timestamp>, [AUTH-1002], <sequence-number>,, ERROR, <system-name>,  
<Operation type> has failed.
```

### Probable Cause

Indicates that the specified action has failed to update the secret database using the **secAuthSecret** command. The values for *Operation type* can be “set” or “remove”.

### Recommended Action

Retry the **secAuthSecret** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1003

### Message

```
<timestamp>, [AUTH-1003], <sequence-number>,, INFO, <system-name>,  
<data type> type has been successfully set to <setting value>.
```

**Probable Cause** Indicates an authentication configuration value was set to a specified value. The data type is either authentication type or DH group type.

**Recommended Action** No action is required.

**Severity** INFO

## AUTH-1004

### Message

```
<timestamp>, [AUTH-1004], <sequence-number>,, ERROR, <system-name>,
Failed to set <data type> type to <setting value>.
```

**Probable Cause** Indicates that the **authUtil** command has failed to set the authentication configuration value. The data type can be either authentication type or DH group type.

**Recommended Action** Retry the **authUtil** command.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1005

### Message

```
<timestamp>, [AUTH-1005], <sequence-number>,, ERROR, <system-name>,
Authentication file does not exist: <error code>.
```

**Probable Cause** Indicates an authentication file corruption.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1006

### Message

```
<timestamp>, [AUTH-1006], <sequence-number>,, WARNING, <system-
name>, Failed to open authentication configuration file.
```

**Probable Cause** Indicates an internal problem with the Secure Fabric OS.

**Recommended Action** Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## AUTH-1007

### Message

```
<timestamp>, [AUTH-1007], <sequence-number>,, ERROR, <system-name>,
The proposed authentication protocol(s) are not supported: port
<port number>.
```

**Probable Cause** Indicates that the proposed authentication protocol type or types are not supported by the local port.

**Recommended Action** Run the **authUtil** command to make sure the local switch supports the specified protocols: FCAP or DH-CHAP.

**Severity** ERROR

## AUTH-1008

### Message

```
<timestamp>, [AUTH-1008], <sequence-number>,, ERROR, <system-name>,
No security license, operation failed.
```

**Probable Cause** Indicates that the switch does not have a security license.

**Recommended Action** Verify that the security license is installed using the **licenseShow** command. If necessary, reinstall the license using the **licenseAdd** command.

**Severity** ERROR

## AUTH-1010

### Message

```
<timestamp>, [AUTH-1010], <sequence-number>,, ERROR, <system-name>,
Failed to initialize security policy: switch <switch number>, error
<error code>.
```

**Probable Cause** Indicates an internal problem with the Secure Fabric OS.

**Recommended Action** Reboot or power cycle the switch.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1011

### Message

```
<timestamp>, [AUTH-1011], <sequence-number>,, WARNING, <system-name>, Failed to register for failover operation: switch <switch number> error <error code>
```

**Probable Cause** Indicates an internal problem with the Secure Fabric OS.

**Recommended Action** Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## AUTH-1012

### Message

```
<timestamp>, [AUTH-1012], <sequence-number>,, WARNING, <system-name>, Authentication <code> is rejected: port <port number> explain <explain code> reason <reason code>
```

**Probable Cause** Indicates that an authentication is rejected because the remote entity does not support authentication.

**Recommended Action** Make sure the entity at the other end of the link supports authentication.

**Severity** WARNING



## AUTH-1013

### Message

```
<timestamp>, [AUTH-1013], <sequence-number>,, WARNING, <system-name>, Can not perform authentication request message: port <port number>, message code <message code>
```

### Probable Cause

Indicates that the system is running low on resources when receiving an authentication request.

### Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## AUTH-1014

### Message

```
<timestamp>, [AUTH-1014], <sequence-number>,, ERROR, <system-name>, Invalid port value to <operation>: port <port number>
```

### Probable Cause

Indicates an internal problem with the Secure Fabric OS.

### Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1017

### Message

```
<timestamp>, [AUTH-1017], <sequence-number>,, ERROR, <system-name>, Invalid value to start authentication request: port <port number>, opcode <operation code>
```

### Probable Cause

Indicates an internal problem with the Secure Fabric OS.

**Recommended Action** Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1018

### Message

```
<timestamp>, [AUTH-1018], <sequence-number>,, ERROR, <system-name>,
Invalid value to check protocol type: port <port number>
```

**Probable Cause** Indicates an internal problem with the Secure Fabric OS.

**Recommended Action** Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1020

### Message

```
<timestamp>, [AUTH-1020], <sequence-number>,, INFO, <system-name>,
Failed to create timer for authentication: port <port number>
```

**Probable Cause** Indicates that an authentication message's timer was not created.

**Recommended Action** Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** INFO

## AUTH-1022

### Message

```
<timestamp>, [AUTH-1022], <sequence-number>,, ERROR, <system-name>,
Failed to extract <data type> from <message> payload: port <port
number>.
```

### Probable Cause

Indicates the authentication process failed to extract a particular value from the receiving payload.

### Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1023

### Message

```
<timestamp>, [AUTH-1023], <sequence-number>,, ERROR, <system-name>,
Failed to <operation type> during <authentication phase>: port
<port number>.
```

### Probable Cause

Indicates an authentication operation failed for a certain authentication phase.

*Operation type* varies depending on authentication type:

- Some operations for SLAP: certificate retrieve, certificate verification signature verification, or nonce signing.
- Some operations for FCAP: certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for DH-CHAP: response calculation, challenge generation, or secret retrieve.

The *authentication phase* specifies which phase of a particular authentication protocol failed.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

### Recommended Action

The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for possible unauthorized access attack.

It might indicate that the PKI object for SLAP or FCAP or secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1025

### Message

```
<timestamp>, [AUTH-1025], <sequence-number>,, ERROR, <system-name>,
Failed to get <data type> during <authentication phase>: port <port
number>
```

### Probable Cause

Indicates the authentication process failed to get expected information during the specified authentication phase.

### Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1027

### Message

```
<timestamp>, [AUTH-1027], <sequence-number>,, ERROR, <system-name>,
Failed to select <authentication value> during <authentication
phase>: value <value> port <port number>.
```

### Probable Cause

Indicates that the authentication process failed to select an authentication value (that is, DH Group, hash value, or protocol type) from a receiving payload for a particular authentication phase. This indicates that the local switch does not support the specified authentication value.

### Recommended Action

Check the authentication configuration and reset the supported value if needed using the **authUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1028

### Message

```
<timestamp>, [AUTH-1028], <sequence-number>,, ERROR, <system-name>,
Failed to allocate <data type> for <operation phase>: port <port
number>
```

**Probable Cause** Indicates that the authentication process failed because the system is low on memory.  
*Data type* is the payload or structure that failed to get memory.  
*Operation phase* specifies which operation of a particular authentication phase failed.

**Recommended Action** Usually this problem is transient. The authentication might fail.  
 Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.  
 If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1029

### Message

```
<timestamp>, [AUTH-1029], <sequence-number>,, ERROR, <system-name>,
Failed to get <data type> for <message phase> message: port <port
number>, retval <error code>
```

**Probable Cause** Indicates that the authentication process failed to get a particular authentication value at certain phase.  
*Data type* is the payload or structure that failed to get memory.

**Recommended Action** Usually this problem is transient. The authentication might fail.  
 Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.  
 If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1030

### Message

```
<timestamp>, [AUTH-1030], <sequence-number>,, ERROR, <system-name>,
Invalid message code for <message phase> message: port <port
number>
```

**Probable Cause** Indicates the receiving payload does not have valid message code for a particular authentication phase.

**Recommended Action** Usually this problem is transient. The authentication might fail.  
 Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1031

### Message

```
<timestamp>, [AUTH-1031], <sequence-number>, , ERROR, <system-name>,
Failed to retrieve secret value: port <port number>
```

**Probable Cause** Indicates that the secret value was not set properly for the authenticated entity.

**Recommended Action** Reset the secret value by using **secAuthSecret** command.  
Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

**Severity** ERROR

## AUTH-1032

### Message

```
<timestamp>, [AUTH-1032], <sequence-number>, , ERROR, <system-name>,
Failed to generate <data type> for <message payload> payload:
length <data length>, error code <error code>, port <port number>
```

**Probable Cause** Indicates that the authentication process failed to generate a particular data (that is, challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure. A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

**Recommended Action** Usually this problem is transient. The authentication might fail.  
Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1033

### Message

```
<timestamp>, [AUTH-1033], <sequence-number>,, ERROR, <system-name>,
Disable port <port number> due to unauthorized switch <switch WWN
value>
```

### Probable Cause

Indicates that an entity was not configured in the SCC policy and tried to connect to the port.

### Recommended Action

Add the entity's WWN to the SCC policy and reinitialize authentication by using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

### Severity

ERROR

## AUTH-1034

### Message

```
<timestamp>, [AUTH-1034], <sequence-number>,, ERROR, <system-name>,
Failed to validate name <entity name> in <authentication message>:
port <port number>
```

### Probable Cause

Indicates that the entity name in the payload is not in the right format.

### Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## AUTH-1035

### Message

```
<timestamp>, [AUTH-1035], <sequence-number>,, ERROR, <system-name>,
Invalid <data type> length in <message phase> message: length <data
length>, port <port number>
```

### Probable Cause

Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to internal failure.

### Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1036

### Message

```
<timestamp>, [AUTH-1036], <sequence-number>,, ERROR, <system-name>,
Invalid state <state value> for <authentication phase>: port <port
number>
```

**Probable Cause** Indicates that the switch received an unexpected authentication message.

**Recommended Action** Usually this problem is transient. The authentication might fail.  
Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## AUTH-1037

### Message

```
<timestamp>, [AUTH-1037], <sequence-number>,, ERROR, <system-name>,
Failed to <operation type> response for <authentication message>:
init_len <data length>, resp_len <data length>, port <port number>.
```

**Probable Cause** Indicates that a DH-CHAP authentication operation failed on the specified port due to mismatched response values between two entities.

**Recommended Action** The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR



## AUTH-1038

### Message

```
<timestamp>, [AUTH-1038], <sequence-number>, , ERROR, <system-name>,  
Failed to retrieve certificate during <authentication phase>: port  
<port number>
```

### Probable Cause

Indicates that the PKI certificate is not installed properly.

### Recommended Action

Reinstall the PKI certificate, using the **pkiCreate** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR



# BL Error Messages

---

## BL-1000

**Message**

```
<timestamp>, [BL-1000], <sequence-number>,, INFO, <system-name>,  
Initializing Ports...
```

**Probable Cause**

Indicates that the switch has started initializing the ports. This message occurs only on the SilkWorm 4100.

**Recommended Action**

No action is required.

**Severity**

INFO

## BL-1001

**Message**

```
<timestamp>, [BL-1001], <sequence-number>,, INFO, <system-name>,  
Port Initialization Completed
```

**Probable Cause**

Indicates that the switch has completed initializing the ports. This message occurs only on the SilkWorm 4100.

**Recommended Action**

No action is required.

**Severity**

INFO

## BL-1002

**Message**

```
<timestamp>, [BL-1002], <sequence-number>,, CRITICAL, <system-  
name>, Init Failed: DISABLED because internal ports were not  
ONLINE, Slot: <slot number>
```

**Probable Cause** Indicates that the blade initiation failed because one or more of the internal ports was not online. The blade is faulted. This message occurs on only the SilkWorm 12000 and 24000.

**Recommended Action** Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Additional blade fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the blade.

**Severity** CRITICAL

## BL-1003

### Message

```
<timestamp>, [BL-1003], <sequence-number>,, CRITICAL, <system-name>, Faulting blade in slot <slot number>
```

**Probable Cause** Indicates a faulty blade in the specified slot number. This message occurs on only the SilkWorm 12000 and 24000.

**Recommended Action** Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

**Severity** CRITICAL

## BL-1004

### Message

```
<timestamp>, [BL-1004], <sequence-number>,, CRITICAL, <system-name>, Suppressing blade fault in slot <slot number>
```

**Probable Cause** Indicates that the specified blade experienced a failure but was not faulted due to a user setting. This message occurs on only the SilkWorm 12000 and 24000.

**Recommended Action** Reboot or power cycle the blade, using the **slotPowerOff** and **slotPowerOn** commands.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

**Severity** CRITICAL

## BL-1006

### Message

```
<timestamp>, [BL-1006], <sequence-number>,, INFO, <system-name>,
Blade <slot number> NOT faulted. Peer blade <slot number>
experienced abrupt failure.
```

### Probable Cause

Indicates that the errors (mostly synchronization errors) on this blade are harmless. Probably, the standby CP blade connected to the active CP blade has experienced transitory problems. This message occurs on only the SilkWorm 12000 and 24000.

### Recommended Action

Check the standby CP. No action is required if the other blade is already removed or faulted.

### Severity

INFO

## BL-1007

### Message

```
<timestamp>, [BL-1007], <sequence-number>,, WARNING, <system-name>,
blade #<blade number>: blade state is inconsistent with EM.
bl_cflags 0x<blade control flags>, slot_on <slot_on flag>, slot_off
<slot_off flag>, faulty <faulty flag>, status <blade status>
```

### Probable Cause

Indicates that a failover occurred while a blade was initializing on the previously active CP. This message occurs on only the SilkWorm 12000 and 24000.

### Recommended Action

No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

### Severity

WARNING

## BL-1008

### Message

```
<timestamp>, [BL-1008], <sequence-number>,, CRITICAL, <system-
name>, Slot <slot number> control-plane failure. Expected value:
0x<value 1>, Actual: 0x<value 2>
```

### Probable Cause

Possibly the blade has experienced a hardware failure or was removed without following the recommended removal procedure. This message occurs on only the SilkWorm 12000 and 24000.

### Recommended Action

Make sure that the blade is seated correctly.  
If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

**Severity** CRITICAL

## BL-1009

### Message

```
<timestamp>, [BL-1009], <sequence-number>,, CRITICAL, <system-name>, Blade in slot <slot number> timed out initializing the chips.
```

**Probable Cause** Indicates that the blade has failed to initialize the ASIC chips. This message occurs on only the SilkWorm 12000 and 24000.

### Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

**Severity** CRITICAL

## BL-1010

### Message

```
<timestamp>, [BL-1010], <sequence-number>,, WARNING, <system-name>, Blade in slot <slot number> inconsistent with the hardware settings.
```

**Probable Cause** Indicates that a failover occurred while some hardware changes were being made on the previously active CP (such as changing the domain ID). This message occurs on only the SilkWorm 12000 and 24000.

### Recommended Action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

**Severity** WARNING

## BL-1011

### Message

```
<timestamp>, [BL-1011], <sequence-number>,, CRITICAL, <system-name>, Busy with emb-port int. for chip <chip number> in minis <minis number> on blade <slot number>, chip int. is disabled. interrupt status=0x<interrupt status>
```

### Probable Cause

Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the CP from becoming too busy.

### Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

Run the **systemVerification** command to verify that the blade or switch does not have hardware problems.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

### Severity

CRITICAL

## BL-1012

### Message

```
<timestamp>, [BL-1012], <sequence-number>,, INFO, <system-name>, bport <port number> port int. is disabled. status=0x<interrupt status> Port <port number> will be re-enabled in 1 minute.
```

### Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

### Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

### Severity

INFO

## BL-1013

### Message

```
<timestamp>, [BL-1013], <sequence-number>,, INFO, <system-name>,
bport <port number> port is faulted. status=0x<interrupt status>
Port <port number> will be re-enabled in 1 minute.
```

### Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

### Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

### Severity

INFO

## BL-1014

### Message

```
<timestamp>, [BL-1014], <sequence-number>,, INFO, <system-name>,
bport <port number> port int. is disabled. status=0x<interrupt
status>
```

### Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

### Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the SilkWorm 12000 or 24000, replace the blade FRU.
- On the SilkWorm 3900, replace the motherboard FRU.
- On the SilkWorm 3016, 3250, 3850, or 4100, replace the switch.

### Severity

INFO



## BL-1015

### Message

```
<timestamp>, [BL-1015], <sequence-number>,, INFO, <system-name>,
bport <port number> port is faulted. status=0x<interrupt status>
```

### Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

### Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the SilkWorm 12000 or 24000, replace the blade FRU.
- On the SilkWorm 3900, replace the motherboard FRU.
- On the SilkWorm 3016, 3250, 3850, or 4100, replace the switch.

### Severity

INFO

## BL-1016

### Message

```
<timestamp>, [BL-1016], <sequence-number>,, CRITICAL, <system-
name>, Blade port <port number> in slot <slot number> failed to
enable.
```

### Probable Cause

Indicates that the specified blade port has failed to get enabled.

### Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

### Severity

CRITICAL



# BLL Error Messages

---

## BLL-1000

### Message

```
<timestamp>, [BLL-1000], <sequence-number>,, CRITICAL, <system-name>, ASIC driver detected Slot <slot number> port <port number> as faulty (reason: <reason>)
```

### Probable Cause

Indicates that a blade regulation problem was reported on the specified *slot number*. The blade is faulted. All blade register fault codes are associated with BLOOM error messages. This message is always paired with a BLOOM message that provides more information on the specific error. This message occurs on only the SilkWorm 12000 and 24000.

The reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E\_Port
- 7 = Excessive RCC VC on FL\_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = CMI interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error

- 21 = RAM parity error
- 22 = BISR or RAMINIT error

**Recommended  
Action**

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the blade.

**Severity**

CRITICAL

# CER Error Messages

---

## CER-1001

### Message

```
<timestamp>, [CER-1001], <sequence-number>,, ERROR, <system-name>,  
HA Sync broken, since standby Advanced Performance Tuning module  
does not support FICON Management Server (FMS).
```

### Probable Cause

Indicates that the HA synchronization between the active and standby CPs is broken because there is downlevel firmware loaded on the standby CP. The standby CP does not support the Advanced Performance Tuning module when FICON Management Server is enabled.

### Recommended Action

Run the **firmwareDownload** command to upgrade the firmware on the standby CP.  
You can also disable FMS on the active CP.

**Severity** ERROR



# EM Error Messages

---

## EM-1001

### Message

```
<timestamp>, [EM-1001], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> is over heating: Shutting down
```

### Probable Cause

Indicates that a field replaceable unit (FRU) is shutting down due to overheating. This is typically due to a faulty fan but can also be caused by the switch environment.

### Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced. Healthy fan speeds are as follows:

- SilkWorm 24000 fans run at approximately 2500 RPM.
- SilkWorm 12000 fans run at approximately 2500 RPM.
- SilkWorm 4100 fans run at approximately 6000 RPM.
- SilkWorm 3900 fans run at approximately 3500 RPM.
- SilkWorm 3850 fans run at approximately 9000 RPM.
- SilkWorm 3250 fans run at approximately 5500 RPM.
- SilkWorm 3016 has no fans.

The SilkWorm 3250 has three fans, and the SilkWorm 3850 has four fans. Values for the individual fans might display in this message, but these parts cannot be replaced: the entire switch is a FRU.

**Severity** CRITICAL

## EM-1002

### Message

```
<timestamp>, [EM-1002], <sequence-number>,, CRITICAL, <system-name>, System fan(s) status <fan fru>
```

### Probable Cause

Indicates that a nonbladed system has overheated and is going to shut down. Before doing so, all fan speeds are dumped to the console.

<b>Recommended Action</b>	<p>Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.</p> <p>Run the <b>fanShow</b> command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced. Healthy fan speeds are as follows:</p> <ul style="list-style-type: none"> <li>• SilkWorm 24000 fans run at approximately 2500 RPM.</li> <li>• SilkWorm 12000 fans run at approximately 2500 RPM.</li> <li>• SilkWorm 4100 fans run at approximately 6000 RPM.</li> <li>• SilkWorm 3900 fans run at approximately 3500 RPM.</li> <li>• SilkWorm 3850 fans run at approximately 9000 RPM.</li> <li>• SilkWorm 3250 fans run at approximately 5500 RPM.</li> <li>• SilkWorm 3016 has no fans.</li> </ul> <p>The SilkWorm 3250 has three fans, and the SilkWorm 3850 has four fans. Values for the individual fans might display in this message, but these parts cannot be replaced: the entire switch is a FRU.</p>
<b>Severity</b>	CRITICAL

## EM-1003

### Message

```
<timestamp>, [EM-1003], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> has unknown hardware identifier: FRU is being faulted.
```

### Probable Cause

Indicates that a fan FRU header could not be read or is not valid. The FRU is faulted.

### Recommended Action

On SilkWorm 12000 or SilkWorm 24000, try reseating the specified FRU.

Reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

On the SilkWorm 12000 and 24000, replace the specified FRU.

On the SilkWorm 3900 and 4100, replace the motherboard FRU.

On the SilkWorm 3016, 3250 and 3850, replace the whole switch as these switches do not have FRUs: the entire switch is a FRU.

**Severity** CRITICAL

## EM-1004

### Message

```
<timestamp>, [EM-1004], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> failed to power on
```



<b>Probable Cause</b>	<p>Indicates that a FRU failed to power on and is not being used. The type of FRU is specified in the message.</p> <p>The <i>FRU ID</i> value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The <i>FRU ID</i> value can be:</p> <ul style="list-style-type: none"> <li>• <i>Switch</i> for fixed port count switches.</li> <li>• <i>Slot 1</i> through <i>Slot 10</i> for the SilkWorm 12000 and 24000.</li> <li>• <i>PS 1</i> through <i>PS 4</i> (power supplies) for the SilkWorm 12000 and 24000, or <i>PS 1</i> through <i>PS 2</i> for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>Fan 1</i> through <i>Fan 3</i> for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). <i>Fan 1</i> through <i>Fan 6</i> for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>WWN 1</i> or <i>WWN 2</i> for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.</li> </ul> <p>The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.</p> <p>The SilkWorm 3016 does not have any fans, power supplies or WWN cards.</p>
-----------------------	---

**Recommended Action** Try reseating the FRU. If this fails to correct the error, replace the unit.

**Severity** CRITICAL

## EM-1005

### Message

```
<timestamp>, [EM-1005], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> is shutting down
```

**Probable Cause** Indicates that a blade in the specified slot or the switch (for nonbladed switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.

**Recommended Action** Check the environment and make sure the room temperature is within the operational range of the switch. Use the **fanShow** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

**Severity** CRITICAL

## EM-1006

### Message

```
<timestamp>, [EM-1006], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> has faulted. Sensor(s) below minimum limits
```

### Probable Cause

Indicates that the sensors show the voltage is below minimum limits. The blade in the specified slot is being shut down for environmental reasons; the voltage is too low.

### Recommended Action

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

### Severity

CRITICAL

## EM-1007

### Message

```
<timestamp>, [EM-1007], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> is being reset. Sensor(s) has exceeded max limits
```

### Probable Cause

Indicates that the voltage on a switch has exceeded environmental limits. A reset is sent to the faulty slot or the switch for nonbladed switches.

### Recommended Action

There is most likely a voltage hardware problem on the blade or motherboard of the switch.

For the SilkWorm 12000 and 24000, replace the blade FRU.

For the SilkWorm 3900, replace the motherboard FRU.

For the SilkWorm 3016, 3250, 3850, and 4100 you must replace the switch.

### Severity

CRITICAL

## EM-1008

### Message

```
<timestamp>, [EM-1008], <sequence-number>,, CRITICAL, <system-name>, Incompatible unit in <FRU Id> is being faulted
```

### Probable Cause

Indicates that a FRU inserted in the specified slot is not compatible with the switch software. The blade will not be used. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

### Recommended Action

Replace the blade. Make sure the replacement is compatible with your switch type.

### Severity

CRITICAL

## EM-1009

### Message

```
<timestamp>, [EM-1009], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> powered down unexpectedly
```

### Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified FRU. This might indicate a hardware malfunction in the FRU. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

### Recommended Action

Try reseating the blade. If this fails to correct the error, replace the FRU unit.

### Severity

CRITICAL

## EM-1010

### Message

```
<timestamp>, [EM-1010], <sequence-number>,, CRITICAL, <system-name>, Received unexpected power down for <FRU Id> But <FRU Id> still has power
```

### Probable Cause

Indicates that the environmental monitor received an unexpected power-down notification from the specified FRU. However, the specified FRU still appears to be powered up after four seconds. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

### Recommended Action

Try reseating the blade. If this fails to correct the error, replace the FRU unit.

### Severity

CRITICAL

## EM-1011

### Message

```
<timestamp>, [EM-1011], <sequence-number>,, CRITICAL, <system-name>, Can not determine if <FRU Id> has powered down
```

### Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the FRU specified; however, after four seconds it cannot be determined if it has powered down or not. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

### Recommended Action

Try reseating the blade. If this fails to correct the error, replace the unit.

### Severity

CRITICAL

## EM-1012

### Message

```
<timestamp>, [EM-1012], <sequence-number>,, CRITICAL, <system-name>, <FRU Id> failed <state> transition
```

### Probable Cause

Indicates that a switch blade failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.

### Recommended Action

On SilkWorm 12000 and SilkWorm 24000, try reseating the indicated FRU.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the FRU.

### Severity

CRITICAL

## EM-1013

### Message

```
<timestamp>, [EM-1013], <sequence-number>,, ERROR, <system-name>, Failed to update FRU information for <FRU Id>
```

<b>Probable Cause</b>	<p>Indicates that the environmental monitor was unable to update the time alive or OEM data in the memory on a FRU.</p> <p>The <i>FRU ID</i> value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The <i>FRU ID</i> value can be:</p> <ul style="list-style-type: none"> <li>• <i>Switch</i> for fixed port count switches.</li> <li>• <i>Slot 1</i> through <i>Slot 10</i> for the SilkWorm 12000 and 24000.</li> <li>• <i>PS 1</i> through <i>PS 4</i> (power supplies) for the SilkWorm 12000 and 24000, or <i>PS 1</i> through <i>PS 2</i> for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>Fan 1</i> through <i>Fan 3</i> for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). <i>Fan 1</i> through <i>Fan 6</i> for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>WWN 1</i> or <i>WWN 2</i> for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.</li> </ul> <p>The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.</p> <p>The SilkWorm 3016 does not have any fans, power supplies or WWN cards.</p>
<b>Recommended Action</b>	<p>If the <b>fruInfoSet</b> command was being run, try the command again; otherwise, the update is automatically reattempted. If it continues to fail, try reseating the FRU.</p> <p>If the message persists, replace the unit.</p>
<b>Severity</b>	ERROR

## EM-1014

### Message

```
<timestamp>, [EM-1014], <sequence-number>, , ERROR, <system-name>,
Unable to read sensor on <FRU Id> (<Return code>)
```

<b>Probable Cause</b>	<p>Indicates that the environmental monitor was unable to access the sensors on the specified FRU.</p> <p>The <i>FRU ID</i> value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The <i>FRU ID</i> value can be:</p> <ul style="list-style-type: none"> <li>• <i>Switch</i> for fixed port count switches.</li> <li>• <i>Slot 1</i> through <i>Slot 10</i> for the SilkWorm 12000 and 24000.</li> <li>• <i>PS 1</i> through <i>PS 4</i> (power supplies) for the SilkWorm 12000 and 24000, or <i>PS 1</i> through <i>PS 2</i> for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>Fan 1</i> through <i>Fan 3</i> for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). <i>Fan 1</i> through <i>Fan 6</i> for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.</li> <li>• <i>WWN 1</i> or <i>WWN 2</i> for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.</li> </ul>
-----------------------	---

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

**Recommended Action** If the message persists, replace the unit.

**Severity** ERROR

## EM-1015

### Message

```
<timestamp>, [EM-1015], <sequence-number>,, WARNING, <system-name>,
Warm recovery failed (<Return code>)
```

**Probable Cause** Indicates that a problem was discovered when performing consistency checks during a warm boot.

**Recommended Action** A **reboot** or power cycle is required to clear the situation.

**Severity** WARNING

## EM-1016

### Message

```
<timestamp>, [EM-1016], <sequence-number>,, WARNING, <system-name>,
Cold recovery failed (<Return code>)
```

**Probable Cause** Indicates that consistency checks during a cold boot discovered a problem.

**Recommended Action** Monitor the switch.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## EM-1017

### Message

```
<timestamp>, [EM-1017], <sequence-number>,, WARNING, <system-name>,
Uncommitted WWN change detected. Cold reboot required.
```

**Probable Cause** Indicates that a user did not commit a changed WWN value prior executing a **reboot**, power cycle, or **firmwareDownload** operation.

**Recommended Action** Change and commit the new WWN value.

**Severity** WARNING

## EM-1028

### Message

```
<timestamp>, [EM-1028], <sequence-number>, , ERROR, <system-name>,
HIL Error: <function> failed to access FRU: <FRU Id> (rc=<return
code>).
```

**Probable Cause** Indicates that problems were encountered when the software attempted to write to the memory of the FRU specified in the error message. The return code is for internal use only. This is a serious FRU hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

**Recommended Action** Try reseating the FRU, if possible. If this fails to correct the error, replace the specified unit.

**Severity** ERROR

## EM-1029

### Message

```
<timestamp>, [EM-1029], <sequence-number>,, ERROR, <system-name>,
<FRU Id> I2C access problems (<error code>): state <current state>
```

### Probable Cause

Indicates that the I2C bus had problems and a timeout occurred.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

### Recommended Action

This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the FRU. If it continues to fail, replace the unit.

### Severity

ERROR

## EM-1031

### Message

```
<timestamp>, [EM-1031], <sequence-number>,, ERROR, <system-name>,
<FRU Id> ejector not closed
```

### Probable Cause

Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but at least one ejector switch is not latched. The blade in the specified slot is treated as not inserted. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

### Recommended Action

Close the ejector switch if the FRU is intended for use.



**Severity** ERROR

## EM-1033

### Message

```
<timestamp>, [EM-1033], <sequence-number>,, ERROR, <system-name>,
CP in <FRU Id> set to faulty because CP ERROR asserted
```

### Probable Cause

Indicates that the standby CP has been detected as faulty. The High Availability feature will not be available. This message occurs every time the other CP reboots, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the CP; however, you might want to find out why the failover occurred. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.

### Recommended Action

If the standby CP was just rebooted, wait for the error to clear (run **slotShow** to determine if it has cleared). Watch for the EM-1047 message to verify this error cleared.

If the standby CP continues to be faulty or if it was not intentionally rebooted, check the error logs on the other CP (using the **errDump** command) to determine the cause of the error state.

If the state persists, try reseating the FRU.

If the message persists, replace the FRU.

**Severity** ERROR

## EM-1034

### Message

```
<timestamp>, [EM-1034], <sequence-number>,, ERROR, <system-name>,
<FRU Id> set to faulty, rc=<return code>
```

### Probable Cause

Indicates that the specified FRU has been marked as faulty for the specified reason.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

**Recommended  
Action**

Try reseating the FRU.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the fault persists, replace the FRU.

**Severity**

ERROR

## EM-1036

**Message**

```
<timestamp>, [EM-1036], <sequence-number>, , WARNING, <system-name>,
<FRU Id> is not accessible.
```

**Probable  
Cause**

Indicates that the specified FRU does not seem to be present on the switch.

If the FRU is a WWN card, then default WWN and IP addresses are used for the switch.

**Recommended  
Action**

Reseat the FRU card.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the FRU.

**Severity**

WARNING

## EM-1041

**Message**

```
<timestamp>, [EM-1041], <sequence-number>, , WARNING, <system-name>,
Sensor values for <FRU Id>: <Sensor Value> <Sensor Value> <Sensor
Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value>
```

**Probable  
Cause**

Indicates that sensors detected a warning condition. All significant sensors for the FRU are displayed; each contains a header.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.

- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

This message can display:

- voltages in volts
- temperature in Celsius
- fan speeds in RPM

**Recommended Action** If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended action for those messages.

**Severity** WARNING

## EM-1042

### Message

```
<timestamp>, [EM-1042], <sequence-number>,, WARNING, <system-name>,
Important FRU header data for <FRU Id> is not valid).
```

**Probable Cause** Indicates that the indicated FRU has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly or corrupted in the object database, which contains information about all FRUs.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

<b>Recommended Action</b>	Try reseating the FRU. If the condition persists, replace the FRU unit.
<b>Severity</b>	WARNING

## EM-1043

### Message

```
<timestamp>, [EM-1043], <sequence-number>,, WARNING, <system-name>,
Can't power <FRU Id> <state (on or off)>.
```

<b>Probable Cause</b>	Indicates that the specified FRU cannot be powered on or off.
-----------------------	---

<b>Recommended Action</b>	The specified FRU is not responding to commands and should be replaced.
<b>Severity</b>	WARNING

## EM-1044

### Message

```
<timestamp>, [EM-1044], <sequence-number>,, WARNING, <system-name>,
Can't power on <FRU Id>, its logical switch is shut down
```

<b>Probable Cause</b>	Indicates that the specified FRU cannot be powered on because the associated logical switch is shut down.
-----------------------	---

<b>Recommended Action</b>	Run the <b>switchStart</b> command on the associated logical switch.
<b>Severity</b>	WARNING

## EM-1045

### Message

```
<timestamp>, [EM-1045], <sequence-number>,, WARNING, <system-name>,
<FRU Id> is being powered <new state>
```

<b>Probable Cause</b>	Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. If new_state is On, a port blade is being powered on because more power is available (either a power supply was inserted or a port blade was removed or powered down). If new_state is Off, a port blade has been powered down because a power supply has been faulted, because it is indicating a predicted failure. If new_state is Down (not enough power), a newly inserted port blade was not powered on because there was not enough power available.
<b>Recommended Action</b>	The SilkWorm 12000 requires two power supplies for a fully populated chassis; however, you should always operate the system with four operating power supplies for redundancy.  The SilkWorm 24000 requires only a single power supply for a fully populated chassis; however, you should always operate the system with at least two power supplies for redundancy.
<b>Severity</b>	WARNING

## EM-1046

### Message

```
<timestamp>, [EM-1046], <sequence-number>,, WARNING, <system-name>,
Sysctrl reports error status for blade ID <id value> for the blade
in slot <slot number>
```

<b>Probable Cause</b>	Indicates that the system controller encountered a blade with an unknown ID in the slot specified. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.
<b>Recommended Action</b>	If the blade ID listed is not correct, then the FRU header for the blade is corrupted and the blade must be replaced. For the SilkWorm 12000, the blade ID should be 1 for a CP blade and 2 for a port blade. For the SilkWorm 24000, the blade ID should be 5 for a CP blade and 4 for a port blade.
<b>Severity</b>	WARNING

## EM-1047

### Message

```
<timestamp>, [EM-1047], <sequence-number>,, INFO, <system-name>, CP
in slot <slot number> not faulty, CP ERROR deasserted
```

<b>Probable Cause</b>	Indicates that the EM-1033 message has been turned off. The new standby CP is in the process of rebooting and has turned off the CP_ERR signal. This message occurs only on the SilkWorm 12000 and SilkWorm 24000.
<b>Recommended Action</b>	No action is required.
<b>Severity</b>	INFO

## EM-1048

### Message

```
<timestamp>, [EM-1048], <sequence-number>,, INFO, <system-name>,
<FRU Id> I2C access recovered: state <current state>
```

### Probable Cause

Indicates that the I2C bus problems have been resolved and I2C access to the FRU has become available again.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

### Recommended Action

The EM-1029 error can be a transitory error; if the problem resolves, the EM-1048 message is displayed.

### Severity

INFO

## EM-1049

### Message

```
<timestamp>, [EM-1049], <sequence-number>,, INFO, <system-name>,
FRU <FRU Id> insertion detected.
```

### Probable Cause

Indicates that a FRU of the type and location specified by the *FRU ID* was detected as having been inserted into the chassis.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.

- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

**Recommended Action** Verify that the unit is in service.

**Severity** INFO

## EM-1050

### Message

```
<timestamp>, [EM-1050], <sequence-number>,, INFO, <system-name>,
FRU <FRU Id> removal detected.
```

**Probable Cause** Indicates that a FRU of the specified type and location was removed from the chassis.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. These FRU values might display in this message for these switches, but these parts cannot be replaced separately. The entire switch is a FRU.

**Recommended Action** Verify that the unit was intended to be removed. Replace the unit as soon as possible.

**Severity** INFO

## EM-1051

### Message

```
<timestamp>, [EM-1051], <sequence-number>,, INFO, <system-name>,
<FRU Id>: Inconsistency detected, FRU re-initialized
```

### Probable Cause

Indicates that an inconsistent state was found in the FRU. This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and traffic might have been disrupted.

### Recommended Action

No action is required.

### Severity

INFO

## EM-1052

### Message

```
<timestamp>, [EM-1052], <sequence-number>,, WARNING, <system-name>,
<FRU Id> sensor 0x<Sensor Code> value out of range: <Raw Sensor
Value>/<Retry Count>
```

### Probable Cause

Indicates that one or more sensor values for a FRU are radically out of range. This might be an environmental problem or a problem with the sensor hardware.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *WWN 1* or *WWN 2* for the SilkWorm 12000 and 24000. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

This message can display:

- voltages in volts
- temperature in Celsius
- fan speeds in RPM



<b>Recommended Action</b>	<p>If the message is isolated, it might be a transient problem with the sensor hardware; monitor the error messages on the switch. If the message is persistent, without other environmental errors, replace the FRU.</p> <p>If the message is persistent, and there are other associated environmental messages, follow the actions for those messages.</p>
<b>Severity</b>	WARNING

## EM-1053

### Message

```
<timestamp>, [EM-1053], <sequence-number>,, WARNING, <system-name>,
No cached sensor values available for <FRU ID>
```

### Probable Cause

Indicates that there are no cached sensor values for the sensor, and software was unable to read new values.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- *Switch* for fixed port count switches.
- *Slot 1* through *Slot 10* for the SilkWorm 12000 and 24000.
- *PS 1* through *PS 4* (power supplies) for the SilkWorm 12000 and 24000, or *PS 1* through *PS 2* for the SilkWorm 3900 and 4100. The power supplies on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.
- *Fan 1* through *Fan 3* for the SilkWorm 12000, 24000, and 4100 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SilkWorm 3900 (six fans in three FRUs). The fans on the SilkWorm 3250 and the SilkWorm 3850 are not field replaceable.

The SilkWorm 3250 has one power supply and three fans, and the SilkWorm 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The SilkWorm 3016 does not have any fans, power supplies or WWN cards.

<b>Recommended Action</b>	<p>If the message is isolated, it might be a transient problem with the sensor hardware; monitor the error messages on the switch.</p> <p>If the message is persistent, replace the FRU.</p>
<b>Severity</b>	WARNING

## EM-1055

### Message

```
<timestamp>, [EM-1055], <sequence-number>,, WARNING, <system-name>,
<FRU ID>: Port media incompatible. Reason: <Reason for
incompatibility>
```

**Probable Cause** Indicates that an incompatible port media is detected.

**Cause**

The possible causes are:

- The port media is not capable of running at the configured port speed.
- The port media generates too much heat to be used in the slot.

**Recommended Action** Verify that the media can be run at the configured port speed.

If the port media is extended long wavelength, move it to a port that can support the heat generated.

**Severity** WARNING

## EM-1056

**Message**

```
<timestamp>, [EM-1056], <sequence-number>,, WARNING, <system-name>,  
<FRU Id>: Port faulted. Reason: <Reason code for the fault>
```

**Probable Cause** Indicates a faulty port media is detected. The reason code for this message is for internal use only. This message is valid for only the SilkWorm 4100.

**Recommended Action** Replace the defective port media.

**Severity** WARNING

# EVMD Error Messages

---

## EVMD-1001

### Message

```
<timestamp>, [EVMD-1001], <sequence-number>,, WARNING, <system-name>, Event session killed, host IP = <Host IP address>, port = <Host TCP port number>
```

### Probable Cause

The TCP socket is closed because of a TCP write error. There can be many causes for this loss of connection:

- The API host application exits without notifying the switch.
- The API host computer is shut down.
- There has been a network problem.
- The Ethernet cable is not properly connected to the switch.
- A user has unplugged the Ethernet cable and then plugged it back in.

### Recommended Action

This problem can be transient; try to reestablish the connection.

If the cause is a network or Ethernet cable problem, you must fix the problem before you can reestablish an API session. Verify that your workstation has a TCP connection to the switch.

The Fabric OS automatically kills unused sessions to prevent resource leaking.

### Severity

WARNING



# FABR Error Messages

---

## FABR-1001

### Message

```
<timestamp>, [FABR-1001], <sequence-number>,, WARNING, <system-name>, port <port number>, <segmentation reason>
```

### Probable Cause

Indicates that the specified switch port is isolated because of a segmentation due to mismatched configuration parameters.

### Recommended Action

Based on the segmentation reason displayed with the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

### Severity

WARNING

## FABR-1002

### Message

```
<timestamp>, [FABR-1002], <sequence-number>,, WARNING, <system-name>, fabGaid: no free multicast alias IDs
```

### Probable Cause

Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

### Recommended Action

Verify alias IDs using the **fabricShow** command on the principal switch.

### Severity

WARNING

## FABR-1003

### Message

```
<timestamp>, [FABR-1003], <sequence-number>,, WARNING, <system-
name>, port <port number>: ILS <command> bad size <payload size>,
wanted <expected payload size>
```

### Probable Cause

Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent an invalid sized payload.

### Recommended Action

Investigate the neighbor switch for problems. Run the **errShow** command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStateShow** command on both the receiving and transmitting switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## FABR-1004

### Message

```
<timestamp>, [FABR-1004], <sequence-number>,, WARNING, <system-
name>, port: <port number>, req iu: 0x<address of IU request sent>,
state: 0x<command sent>, resp iu: 0x<address of response IU
received>, state 0x<response IU state>, <additional description>
```

### Probable Cause

Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

### Recommended Action

If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## FABR-1005

### Message

```
<timestamp>, [FABR-1005], <sequence-number>,, WARNING, <system-name>, <command sent>: port <port number>: status 0x<reason for failure> (<description of failure reason>) xid = 0x<exchange ID of command>
```

### Probable Cause

Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

### Recommended Action

This message is often transitory. No action is required.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## FABR-1006

### Message

```
<timestamp>, [FABR-1006], <sequence-number>,, WARNING, <system-name>, Node free error, caller: <error description>
```

### Probable Cause

Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

### Recommended Action

In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## FABR-1007

### Message

```
<timestamp>, [FABR-1007], <sequence-number>,, WARNING, <system-name>, IU free error, caller: <function attempting to de-allocate IU>
```

### Probable Cause

Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

### Recommended Action

In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FABR-1008

### Message

```
<timestamp>, [FABR-1008], <sequence-number>,, WARNING, <system-name>, <error description>
```

### Probable Cause

Indicates that errors occurred during the request domain ID state; the information unit cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

### Recommended Action

No action is required if the message appears with the FABR\_1005 message.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FABR-1009

### Message

```
<timestamp>, [FABR-1009], <sequence-number>,, WARNING, <system-name>, <error description>
```

### Probable Cause

Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty EFP type. This message is rare and usually indicates a problem with the Fabric OS.

### Recommended Action

The fabric daemon will discard the EFP. The system will recover through the EFP retrieval process.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FABR-1010

### Message

```
<timestamp>, [FABR-1010], <sequence-number>,, WARNING, <system-name>, <error description>
```



**Probable Cause** Indicates that the errors occurred while cleaning up the RDI (request domain ID). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

**Recommended Action** If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FABR-1011

### Message

```
<timestamp>, [FABR-1011], <sequence-number>, , ERROR, <system-name>,
<error description>
```

**Probable Cause** Indicates that the Fabric OS is unable to inform the FSSME (Fabric OS State Synchronization Management module) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

**Recommended Action** If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## FABR-1012

### Message

```
<timestamp>, [FABR-1012], <sequence-number>, , WARNING, <system-
name>, <function stream>: no such type, <invalid type>
```

**Probable Cause** Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

**Recommended Action** The fabric daemon will take proper action to recover from the error.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FABR-1013

### Message

```
<timestamp>, [FABR-1013], <sequence-number>, , CRITICAL, <system-
name>, No Memory: pid=<fabric process id> file=<source file name>
line=<line number within the source file>
```

**Probable Cause** Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

**Recommended Action** The system will recover by failing over to the standby CP.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** CRITICAL

## FABR-1014

### Message

```
<timestamp>, [FABR-1014], <sequence-number>,, ERROR, <system-name>,
Port <port number> Disabled: Insistent Domain ID <Domain ID> could
not be obtained. Principal Assigned Domain ID = <Domain ID>
```

**Probable Cause** Indicates that the specified port received an RDI (request domain ID) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). FICON mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

**Recommended Action** Run the **configShow** command to view the fabric.ididmode. A 0 means the IDID mode is disabled; a 1 means it is enabled.  
Set the switch to insistent domain ID mode. This mode is set under the **configure** command or in Web Tools on the **Switch Admin > configure** window.

**Severity** ERROR

## FABR-1015

### Message

```
<timestamp>, [FABR-1015], <sequence-number>,, ERROR, <system-name>,
FICON Insistent DID max retry exceeded: All E-Ports will be
disabled. Switch is isolated.
```

**Probable Cause** Indicates that the application exceeded RDI (request domain ID) requests for the insistent domain ID. All E\_Ports are disabled, isolating the specified switch from the fabric.

**Recommended Action** Verify that the insistent domain ID is unique in the fabric and then reenble the E\_Ports. Run the **fabricShow** command to view the domain IDs across the fabric and the **configure** command to change the insistent domain ID mode. Refer to the *Fabric OS Command Reference Manual* for more information on these commands.

**Severity** ERROR

## FABR-1016

### Message

```
<timestamp>, [FABR-1016], <sequence-number>,, WARNING, <system-name>, ficonMode is enabled.
```

### Probable Cause

Indicates that FICON mode is enabled on the switch through a user interface command.

### Recommended Action

No action is required.

### Severity

WARNING

## FABR-1017

### Message

```
<timestamp>, [FABR-1017], <sequence-number>,, WARNING, <system-name>, ficonMode is disabled.
```

### Probable Cause

Indicates that FICON mode is disabled on the switch through a user interface command.

### Recommended Action

No action is required.

### Severity

WARNING

## FABR-1018

### Message

```
<timestamp>, [FABR-1018], <sequence-number>,, WARNING, <system-name>, PSS principal failed (<reason for not becoming the principal switch>: <WWN of new principal switch>)
```

### Probable Cause

Indicates that a failure occurred when trying to set the principal switch using the **fabricPrincipal** command. The message notifies the user that the switch failed to become the principal switch because either:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower WWN.

### Recommended Action

Make sure that no other switches is configured as the principal switch. Force a fabric rebuild by using the **switchDisable** and **switchEnable** commands.

Refer to the *Fabric OS Command Reference Manual* for more information the **fabricPrincipal** command.

**Severity** WARNING

## FABR-1019

### Message

```
<timestamp>, [FABR-1019], <sequence-number>,, CRITICAL, <system-name>, Critical fabric size (<current domains>) exceeds supported configuration (<supported domains>)
```

**Probable Cause** Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

**Recommended Action** Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

**Severity** CRITICAL

## FABR-1020

### Message

```
<timestamp>, [FABR-1020], <sequence-number>,, CRITICAL, <system-name>, Webtool will be disabled in <days> days <hours> hours and <minutes> minutes
```

**Probable Cause** Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

**Recommended Action** Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

**Severity** CRITICAL

## FABR-1021

### Message

```
<timestamp>, [FABR-1021], <sequence-number>,, CRITICAL, <system-name>, Webtool is disabled
```

**Probable Cause** Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

**Recommended Action** Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

**Severity** CRITICAL

## FABR-1022

### Message

```
<timestamp>, [FABR-1022], <sequence-number>,, CRITICAL, <system-name>, Fabric size (<actual domains>) exceeds supported configuration (<supported domains>). Fabric limit timer (<type>) started from <grace period in seconds>.
```

**Probable Cause** Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

**Recommended Action** Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

**Severity** CRITICAL

## FABR-1023

### Message

```
<timestamp>, [FABR-1023], <sequence-number>,, INFO, <system-name>, Fabric size is within supported configuration (<supporteddomains>). Fabric limit timer (<type>) stopped at <grace period in seconds>.
```

**Probable Cause** Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

**Recommended Action** No action is required.

**Severity** INFO

## FABR-1024

### Message

```
<timestamp>, [FABR-1024], <sequence-number>,, INFO, <system-name>,
Initializing fabric size limit timer <grace period>
```

### Probable Cause

Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size: a specified limit to the number of domains. This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace-period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

### Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

### Severity

INFO

## FABR-1029

### Message

```
<timestamp>, [FABR-1029], <sequence-number>,, INFO, <system-name>,
Port <port number> negotiated <flow control mode description> (mode
= <received flow control mode>)
```

### Probable Cause

Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC\_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R\_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R\_RDY primitive for flow control.
- DUAL\_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of ELP exchange. This mode also uses the R\_RDY primitive for flow control.

### Recommended Action

No action is required.

### Severity

INFO

# FABS Error Messages

---

## FABS-1001

### Message

```
<timestamp>, [FABS-1001], <sequence-number>,, CRITICAL, <system-name>, <Function name> <Description of memory need>
```

### Probable Cause

Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. *Description of memory need* indicates how much memory was being requested. The value could be any whole number.

### Recommended Action

Reboot or power cycle the switch.

### Severity

CRITICAL

## FABS-1002

### Message

```
<timestamp>, [FABS-1002], <sequence-number>,, WARNING, <system-name>, <Function name> <Description of problem>
```

### Probable Cause

Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

### Recommended Action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

### Severity

WARNING

## FABS-1004

### Message

```
<timestamp>, [FABS-1004], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem> process <Process ID number> (<Current command name>) <Pending signal number>
```

**Probable Cause** Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

**Recommended Action** Reboot or power cycle the switch.

**Severity** WARNING

## FABS-1005

### Message

```
<timestamp>, [FABS-1005], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem> (<ID type>= <ID number>)
```

**Probable Cause** Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The possible values for *function name and description of problem* are:

fabsys\_write: Unsupported write operation: process xxx

where xxx is the process ID (PID), which could be any whole number.

**Recommended Action** Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems). If the message persists, run the **firmwareDownload** command to update the firmware.

**Severity** WARNING

## FABS-1006

### Message

```
<timestamp>, [FABS-1006], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem>: object <object type id> unit <slot>
```

**Probable Cause** Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate that a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media\_sync: Media oid mapping failed
- fabsys\_media\_i2c\_op: Media oid mapping failed
- fabsys\_media\_i2c\_op: obj is not media type
- media\_class\_hndlr: failed sending media state to blade driver

**Recommended Action** If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, fail over or reboot the switch.



If the message persists, run the **firmwareDownload** command to update the firmware.

**Severity** WARNING

## FABS-1007

### Message

```
<timestamp>, [FABS-1007], <sequence-number>,, WARNING, <system-name>, <Function name>: Media state is invalid - status=<Status value>
```

**Probable Cause** Indicates that the Fabric OS has detected an invalid value in an object's status field. This is usually an internal Fabric OS problem or file corruption.

**Recommended Action** Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

**Severity** WARNING

## FABS-1008

### Message

```
<timestamp>, [FABS-1008], <sequence-number>,, WARNING, <system-name>, <Function name>: Media oid mapping failed
```

**Probable Cause** Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

**Recommended Action** Reboot or power cycle the switch.

**Severity** WARNING

## FABS-1009

### Message

```
<timestamp>, [FABS-1009], <sequence-number>,, WARNING, <system-name>, <Function name>: type is not media
```

**Probable Cause** Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

**Recommended Action** Reboot or power cycle the switch.

**Severity** WARNING

## FABS-1010

### Message

```
<timestamp>, [FABS-1010], <sequence-number>,, WARNING, <system-name>, <Function name>: Wrong media_event <Event number>
```

### Probable Cause

Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

### Recommended Action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

### Severity

WARNING

# FCMC Error Messages

---

## FCMC-1001

**Message**

```
<timestamp>, [FCMC-1001], <sequence-number>,, CRITICAL, <system-name>, <function>: <failed function call> failed, out of memory condition
```

**Probable Cause**

Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

**Recommended Action**

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

**Severity**

CRITICAL



# FCPD Error Messages

---

## FCPD-1001

### Message

```
<timestamp>, [FCPD-1001], <sequence-number>,, WARNING, <system-name>, Probing failed on <error string>
```

### Probable Cause

Indicates that an FCP switch probed devices on a loop port, and probing failed on either the L\_Port, AL\_PA address, or the F\_Port. For the AL\_PA, the valid range is 00 through FF. The error string can be either:

- L\_Port *port\_number* ALPA *alpa\_number*
- F\_Port *port\_number*

### Recommended Action

This can happen when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

The SilkWorm 4100 does not support private loop devices.

### Severity

WARNING

## FCPD-1002

### Message

```
<timestamp>, [FCPD-1002], <sequence-number>,, WARNING, <system-name>, port <port number>, bad R_CTL for fcp probing: 0x<R_CTL value>
```

### Probable Cause

Indicates that the response frame received on the specified port for an inquiry request contains an invalid value in the routing control field.

### Recommended Action

This can happen only if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

### Severity

WARNING

## FCPD-1003

**Message**

```
<timestamp>, [FCPD-1003], <sequence-number>,, INFO, <system-name>,  
Probing failed on <error string> which is possibly a private device  
which is not supported in this port type
```

**Probable  
Cause**

Private devices will not respond to the switch PLOGI during probing.

**Recommended  
Action**

Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

**Severity**

INFO

# FCPH Error Messages

---

## FCPH-1001

### Message

```
<timestamp>, [FCPH-1001], <sequence-number>,, CRITICAL, <system-name>, <function>: <failed function call> failed, out of memory condition
```

### Probable Cause

Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* can only be `fc_create`. This function creates a Fibre Channel driver instance.

The *failed function call* is `kmalloc_wrapper` failed. This function call is for kernel memory allocation.

### Recommended Action

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over, and the standby CP will become the active CP.

### Severity

CRITICAL





# FICU Error Messages

---

## FICU-1001

### Message

```
<timestamp>, [FICU-1001], <sequence-number>,, ERROR, <system-name>,  
<function name>: config<config Set(key)|Get(key)| Save> failed rc =  
<error>
```

**Probable Cause** Indicates that one of the configuration management functions failed. The key variable is part of the Fabric OS configuration database and is for support use only. The error variable is an internal error number.

**Recommended Action** Execute an **haFailover** on the switch if it has redundant CPs or reboot the switch. Run the **saveCore** command to check if your flash is full. If the flash is full, run the **saveCore** command to clear the core files. Refer to the *Fabric OS Command Reference Manual* for more information on these commands.

**Severity** ERROR

## FICU-1002

### Message

```
<timestamp>, [FICU-1002], <sequence-number>,, ERROR, <system-name>,  
Failed to get RNID from Management Server Domain=<domain>  
rc=<error>
```

**Probable Cause** Indicates that the FICON-CUP daemon failed to get switch RNID from the management server due to a Fabric OS problem. The domain variable displays the domain ID of the target switch for this RNID. The error variable is an internal error number.

**Recommended Action** If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

**Severity** ERROR

## FICU-1003

### Message

```
<timestamp>, [FICU-1003], <sequence-number>,, WARNING, <system-name>, <function name>: <message> FICON-CUP License Not Installed (<error>)
```

### Probable Cause

Indicates that the FICON-CUP license is not installed on the switch.

### Recommended Action

Run the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Run the **licenseAdd** command to add the license to your switch.

### Severity

WARNING

## FICU-1004

### Message

```
<timestamp>, [FICU-1004], <sequence-number>,, WARNING, <system-name>, <function name>: Failed to set FMS mode: conflicting PID Format:<pid_format>, FMS Mode:<mode>
```

### Probable Cause

Indicates that a PID format conflict was encountered. The core PID format is required for FICON-CUP. The `pid_format` variable displays the PID format currently running on the fabric:

- 0 is VC-encoded PID format
- 1 is core PID format
- 2 is extended-edge PID format

FMS mode displays whether FICON Management Server mode is enabled; a 0 means this mode is enabled and a 1 means this mode is disabled.

### Recommended Action

For FICON Management Server mode (`fmsmode`) to be enabled, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and reenables `fmsmode` using **ficoncupset** command. Refer to the *Fabric OS Procedures Guide* for information on core PID mode and the *Fabric OS Command Reference Manual* for information on the **configure** command and **ficoncupset** command.

### Severity

WARNING

## FICU-1005

### Message

```
<timestamp>, [FICU-1005], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>
```

**Probable Cause** Indicates that an initialization of a module within the FICON-CUP daemon failed.

**Recommended Action** Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

**Severity** ERROR

## FICU-1006

### Message

```
<timestamp>, [FICU-1006], <sequence-number>,, WARNING, <system-name>, Control Device Allegiance Reset (Logical Path: 0x<PID>:0x<channel image ID>)
```

**Probable Cause** Indicates that the path with the specified PID and channel image ID lost allegiance to a FICON-CUP device.

**Recommended Action** Check if the FICON channel corresponding to the PID in the message is functioning correctly.

**Severity** WARNING

## FICU-1007

### Message

```
<timestamp>, [FICU-1007], <sequence-number>,, WARNING, <system-name>, <function name>: Failed to allocate memory while performing <message>
```

**Probable Cause** Indicates that memory resources are low. This might be a transient problem.

**Recommended Action** If the message persists, check the memory usage on the switch, using the **memShow** command. If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FICU-1008

### Message

```
<timestamp>, [FICU-1008], <sequence-number>,, WARNING, <system-name>, FMS mode has been enabled. Port:<port number> has been disabled due to port address conflict.
```

**Probable Cause** Indicates that the specified port was disabled when the switch was enabled for FICON Management Server mode (fmsmode). This was due to a port address conflict.

**Recommended Action** No action is required.

**Severity** WARNING

## FICU-1009

### Message

```
<timestamp>, [FICU-1009], <sequence-number>,, WARNING, <system-name>, FMS Mode enable failed due to insufficient frame filtering resources on some ports
```

**Probable Cause** Indicates that the frame filtering resources required to enable FICON Management Server mode (fmsmode) were not available on some of the ports.

**Recommended Action** Use the **perfDelFilterMonitor** command to delete the filter-based performance monitors used on all ports to free up the resources.

**Severity** WARNING

## FKLB Error Messages

---

### FKLB-1001

**Message**

```
<timestamp>, [FKLB-1001], <sequence-number>,, WARNING, <system-name>, exchange <xid> overlapped, pid=<pid>
```

**Probable Cause**

Indicates that the FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application will overlap. This happens on a timed-out exchange; it automatically recovers after the application times the exchange out.

**Recommended Action**

No action is required.

**Severity**

WARNING



# FLOD Error Messages

---

## FLOD-1001

### Message

```
<timestamp>, [FLOD-1001], <sequence-number>,, WARNING, <system-name>, Unknown LSR type: port <port number>, type <LSR header type>
```

### Probable Cause

Indicates that the link state record (LSR) type is unknown. The following two LSR header types are the only known types: 1 - Unicast and 3 - Multicast.

### Recommended Action

No action is required. The record is discarded.

### Severity

WARNING

## FLOD-1003

### Message

```
<timestamp>, [FLOD-1003], <sequence-number>,, WARNING, <system-name>, Link count exceeded in received LSR, value = <link count number>
```

### Probable Cause

Indicates that the acceptable link count received was exceeded in the link state record (LSR).

### Recommended Action

No action is required. The record is discarded.

### Severity

WARNING

## FLOD-1004

### Message

```
<timestamp>, [FLOD-1004], <sequence-number>,, ERROR, <system-name>, Excessive LSU length = <LSU length>
```

**Probable Cause** Indicates that the LSU size exceeds what the system can support.

**Recommended Action** Reduce the number of switches in the fabric or reduce the number of redundant ISLs between two switches.

**Severity** ERROR

## FLOD-1005

### Message

```
<timestamp>, [FLOD-1005], <sequence-number>,, WARNING, <system-name>, Invalid received domain ID: <domain number>
```

**Probable Cause** Indicates that the received LSR contained an invalid domain number.

**Recommended Action** No action is required. The LSR is discarded.

**Severity** WARNING

## FLOD-1006

### Message

```
<timestamp>, [FLOD-1006], <sequence-number>,, WARNING, <system-name>, Transmitting invalid domain ID: <domain number>
```

**Probable Cause** Indicates that the transmit LSR contained an invalid domain number.

**Recommended Action** No action is required. The LSR is discarded.

**Severity** WARNING



# FSPF Error Messages

---

## FSPF-1001

**Message**

```
<timestamp>, [FSPF-1001], <sequence-number>,, ERROR, <system-name>,  
Input Port <port number> out of range
```

**Probable Cause**

Indicates that the specified input port number is out of range; it does not exist on the switch.

**Recommended Action**

No action is required.

**Severity**

ERROR

## FSPF-1002

**Message**

```
<timestamp>, [FSPF-1002], <sequence-number>,, INFO, <system-name>,  
Wrong neighbor ID (<domain ID>) in Hello message from port <port  
number>, expected ID = <domain ID>
```

**Probable Cause**

Indicates that the switch received the wrong domain ID from a neighbor (adjacent) switch in the HELLO message from a specified port. This might happen when a domain ID for a switch has been changed.

**Recommended Action**

No action is required.

**Severity**

INFO

## FSPF-1003

**Message**

```
<timestamp>, [FSPF-1003], <sequence-number>,, ERROR, <system-name>,  
Remote Domain ID <domain number> out of range, input port = <port  
number>
```

**Probable Cause** Indicates that the specified remote domain ID is out of range.

**Recommended Action** No action is required. The frame is discarded.

**Severity** ERROR

## FSPF-1005

### Message

```
<timestamp>, [FSPF-1005], <sequence-number>,, ERROR, <system-name>,
Wrong Section Id <section number>, should be <section number>,
input port = <port number>
```

**Probable Cause** Indicates that an incorrect section ID was reported from the specified input port. The section ID is used to identify a set of switches that share an identical topology database. The section ID is implemented inside the protocol. The error message itself will indicate the mismatched section ID. It should be set to 0 for a nonhierarchical fabric. SilkWorm switches support only section ID 0.

**Recommended Action** Use a frame analyzer to verify that the reported section ID is 0. Any connected (other manufacturer) switch with a section ID other than 0 is incompatible in a fabric of SilkWorm switches. Disconnect the offending switch.

**Severity** ERROR

## FSPF-1006

### Message

```
<timestamp>, [FSPF-1006], <sequence-number>,, ERROR, <system-name>,
FSPF Version <FSFP version> not supported, input port = <port
number>
```

**Probable Cause** Indicates that the FSPF version is not supported on the specified input port.

**Recommended Action** Update the FSPF version by running the **firmwareDownload** command to update the firmware to the latest version. All current versions of the Fabric OS support FSPF version 2, which is the correct version.

**Severity** ERROR

# FSS Error Messages

---

## FSS-1001

**Message**

```
<timestamp>, [FSS-1001], <sequence-number>,, WARNING, <system-name>, Application dropping HA data update.
```

**Probable Cause**

Indicates that an application has dropped a high availability (HA) data update.

**Recommended Action**

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**

WARNING

## FSS-1002

**Message**

```
<timestamp>, [FSS-1002], <sequence-number>,, WARNING, <system-name>, Application sending too many concurrent HA data updates
```

**Probable Cause**

Indicates that an application has sent too many concurrent high availability (HA) data updates.

**Recommended Action**

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**

WARNING

## FSS-1003

### Message

```
<timestamp>, [FSS-1003], <sequence-number>,, WARNING, <system-name>, Application missing first HA data update
```

### Probable Cause

Indicates that the FSS has dropped the update because an application has not set the transaction flag correctly.

### Recommended Action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## FSS-1004

### Message

```
<timestamp>, [FSS-1004], <sequence-number>,, ERROR, <system-name>, Memory shortage
```

### Probable Cause

Indicates that the system ran out of memory.

### Recommended Action

Run the **memShow** command to view memory usage.

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## FSS-1005

### Message

```
<timestamp>, [FSS-1005], <sequence-number>,, WARNING, <system-name>, FSS read failure
```

### Probable Cause

Indicates that the read system call to the FSS device failed.

### Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## FSS-1006

### Message

```
<timestamp>, [FSS-1006], <sequence-number>,, WARNING, <system-name>, No message available
```

**Probable Cause** Indicates that data is not available on the FSS device.

**Recommended Action** Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING



# FSSM Error Messages

---

## FSSM-1002

### Message

```
<timestamp>, [FSSM-1002], <sequence-number>,, INFO, <system-name>,  
HA State is in sync
```

### Probable Cause

Indicates that the HA state for the active CP is in synchronization with the HA state of the standby CP. If the standby CP is healthy, then a failover is nondisruptive. For more information on the **haFailover** command, refer to the *Fabric OS Command Reference Manual*.

### Recommended Action

No action is required.

### Severity

INFO

## FSSM-1003

### Message

```
<timestamp>, [FSSM-1003], <sequence-number>,, WARNING, <system-  
name>, HA State out of sync
```

### Probable Cause

Indicates that the HA state for the active CP is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of sync, the failover is disruptive.

### Recommended Action

If this message was logged as a result of a user-initiated action (such as running the **switchReboot** command), then no action is required.

Otherwise, issue the **haSyncStart** command on the active CP and try resynchronizing the HA state.

If the HA state does not become synchronized, run the **haDump** command to diagnose the problem.

### Severity

WARNING

## FSSM-1004

### Message

```
<timestamp>, [FSSM-1004], <sequence-number>,, CRITICAL, <system-name>, Active and the standby CP have incompatible software.
```

### Probable Cause

Indicates that the active CP and the standby CP are running firmware that are incompatible with each other. If the active CP fails, the failover will be disruptive.

### Recommended Action

Run the **firmwareDownload** command to load compatible firmware on the standby CP. For details on this command, refer to the *Fabric OS Command Reference Manual*.

### Severity

CRITICAL



## FW Error Messages

---

### FW-1001

**Message**

```
<timestamp>, [FW-1001], <sequence-number>,, INFO, <system-name>,  
<label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the internal temperature of the switch has changed.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

**Severity**

INFO

### FW-1002

**Message**

```
<timestamp>, [FW-1002], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the internal temperature of the switch has fallen below the low boundary.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

**Severity**

WARNING

## FW-1003

### Message

```
<timestamp>, [FW-1003], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the internal temperature of the switch has risen above the high boundary to a value that might damage the switch.

**Recommended Action** This message generally appears when a fan fails. If so, a fan-failure message accompanies this message. Replace the fan.

**Severity** WARNING

## FW-1004

### Message

```
<timestamp>, [FW-1004], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

**Severity** INFO

## FW-1005

### Message

```
<timestamp>, [FW-1005], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

**Severity** INFO

## FW-1006

### Message

```
<timestamp>, [FW-1006], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the speed of the fan has fallen below the low boundary. Fan problems typically contribute to temperature problems.

### Recommended Action

Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan FRU.

### Severity

WARNING

## FW-1007

### Message

```
<timestamp>, [FW-1007], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

### Recommended Action

Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan FRU.

### Severity

WARNING

## FW-1008

### Message

```
<timestamp>, [FW-1008], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

### Recommended Action

No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan FRU.

### Severity

INFO

## FW-1009

### Message

```
<timestamp>, [FW-1009], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the state of the power supply has changed from faulty to functional or from functional to faulty.

### Recommended Action

If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **psShow** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

### Severity

INFO

## FW-1010

### Message

```
<timestamp>, [FW-1010], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the power supply is faulty. The power supply is not producing enough power.

### Recommended Action

Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

### Severity

WARNING

## FW-1011

### Message

```
<timestamp>, [FW-1011], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the power supply is functioning properly.

### Recommended Action

No action is required. Set the high boundary above the normal operation range.

**Severity** INFO

## FW-1012

### Message

```
<timestamp>, [FW-1012], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1033

### Message

```
<timestamp>, [FW-1033], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the temperature of the SFP has changed.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in SFP temperature might indicate a deteriorating SFP.

**Severity** INFO

## FW-1034

### Message

```
<timestamp>, [FW-1034], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the temperature of the SFP has fallen below the low boundary.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** WARNING

## FW-1035

### Message

```
<timestamp>, [FW-1035], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the temperature of the SFP has risen above the high boundary.

**Recommended Action** Frequent fluctuations in temperature might indicate a deteriorating SFP. Replace the SFP.

**Severity** WARNING

## FW-1036

### Message

```
<timestamp>, [FW-1036], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the temperature of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action** No action is required.  
Frequent fluctuations in temperature might indicate a deteriorating SFP.

**Severity** INFO

## FW-1037

### Message

```
<timestamp>, [FW-1037], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the receive power value of the SFP has changed. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Incoming laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

**Severity** INFO

## FW-1038

### Message

```
<timestamp>, [FW-1038], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the receive power value of the SFP has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

**Severity** WARNING

## FW-1039

### Message

```
<timestamp>, [FW-1039], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the receive power value of the SFP has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Replace the SFP before it deteriorates.

**Severity** WARNING

## FW-1040

### Message

```
<timestamp>, [FW-1040], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the receive power value of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1041

### Message

```
<timestamp>, [FW-1041], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the transmit power value of the SFP has changed. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Transmitting laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

**Severity** INFO

## FW-1042

### Message

```
<timestamp>, [FW-1042], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the transmit power value of the SFP has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

**Severity** WARNING

## FW-1043

### Message

```
<timestamp>, [FW-1043], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```



**Probable Cause** Indicates that the transmit power value of the SFP has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** Replace the SFP.

**Severity** WARNING

## FW-1044

### Message

```
<timestamp>, [FW-1044], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the transmit power value of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1045

### Message

```
<timestamp>, [FW-1045], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the value of the SFP voltage has changed.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If the supplied voltage of the SFP transceiver is outside of the normal range, this might indicate a hardware failure. Frequent messages indicate that you must replace the SFP.

**Severity** INFO

## FW-1046

### Message

```
<timestamp>, [FW-1046], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has fallen below the low boundary.

### Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

### Severity

WARNING

## FW-1047

### Message

```
<timestamp>, [FW-1047], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has risen above the high boundary.

### Recommended Action

The supplied current of the SFP transceiver is outside of the normal range, indicating possible hardware failure. If the current rises above the high boundary, you must replace the SFP.

### Severity

WARNING

## FW-1048

### Message

```
<timestamp>, [FW-1048], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1049

### Message

```
<timestamp>, [FW-1049], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has changed.

### Recommended Action

Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

### Severity

INFO

## FW-1050

### Message

```
<timestamp>, [FW-1050], <sequence-number>,, WARNING, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has fallen below the low boundary.

### Recommended Action

Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out\_of\_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

### Severity

WARNING

## FW-1051

### Message

```
<timestamp>, [FW-1051], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has risen above the high boundary. High voltages indicate possible hardware failures.

### Recommended Action

Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

### Severity

WARNING

## FW-1052

### Message

```
<timestamp>, [FW-1052], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the value of the SFP voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1113

### Message

```
<timestamp>, [FW-1113], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of times E\_Ports have gone down has changed. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Port downs might be caused by transient errors.

### Recommended Action

Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

### Severity

INFO

## FW-1114

### Message

```
<timestamp>, [FW-1114], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of times E\_Ports have gone down has fallen below the low boundary. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Port downs might be caused by transient errors.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of E\_Port failures means that the switch is functioning normally.

### Severity

INFO

## FW-1115

### Message

```
<timestamp>, [FW-1115], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of times E\_Ports have gone down has risen above the high boundary. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Port downs might be caused by transient errors.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

### Severity

INFO

## FW-1116

### Message

```
<timestamp>, [FW-1116], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of times E\_Ports have gone down has changed from a value outside of the acceptable range to a value within the acceptable range. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Port downs might be caused by transient errors.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1117

### Message

```
<timestamp>, [FW-1117], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of fabric reconfigures has changed. The following actions can cause a fabric reconfiguration:

- two switches with the same domain ID have connected to one another.
- two fabrics have joined.
- an E\_Port has gone offline.

- a principal link has segmented from the fabric.

**Recommended Action** Verify that the cable is properly connected at both ends. Verify that the SFPs have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

**Severity** INFO

## FW-1118

### Message

```
<timestamp>, [FW-1118], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of fabric reconfigures has fallen below the low boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E\_Port has gone offline.
- A principal link has segmented from the fabric.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of fabric reconfigurations means that the fabric is functioning normally.

**Severity** INFO

## FW-1119

### Message

```
<timestamp>, [FW-1119], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of fabric reconfigures has risen above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E\_Port has gone offline.
- A principal link has segmented from the fabric.

**Recommended Action** Verify that all ISL cables are properly connected at both ends. Verify that the SFP has not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

**Severity** INFO

## FW-1120

### Message

```
<timestamp>, [FW-1120], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of fabric reconfigures has changed from a value outside of the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E\_Port has gone offline.
- A principal link has segmented from the fabric.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1121

### Message

```
<timestamp>, [FW-1121], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of domain ID changes has changed. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1122

### Message

```
<timestamp>, [FW-1122], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of domain ID changes has fallen below the low boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of domain ID changes means that the fabric is functioning normally.

**Severity** INFO

## FW-1123

### Message

```
<timestamp>, [FW-1123], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of domain ID changes has risen above the high boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1124

### Message

```
<timestamp>, [FW-1124], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of domain ID changes has changed from a value outside of the acceptable range to a value within the acceptable range. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO



## FW-1125

### Message

```
<timestamp>, [FW-1125], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of segmentations has changed. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1126

### Message

```
<timestamp>, [FW-1126], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of segmentations has fallen below the low boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of segmentation errors means that the fabric is functioning normally.

### Severity

INFO

## FW-1127

### Message

```
<timestamp>, [FW-1127], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of segmentations has risen above the high boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1128

### Message

```
<timestamp>, [FW-1128], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of segmentations has changed from a value outside of the acceptable range to a value within the acceptable range. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1129

### Message

```
<timestamp>, [FW-1129], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of zone changes has changed. Zone changes occur when there is a change to the effective zone configuration.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1130

### Message

```
<timestamp>, [FW-1130], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of zone changes has fallen below the low boundary. Zone changes occur when there is a change to the effective zone configuration.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of zone configuration changes means that the fabric is functioning normally.

### Severity

INFO

## FW-1131

### Message

```
<timestamp>, [FW-1131], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of zone changes has risen above the high boundary. Zone changes occur when there is a change to the effective zone configuration.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

**FW-1132****Message**

```
<timestamp>, [FW-1132], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of zone changes has changed from a value outside of the acceptable range to a value within the acceptable range. Zone changes occur when there is a change to the effective zone configuration.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

**FW-1133****Message**

```
<timestamp>, [FW-1133], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of fabric logins has changed. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

**FW-1134****Message**

```
<timestamp>, [FW-1134], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of fabric logins has fallen below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of fabric logins means that the fabric is functioning normally.

**Severity**

INFO

## FW-1135

### Message

```
<timestamp>, [FW-1135], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of fabric logins has risen above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1136

### Message

```
<timestamp>, [FW-1136], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of fabric logins has changed from a value outside of the acceptable range to a value within the acceptable range. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1137

### Message

```
<timestamp>, [FW-1137], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SFP state changes has changed. SFP state changes occur when the SFP is inserted or removed.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1138

### Message

```
<timestamp>, [FW-1138], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SFP state changes has fallen below the low boundary. SFP state changes occur when the SFP is inserted or removed.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of SFP state changes means that the switch is functioning normally.

**Severity** INFO

## FW-1139

### Message

```
<timestamp>, [FW-1139], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SFP state changes has risen above the high boundary. SFP state changes occur when the SFP is inserted or removed.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1140

### Message

```
<timestamp>, [FW-1140], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SFP state changes has changed from a value outside of the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1141

### Message

```
<timestamp>, [FW-1141], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of QuickLoop changes has changed.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1142

### Message

```
<timestamp>, [FW-1142], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of QuickLoop changes has fallen below the low boundary.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1143

### Message

```
<timestamp>, [FW-1143], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of QuickLoop changes has risen above the high boundary.

### Recommended Action

Verify that the cable is properly connected at both ends. This might be a transient error and might not require troubleshooting.

### Severity

INFO

**FW-1144****Message**

```
<timestamp>, [FW-1144], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of QuickLoop changes has changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

**FW-1160****Message**

```
<timestamp>, [FW-1160], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of link failures that the port experiences has changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

**Recommended Action** Check both ends of your cable connection. Verify that the cable and SFPs are not faulty. Losses of synchronization commonly causes link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

**Severity** INFO

**FW-1161****Message**

```
<timestamp>, [FW-1161], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of link failures that the port experiences has fallen below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.



**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of link loss errors means that the switch is functioning normally.

**Severity** INFO

## FW-1162

### Message

```
<timestamp>, [FW-1162], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of link failures that the port experiences has risen above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

**Recommended Action** Check both ends of your cable connection. Verify that the cable and SFPs are not faulty. Losses of synchronization commonly cause link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

**Severity** WARNING

## FW-1163

### Message

```
<timestamp>, [FW-1163], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of link failures that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1164

### Message

```
<timestamp>, [FW-1164], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of synchronization losses that the port experiences has changed. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

### Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

If you continue to experience synchronization loss errors, troubleshoot your HBA and contact your switch service provider.

### Severity

INFO

## FW-1165

### Message

```
<timestamp>, [FW-1165], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of synchronization losses that the port experiences has fallen below the low boundary. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of synchronization losses means that the switch is functioning normally.

### Severity

INFO

## FW-1166

### Message

```
<timestamp>, [FW-1166], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of synchronization losses that the port experiences has risen above the high boundary. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

**Recommended Action** Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.  
If you continue to experience loss-of-synchronization errors, troubleshoot your HBA and contact your switch service provider.

**Severity** WARNING

## FW-1167

### Message

```
<timestamp>, [FW-1167], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of synchronization losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1168

### Message

```
<timestamp>, [FW-1168], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of signal losses that the port experiences has changed. Loss of signal generally indicates a physical problem.

**Recommended Action** Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

**Severity** INFO

## FW-1169

### Message

```
<timestamp>, [FW-1169], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of signal losses that the port experiences has fallen below the low boundary. Loss of signal generally indicates a physical problem.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of signal loss errors means that the switch is functioning normally.

**Severity** INFO

## FW-1170

### Message

```
<timestamp>, [FW-1170], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of signal losses that the port experiences has risen above the high boundary. Loss of signal generally indicates a physical problem.

**Recommended Action** Check both ends of your cable connection. Verify that the cable is not faulty.

**Severity** WARNING

## FW-1171

### Message

```
<timestamp>, [FW-1171], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of signal losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of signal generally indicates a physical problem.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem.

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

**Severity** INFO

## FW-1172

### Message

```
<timestamp>, [FW-1172], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of protocol errors that the port experiences has changed. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

### Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

### Severity

INFO

## FW-1173

### Message

```
<timestamp>, [FW-1173], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of protocol errors that the port experiences has fallen below the low boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of protocol errors means that the switch is functioning normally.

### Severity

INFO

## FW-1174

### Message

```
<timestamp>, [FW-1174], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of protocol errors that the port experiences has risen above the high boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

### Recommended Action

Check both ends of your connection. Verify that your cable and SFP are not faulty.

### Severity

WARNING

**FW-1175****Message**

```
<timestamp>, [FW-1175], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of protocol errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

**FW-1176****Message**

```
<timestamp>, [FW-1176], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of invalid words that the port experiences has changed. Invalid words usually indicate a hardware problem with an SFP or cable.

**Recommended Action**

Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

**Severity**

INFO

**FW-1177****Message**

```
<timestamp>, [FW-1177], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the number of invalid words that the port experiences has fallen below the low boundary. Invalid words usually indicate a hardware problem with an SFP or cable.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid words means that the switch is functioning normally.

**Severity**

INFO

## FW-1178

### Message

```
<timestamp>, [FW-1178], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid words that the port experiences has risen above the high boundary. Invalid words usually indicate a hardware problem with an SFP or cable.

### Recommended Action

Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

### Severity

WARNING

## FW-1179

### Message

```
<timestamp>, [FW-1179], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid words that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with an SFP or cable.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1180

### Message

```
<timestamp>, [FW-1180], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid CRCs that the port experiences has changed.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

### Severity

INFO

## FW-1181

### Message

```
<timestamp>, [FW-1181], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid CRCs that the port experiences has fallen below the low boundary.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid CRCs means that the switch is functioning normally.

### Severity

INFO

## FW-1182

### Message

```
<timestamp>, [FW-1182], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid CRCs that the port experiences has risen above the high boundary.

### Recommended Action

This error generally indicates an deteriorating fabric hardware. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

### Severity

WARNING

## FW-1183

### Message

```
<timestamp>, [FW-1183], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid CRCs that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

### Severity

INFO



## FW-1184

### Message

```
<timestamp>, [FW-1184], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has changed.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1185

### Message

```
<timestamp>, [FW-1185], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has fallen below the low boundary.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1186

### Message

```
<timestamp>, [FW-1186], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has risen above the high boundary.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

**FW-1187****Message**

```
<timestamp>, [FW-1187], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the percentage of incoming traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

**FW-1188****Message**

```
<timestamp>, [FW-1188], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the percentage of outgoing traffic that the port experiences has changed.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

**FW-1189****Message**

```
<timestamp>, [FW-1189], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause**

Indicates that the percentage of outgoing traffic that the port experiences has fallen below the low boundary.

**Recommended Action**

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity**

INFO

## FW-1190

### Message

```
<timestamp>, [FW-1190], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the percentage of outgoing traffic that the port experiences has risen above the high boundary.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1191

### Message

```
<timestamp>, [FW-1191], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the percentage of outgoing traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1192

### Message

```
<timestamp>, [FW-1192], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of state changes that the port experiences has changed. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E\_Port, has become an F\_Port, has segmented, or has become a trunk port.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1193

### Message

```
<timestamp>, [FW-1193], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is below low boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of state changes that the port experiences has fallen below the low boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E\_Port, has become an F\_Port, has segmented, or has become a trunk port.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of port state changes means that the switch is functioning normally.

### Severity

INFO

## FW-1194

### Message

```
<timestamp>, [FW-1194], <sequence-number>,, WARNING, <system-name>,
<Port Name>, <Label>, is above high boundary(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of state changes that the port experiences has risen above the high boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E\_Port, has become an F\_Port, has segmented, or has become a trunk port.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

WARNING

## FW-1195

### Message

```
<timestamp>, [FW-1195], <sequence-number>,, INFO, <system-name>,
<Port Name>, <Label>, is between high and low boundaries(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of state changes that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E\_Port, has become an F\_Port, has segmented, or has become a trunk port.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1216

### Message

```
<timestamp>, [FW-1216], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of AL\_PA CRC errors has changed. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

**Recommended Action** Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

**Severity** INFO

## FW-1217

### Message

```
<timestamp>, [FW-1217], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of AL\_PA CRC errors has fallen below the low boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low level of invalid CRC errors means that the switch is functioning normally.

**Severity** INFO

## FW-1218

### Message

```
<timestamp>, [FW-1218], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of CRC errors has risen above the high boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

### Recommended Action

You should configure a five- or six-figure high boundary for this area. Only five-figure (or higher) values for CRC errors indicate problems. When an "above" message is received, check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. Try cleaning the connectors. Check for damage from heat or deterioration from age.

**Severity** WARNING

## FW-1219

### Message

```
<timestamp>, [FW-1219], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of CRC errors has changed from a value outside of the acceptable range to a value within the acceptable range. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1240

### Message

```
<timestamp>, [FW-1240], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE CRC errors has changed. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1241

### Message

```
<timestamp>, [FW-1241], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE CRC errors has fallen below the low boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of CRC errors means that the fabric is functioning normally. The CRC error area of the End-to-End Performance Monitor class helps you tune your fabric. To reduce CRC messages, experiment with alternative topologies and cabling schemes.

**Severity** INFO

## FW-1242

### Message

```
<timestamp>, [FW-1242], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE CRC errors has risen above the high boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

**Recommended Action** The CRC error area of the End-to-End Performance Monitor class helps the user tune the fabric. To reduce CRC errors, experiment with alternative topologies and cabling schemes. Clean equipment, check temperatures, and replace old hardware.

**Severity** WARNING

## FW-1243

### Message

```
<timestamp>, [FW-1243], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of EE CRC errors has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1244

### Message

```
<timestamp>, [FW-1244], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of EE word frames that the switch receives has changed. Receive performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1245

### Message

```
<timestamp>, [FW-1245], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of EE word frames that the switch receives has fallen below the low boundary. Receive performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.



**Severity** INFO

## FW-1246

### Message

```
<timestamp>, [FW-1246], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch receives has risen above the high boundary. Receive performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1247

### Message

```
<timestamp>, [FW-1247], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch receives has changed from a value outside of the acceptable range to a value within the acceptable range. Receive performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1248

### Message

```
<timestamp>, [FW-1248], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch transmits has changed. Transmit performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1249

### Message

```
<timestamp>, [FW-1249], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch transmits has fallen below the low boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1250

### Message

```
<timestamp>, [FW-1250], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch transmits has risen above the high boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1251

### Message

```
<timestamp>, [FW-1251], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of EE word frames that the switch transmits has changed from a value outside of the acceptable range to a value within the acceptable range. Transmit performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1272

### Message

```
<timestamp>, [FW-1272], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of frame types or commands that the port receives has changed. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1273

### Message

```
<timestamp>, [FW-1273], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of frame types or commands that the port receives has fallen below the low boundary. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1274

### Message

```
<timestamp>, [FW-1274], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<Filter Counter>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of frame types or commands that the port receives has risen above the high boundary. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1275

### Message

```
<timestamp>, [FW-1275], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of frame types or commands that the port receives has changed from a value outside of the acceptable range to a value within the acceptable range. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1296

### Message

```
<timestamp>, [FW-1296], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of telnet violations has changed. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1297

### Message

```
<timestamp>, [FW-1297], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of telnet violations has fallen below the low boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** No action is required.

**Severity** INFO

## FW-1298

### Message

```
<timestamp>, [FW-1298], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of telnet violations has risen above the high boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1299

### Message

```
<timestamp>, [FW-1299], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

### Recommended Action

No action is required.

### Severity

INFO

## FW-1300

### Message

```
<timestamp>, [FW-1300], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of HTTP violations has changed. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

### Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1301

### Message

```
<timestamp>, [FW-1301], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of HTTP violations has fallen below the low boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** No action is required.

**Severity** INFO

## FW-1302

### Message

```
<timestamp>, [FW-1302], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of HTTP violations has risen above the high boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1303

### Message

```
<timestamp>, [FW-1303], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of HTTP violations has changed from a value outside of the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** No action is required.

**Severity** INFO

## FW-1304

### Message

```
<timestamp>, [FW-1304], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of API violations has changed. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

### Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1305

### Message

```
<timestamp>, [FW-1305], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of API violations has fallen below the low boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

### Recommended Action

No action is required.

### Severity

INFO

## FW-1306

### Message

```
<timestamp>, [FW-1306], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of API violations has risen above the high boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).



**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1307

### Message

```
<timestamp>, [FW-1307], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of API violations has changed from a value outside of the acceptable range to a value within the acceptable range. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

**Recommended Action** No action is required.

**Severity** INFO

## FW-1308

### Message

```
<timestamp>, [FW-1308], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of RSNMP violations has changed. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1309

### Message

```
<timestamp>, [FW-1309], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of RSNMP violations has fallen below the low boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1310

### Message

```
<timestamp>, [FW-1310], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of RSNMP violations has risen above the high boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

### Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1311

### Message

```
<timestamp>, [FW-1311], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of RSNMP violations has changed from a value outside of the acceptable range to a value within the acceptable range. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1312

### Message

```
<timestamp>, [FW-1312], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of WSNMP violations has changed. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1313

### Message

```
<timestamp>, [FW-1313], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of WSNMP violations has fallen below the low boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1314

### Message

```
<timestamp>, [FW-1314], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of WSNMP violations has risen above the high boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

**Recommended Action** Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1315

### Message

```
<timestamp>, [FW-1315], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of WSNMP violations has changed from a value outside of the acceptable range to a value within the acceptable range. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1316

### Message

```
<timestamp>, [FW-1316], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SES violations has changed. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

### Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1317

### Message

```
<timestamp>, [FW-1317], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SES violations has fallen below the low boundary. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1318

### Message

```
<timestamp>, [FW-1318], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SES violations has risen above the high boundary. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1319

### Message

```
<timestamp>, [FW-1319], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SES violations has changed from a value outside of the acceptable range to a value within the acceptable range. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1320

### Message

```
<timestamp>, [FW-1320], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of MS violations has changed. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

### Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1321

### Message

```
<timestamp>, [FW-1321], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of MS violations has fallen below the low boundary. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1322

### Message

```
<timestamp>, [FW-1322], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of MS violations has risen above the high boundary. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1323

### Message

```
<timestamp>, [FW-1323], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of MS violations has changed from a value outside of the acceptable range to a value within the acceptable range. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1324

### Message

```
<timestamp>, [FW-1324], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of serial violations has changed. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1325

### Message

```
<timestamp>, [FW-1325], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of serial violations has fallen below the low boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1326

### Message

```
<timestamp>, [FW-1326], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of serial violations has risen above the high boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

### Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1327

### Message

```
<timestamp>, [FW-1327], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of serial violations has changed from a value outside of the acceptable range to a value within the acceptable range. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.



**Recommended Action** No action is required.

**Severity** INFO

## FW-1328

### Message

```
<timestamp>, [FW-1328], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of front panel violations has changed. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT\_PANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1329

### Message

```
<timestamp>, [FW-1329], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of front panel violations has fallen below the low boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT\_PANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1330

### Message

```
<timestamp>, [FW-1330], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of front panel violations has risen above the high boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT\_PANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1331

### Message

```
<timestamp>, [FW-1331], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of front panel violations has changed from a value outside of the acceptable range to a value within the acceptable range. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT\_PANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1332

### Message

```
<timestamp>, [FW-1332], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SCC violations has changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

**Recommended Action** Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1333

### Message

```
<timestamp>, [FW-1333], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SCC violations has fallen below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1334

### Message

```
<timestamp>, [FW-1334], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SCC violations has risen above the high boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

### Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1335

### Message

```
<timestamp>, [FW-1335], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SCC violations has changed from a value outside of the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1336

### Message

```
<timestamp>, [FW-1336], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of DCC violations has changed. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

**Recommended Action** Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1337

### Message

```
<timestamp>, [FW-1337], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of DCC violations has fallen below the low boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1338

### Message

```
<timestamp>, [FW-1338], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of DCC violations has risen above the high boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

### Recommended Action

Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1339

### Message

```
<timestamp>, [FW-1339], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of DCC violations has changed from a value outside of the acceptable range to a value within the acceptable range. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1340

### Message

```
<timestamp>, [FW-1340], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of login violations has changed. Login violations indicate that a login failure has been detected.

**Recommended Action** Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1341

### Message

```
<timestamp>, [FW-1341], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1342

### Message

```
<timestamp>, [FW-1342], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

**Recommended Action** Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1343

### Message

```
<timestamp>, [FW-1343], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1344

### Message

```
<timestamp>, [FW-1344], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid timestamps has changed. Invalid-timestamp violations indicate that a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1345

### Message

```
<timestamp>, [FW-1345], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid timestamps has fallen below the low boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1346

### Message

```
<timestamp>, [FW-1346], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid timestamps has risen above the high boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1347

### Message

```
<timestamp>, [FW-1347], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid timestamps has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

**Recommended Action** No action is required.



**Severity** INFO

## FW-1348

### Message

```
<timestamp>, [FW-1348], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid signatures has changed. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1349

### Message

```
<timestamp>, [FW-1349], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid signatures has fallen below the low boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

### Recommended Action

No action is required.

**Severity** INFO

## FW-1350

### Message

```
<timestamp>, [FW-1350], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid signatures has risen above the high boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1351

### Message

```
<timestamp>, [FW-1351], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid signatures has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1352

### Message

```
<timestamp>, [FW-1352], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid certificates has changed. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1353

### Message

```
<timestamp>, [FW-1353], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid certificates has fallen below the low boundary. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1354

### Message

```
<timestamp>, [FW-1354], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of invalid certificates has risen above the high boundary. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1355

### Message

```
<timestamp>, [FW-1355], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of invalid certificates has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1356

### Message

```
<timestamp>, [FW-1356], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of authentication failures has changed. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1357

### Message

```
<timestamp>, [FW-1357], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of authentication failures has fallen below the low boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1358

### Message

```
<timestamp>, [FW-1358], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of authentication failures has risen above the high boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1359

### Message

```
<timestamp>, [FW-1359], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of authentication failures has changed from a value outside of the acceptable range to a value within the acceptable range. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1360

### Message

```
<timestamp>, [FW-1360], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SLAP faulty packets has changed. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1361

### Message

```
<timestamp>, [FW-1361], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SLAP faulty packets has fallen below the low boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1362

### Message

```
<timestamp>, [FW-1362], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of SLAP faulty packets has risen above the high boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1363

### Message

```
<timestamp>, [FW-1363], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of SLAP faulty packets has changed from a value outside of the acceptable range to a value within the acceptable range. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1364

### Message

```
<timestamp>, [FW-1364], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of time service (TS) out-of-sync violations has changed.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1365

### Message

```
<timestamp>, [FW-1365], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of time service out-of-sync violations has fallen below the low boundary.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1366

### Message

```
<timestamp>, [FW-1366], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of time service (TS) out-of-sync violations has risen above the high boundary.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1367

### Message

```
<timestamp>, [FW-1367], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of time service (TS) out-of-sync violations has changed from a value outside of the acceptable range to a value within the acceptable range.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1368

### Message

```
<timestamp>, [FW-1368], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of no-FCS violations has changed. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.



**Severity** INFO

## FW-1369

### Message

```
<timestamp>, [FW-1369], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of no-FCS violations has fallen below the low boundary. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1370

### Message

```
<timestamp>, [FW-1370], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of no-FCS violations has risen above the high boundary. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1371

### Message

```
<timestamp>, [FW-1371], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of no-FCS violations has changed from a value outside of the acceptable range to a value within the acceptable range. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1372

### Message

```
<timestamp>, [FW-1372], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of incompatible security database violations has changed. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1373

### Message

```
<timestamp>, [FW-1373], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of incompatible security database violations has fallen below the low boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1374

### Message

```
<timestamp>, [FW-1374], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of incompatible security database violations has risen above the high boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

### Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1375

### Message

```
<timestamp>, [FW-1375], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of incompatible security database violations has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1376

### Message

```
<timestamp>, [FW-1376], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of illegal commands has changed. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** INFO

## FW-1377

### Message

```
<timestamp>, [FW-1377], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of illegal commands has fallen below the low boundary. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

**Recommended Action** No action is required.

**Severity** INFO

## FW-1378

### Message

```
<timestamp>, [FW-1378], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the number of illegal commands has risen above the high boundary. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

**Recommended Action** Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

**Severity** WARNING

## FW-1379

### Message

```
<timestamp>, [FW-1379], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the number of illegal commands has changed from a value outside of the acceptable range to a value within the acceptable range. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

### Recommended Action

No action is required.

### Severity

INFO

## FW-1400

### Message

```
<timestamp>, [FW-1400], <sequence-number>,, INFO, <system-name>,
<Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the flash usage percentage has changed. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

### Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

### Severity

INFO

## FW-1401

### Message

```
<timestamp>, [FW-1401], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

### Probable Cause

Indicates that the flash usage percentage has fallen below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1402

### Message

```
<timestamp>, [FW-1402], <sequence-number>,, WARNING, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the flash usage percentage has risen above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

**Recommended Action** You might have to remove some unwanted files to create some flash space. Run the **saveCore** command to remove files from the kernel space.

**Severity** WARNING

## FW-1403

### Message

```
<timestamp>, [FW-1403], <sequence-number>,, INFO, <system-name>,
<Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

**Probable Cause** Indicates that the flash usage percentage has changed from a value outside of the acceptable range to a value within the acceptable range. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1424

### Message

```
<timestamp>, [FW-1424], <sequence-number>,, WARNING, <system-name>,
Switch status changed from <Previous state> to <Current state>.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because of a policy violation.

**Recommended Action** Run the **switchStatusShow** command to determine the policy violation.

**Severity** WARNING

## FW-1425

### Message

```
<timestamp>, [FW-1425], <sequence-number>,, INFO, <system-name>,
Switch status changed from <Bad state> to HEALTHY.
```

**Probable Cause** Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated.

**Recommended Action** No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

**Severity** INFO

## FW-1426

### Message

```
<timestamp>, [FW-1426], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Power supply: <Number Bad>
bad, <Number Missing> absent.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Replace the faulty or missing power supply.

**Severity** WARNING

## FW-1427

### Message

```
<timestamp>, [FW-1427], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Power supply: <Number Bad>
bad.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Replace the faulty power supply.

**Severity** WARNING

## FW-1428

### Message

```
<timestamp>, [FW-1428], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Power supply: <Number
Missing> absent.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Replace the missing power supply.

**Severity** WARNING

## FW-1429

### Message

```
<timestamp>, [FW-1429], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor: Power supplies are not
redundant.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

**Recommended Action** Rearrange the power supplies so that one is in an odd slot and other in an even slot to make them redundant.

**Severity** WARNING

## FW-1430

### Message

```
<timestamp>, [FW-1430], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Temperature sensor:
<Number Bad> bad.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **switchStatusPolicySet** command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.



**Recommended Action** Replace the FRU with the faulty temperature sensor.

**Severity** WARNING

## FW-1431

### Message

```
<timestamp>, [FW-1431], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Fan: <Number Bad> bad.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **switchStatusPolicySet** command. A fan is faulty when sensor value is not in the acceptable range or is faulty.

**Recommended Action** Replace the faulty or deteriorating fan FRUs.

**Severity** WARNING

## FW-1432

### Message

```
<timestamp>, [FW-1432], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor WWN: <Number Bad> bad.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty WWN cards is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Replace the faulty WWN card.

**Severity** WARNING

## FW-1433

### Message

```
<timestamp>, [FW-1433], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor CP: CP non-redundant.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty CPs is greater than or equal to the policy set by the **switchStatusPolicySet** command. The CPs are non-redundant.

If you power cycle a SilkWorm 24000 chassis in dual-domain configuration, and then reset the micro-switch of the active CP before the heartbeat is up, this will cause both CPs to come up in a non-redundant state.

<b>Recommended Action</b>	Run the <b>firmwareShow</b> command to verify that both CPs have compatible firmware levels. Run the <b>firmwareDownload</b> command to install the same level of firmware to both CPs. Replace any faulty CPs.  If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat was up on a power cycle, and the CPs came up non-redundant, then you should reboot the CPs again to clear the problem.
<b>Severity</b>	WARNING

## FW-1434

### Message

```
<timestamp>, [FW-1434], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Blade: <Number Bad> blade
failures.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Replace the faulty blade.

**Severity** WARNING

## FW-1435

### Message

```
<timestamp>, [FW-1435], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Flash: usage out of range.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the flash usage is out of range. The policy was set using the **switchStatusPolicySet** command.

**Recommended Action** Run the **saveCore** command to clear out the kernel flash. Refer to the *Fabric OS Command Reference Manual* for more information about this command.

**Severity** WARNING

## FW-1436

### Message

```
<timestamp>, [FW-1436], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Marginal ports: <Num of
marginal ports> marginal ports.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of marginal ports is greater than or equal to the policy set using the **switchStatusPolicySet** command. A port is faulty when the port value for Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, CRC error, Port state change or Buffer Limited Port is above the high boundary.

**Recommended Action** Replace any faulty or deteriorating SFPs.

**Severity** WARNING

## FW-1437

### Message

```
<timestamp>, [FW-1437], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Faulty ports: <Num of
faulty ports> faulty ports.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is considered faulty due to hardware failure such as a faulty SFP or port.

**Recommended Action** Replace any faulty or deteriorating SFPs.

**Severity** WARNING

## FW-1438

### Message

```
<timestamp>, [FW-1438], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Missing SFPs: <Num of
missing SFPs> missing SFPs.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the number of missing SFPs is greater than or equal to the policy set by the **switchStatusPolicySet** command.

**Recommended Action** Run the **switchStatusPolicySet** command to modify the SFP policy or to add SFPs to the empty ports.

**Severity** WARNING

## FW-1439

### Message

```
<timestamp>, [FW-1439], <sequence-number>,, WARNING, <system-name>,
Switch status change contributing factor Switch offline.
```

**Probable Cause** Indicates that the switch status is not in a healthy state. This occurred because the switch is offline.

**Recommended Action** Run the **switchEnable** command.

**Severity** WARNING

## FW-1440

### Message

```
<timestamp>, [FW-1440], <sequence-number>,, INFO, <system-name>,
<FRU label> state has changed to <FRU state>.
```

**Probable Cause** Indicates that the specified FRU's state has changed to "absent".

**Recommended Action** No action is required. Verify that the event was planned.

**Severity** INFO

## FW-1441

### Message

```
<timestamp>, [FW-1441], <sequence-number>,, INFO, <system-name>,
<FRU label> state has changed to <FRU state>.
```

**Probable Cause** Indicates that specified FRU's state has changed to "inserted". This means that a FRU is inserted but not powered on.

**Recommended Action** No action is required. Verify that the event was planned.

**Severity** INFO

## FW-1442

### Message

```
<timestamp>, [FW-1442], <sequence-number>,, INFO, <system-name>,
<FRU label> state has changed to <FRU state>.
```

**Probable Cause** Indicates that specified FRU's state has changed to "on".

**Recommended Action** No action is required. Verify that the event was planned.

**Severity** INFO

## FW-1443

### Message

```
<timestamp>, [FW-1443], <sequence-number>,, INFO, <system-name>,
<FRU label> state has changed to <FRU state>.
```

**Probable Cause** Indicates that specified FRU's state has changed to "off".

**Recommended Action** No action is required. Verify that the event was planned.

**Severity** INFO

## FW-1444

### Message

```
<timestamp>, [FW-1444], <sequence-number>,, WARNING, <system-name>,
<FRU label> state has changed to <FRU state>.
```

**Probable Cause** Indicates that the specified FRU's state has changed to "faulty".

**Recommended Action** Replace the FRU.

**Severity** WARNING



# HAM Error Messages

---

## HAM-1001

**Message**

```
<timestamp>, [HAM-1001], <sequence-number>,, CRITICAL, <system-name>, Standby CP is not Healthy, device <device name> status BAD, severity = <severity>
```

**Probable Cause**

Indicates that a standby CP device error is reported by the high-availability manager (HAM) Health Monitor, with a specific device and severity level. The severity level can be critical, major, or minor.

The active CP will continue to function normally, but because the standby CP is not healthy, nondisruptive failover is not possible.

**Recommended Action**

Reboot the standby CP blade by ejecting the card and reseating it.  
If the problem persists, replace the standby CP.

**Severity**

CRITICAL

## HAM-1002

**Message**

```
<timestamp>, [HAM-1002], <sequence-number>,, INFO, <system-name>, Standby CP is Healthy
```

**Probable Cause**

Indicates that all of the standby CP devices monitored by the HAM Health Monitor report no error.

**Recommended Action**

No action is required.

**Severity**

INFO

## HAM-1004

### Message

```
<timestamp>, [HAM-1004], <sequence-number>,, INFO, <system-name>,  
<Reboot Reason>
```

### Probable Cause

Indicates that the HAM module does not have any information about the reason for switch reboot.

This message records switch reboots that were not initiated by a user or by the **firmwareDownload** command. Some examples of errors that might initiate this message are hardware errors, software errors, compact flash errors, or memory errors. Because the firmware does not know the reason for this reboot, no extra information is displayed.

### Recommended Action

Check the error log on both CPs for additional messages that might indicate the reason for the reboot.

### Severity

INFO

## HAM-1005

### Message

```
<timestamp>, [HAM-1005], <sequence-number>,, CRITICAL, <system-  
name>, <error message>
```

### Probable Cause

This message is logged when HAM encounters a critical error.

### Recommended Action

Run the **haDump** command and capture output; then call your switch service provider.

### Severity

CRITICAL



# HAMK Error Messages

---

## HAMK-1001

### Message

```
<timestamp>, [HAMK-1001], <sequence-number>,, ERROR, <system-name>,  
Error notification received: <error information>
```

### Probable Cause

Indicates that the high-availability manager (HAM) kernel has been notified of a problem in the system. The source error itself is logged before this message is logged. Depending on the severity of the message logged, HAM will fail over for the SilkWorm 12000 or 24000 and reboot for all other platforms.

### Recommended Action

No action is required.

### Severity

ERROR

## HAMK-1002

### Message

```
<timestamp>, [HAMK-1002], <sequence-number>,, WARNING, <system-  
name>, Heartbeat down
```

### Probable Cause

Indicates that the active CP blade determined that the standby CP blade is down. This might happen as a result of an operator-initiated action such as **firmwareDownload**, if the standby CP blade is reset or removed, or as a result of an error in the standby CP blade.

### Recommended Action

Monitor the standby CP blade for a few minutes. If this message is due to a standby CP reboot, the message HAMK-1003 will display after the standby CP has completed the reboot successfully.

If the standby CP does not successfully connect to the active CP after 10 minutes, reboot the standby CP blade by ejecting the blade and reseating it.

### Severity

WARNING

## HAMK-1003

### Message

```
<timestamp>, [HAMK-1003], <sequence-number>,, INFO, <system-name>,  
Heartbeat up
```

### Probable Cause

Indicates that the active CP blade detects the standby CP blade. This message indicates that the standby CP blade is available to take over in case a failure happens on the active CP blade. This message is typically seen when the standby CP blade reboots.

### Recommended Action

No action is required. This message means that the standby CP is healthy.

### Severity

INFO

# HIL Error Messages

---

## HIL-1101

**Message**

```
<timestamp>, [HIL-1101], <sequence-number>,, ERROR, <system-name>,  
Slot <slot number> faulted, <nominal voltage> (<measured voltage>)  
is above threshold.
```

**Probable Cause**

Indicates that the blade voltage is above threshold. This message is specific to the SilkWorm 12000 or 24000.

**Recommended Action**

Replace the faulty blade.

**Severity**

ERROR

## HIL-1102

**Message**

```
<timestamp>, [HIL-1102], <sequence-number>,, ERROR, <system-name>,  
Slot <slot number> faulted, <nominal voltage> (<measured voltage>)  
is below threshold.
```

**Probable Cause**

Indicates that the blade voltage is below threshold. This message is specific to the SilkWorm 12000 or 24000.

**Recommended Action**

Replace the faulty blade.

**Severity**

ERROR

## HIL-1103

### Message

```
<timestamp>, [HIL-1103], <sequence-number>,, ERROR, <system-name>,
Blower <blower number> faulted, <nominal voltage> (<measured
voltage>) is above threshold.
```

### Probable Cause

Indicates that the fan voltage is above threshold.

### Recommended Action

Run the **psShow** command to verify the power supply status.

Try to reseal the faulty fan FRU and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

### Severity

ERROR

## HIL-1104

### Message

```
<timestamp>, [HIL-1104], <sequence-number>,, ERROR, <system-name>,
Blower <blower number> faulted, <nominal voltage> (<measured
voltage>) is below threshold.
```

### Probable Cause

Indicates that the fan voltage is below threshold.

### Recommended Action

Run the **psShow** command to verify the power supply status.

Try to reseal the faulty fan FRU and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

### Severity

ERROR

## HIL-1105

### Message

```
<timestamp>, [HIL-1105], <sequence-number>,, ERROR, <system-name>,
Switch error, <nominal voltage> (<measured voltage>) above
threshold.
```

### Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

### Recommended Action

For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.

For the SilkWorm 3900, replace the motherboard FRU.

For the SilkWorm 4100, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

**Severity** ERROR

## HIL-1106

### Message

```
<timestamp>, [HIL-1106], <sequence-number>,, ERROR, <system-name>,
Switch error, <nominal voltage> (<measured voltage>) below
threshold.
```

**Probable Cause** Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

**Recommended Action** For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.

For the SilkWorm 3900, replace the motherboard FRU.

For the SilkWorm 4100, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

**Severity** ERROR

## HIL-1107

### Message

```
<timestamp>, [HIL-1107], <sequence-number>,, CRITICAL, <system-
name>, Switch faulted, <nominal voltage> (<measured voltage>) above
threshold. System preparing for reset.
```

**Probable Cause** Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

**Recommended Action** For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.

For the SilkWorm 3900, replace the motherboard FRU.

For the SilkWorm 4100, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

**Severity** CRITICAL

## HIL-1108

### Message

```
<timestamp>, [HIL-1108], <sequence-number>,, CRITICAL, <system-name>, Switch faulted, <nominal voltage> (<measured voltage>) below threshold. System preparing for reset.
```

### Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

### Recommended Action

For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.

For the SilkWorm 3900, replace the motherboard FRU.

For the SilkWorm 4100, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

### Severity

CRITICAL

## HIL-1201

### Message

```
<timestamp>, [HIL-1201], <sequence-number>,, WARNING, <system-name>, Blower <blower number>, speed (<measured speed> RPM) above threshold.
```

### Probable Cause

Indicates that the fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

### Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

### Severity

WARNING

## HIL-1202

### Message

```
<timestamp>, [HIL-1202], <sequence-number>,, ERROR, <system-name>,
Blower <blower number> faulted, speed (<measured speed> RPM) below
threshold.
```

### Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold.

### Recommended Action

Replace the fan FRU.

### Severity

ERROR

## HIL-1203

### Message

```
<timestamp>, [HIL-1203], <sequence-number>,, ERROR, <system-name>,
Fan <fan number> faulted, speed (<measured speed> RPM) above
threshold.
```

### Probable Cause

Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

### Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

### Severity

ERROR

## HIL-1204

### Message

```
<timestamp>, [HIL-1204], <sequence-number>,, ERROR, <system-name>,
Fan <fan number> faulted, speed (<measured speed> RPM) below
threshold.
```

### Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

<b>Recommended Action</b>	For the SilkWorm 3900 and 4100, replace the fan FRU. For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.
<b>Severity</b>	ERROR

## HIL-1205

### Message

```
<timestamp>, [HIL-1205], <sequence-number>,, ERROR, <system-name>,
Fan <fan number> sensor <sensor number>, speed (<measured speed>
RPM) above threshold.
```

**Probable Cause** Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

<b>Recommended Action</b>	Run the <b>tempShow</b> command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.  Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.  Run the <b>fanShow</b> command to monitor the speed of the fan generating this error.  If the fan continues to generate this message, replace the fan FRU.
---------------------------	---

**Severity** ERROR

## HIL-1206

### Message

```
<timestamp>, [HIL-1206], <sequence-number>,, ERROR, <system-name>,
Fan <fan number> sensor <sensor number> , speed (<measured speed>
RPM) below threshold.
```

**Probable Cause** Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to nonbladed switches and is not applicable to the SilkWorm 12000 or 24000.

<b>Recommended Action</b>	For the SilkWorm 3900 and 4100, replace the fan FRU. For the SilkWorm 3250 and 3850, the entire switch must be replaced, because these switches do not have FRUs.
<b>Severity</b>	ERROR



## HIL-1301

### Message

```
<timestamp>, [HIL-1301], <sequence-number>,, ERROR, <system-name>,
1 blower failed. Replace failed blower assembly immediately.
```

### Probable Cause

Indicates that a fan FRU has failed. This message is often preceded by a low speed error message. This problem can quickly cause the switch to overheat.

### Recommended Action

Replace the faulty fan FRU immediately.

### Severity

ERROR

## HIL-1302

### Message

```
<timestamp>, [HIL-1302], <sequence-number>,, ERROR, <system-name>,
<count> blowers failed. Replace failed blower assemblies
immediately.
```

### Probable Cause

Indicates that multiple fan FRUs have failed on a switch. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1303

### Message

```
<timestamp>, [HIL-1303], <sequence-number>,, ERROR, <system-name>,
One fan failed. Replace failed fan FRU immediately.
```

### Probable Cause

Indicates that a fan FRU has failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRU immediately.

### Severity

ERROR

## HIL-1304

### Message

```
<timestamp>, [HIL-1304], <sequence-number>,, ERROR, <system-name>,  
Two fans failed. Replace failed fan FRUs immediately.
```

### Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1305

### Message

```
<timestamp>, [HIL-1305], <sequence-number>,, ERROR, <system-name>,  
One or two fan(s) failed. Replace failed fan FRU(s) immediately.
```

### Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1306

### Message

```
<timestamp>, [HIL-1306], <sequence-number>,, ERROR, <system-name>,  
Three fans failed. Replace failed fan FRUs immediately.
```

### Probable Cause

Indicates that three fan FRUs have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1307

### Message

```
<timestamp>, [HIL-1307], <sequence-number>,, ERROR, <system-name>,  
Four or five fans failed. Replace failed fan FRUs immediately.
```

### Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1308

### Message

```
<timestamp>, [HIL-1308], <sequence-number>,, ERROR, <system-name>,  
All fans failed. Replace failed fan FRUs immediately.
```

### Probable Cause

Indicates that all fans have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1309

### Message

```
<timestamp>, [HIL-1309], <sequence-number>,, ERROR, <system-name>,  
<count> fan FRU(s) failed. Replace failed fan FRU(s) immediately.
```

### Probable Cause

Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

### Recommended Action

Replace the faulty fan FRUs immediately.

### Severity

ERROR

## HIL-1401

### Message

```
<timestamp>, [HIL-1401], <sequence-number>,, WARNING, <system-name>, One fan FRU missing. Install fan FRU immediately.
```

### Probable Cause

Indicates that one fan FRU has been removed.

### Recommended Action

Install the missing fan FRU.

### Severity

WARNING

## HIL-1402

### Message

```
<timestamp>, [HIL-1402], <sequence-number>,, WARNING, <system-name>, Two fan FRUs missing. Install fan FRUs immediately.
```

### Probable Cause

Indicates that two fan FRUs have been removed.

### Recommended Action

Install the missing fan FRUs immediately.

### Severity

WARNING

## HIL-1403

### Message

```
<timestamp>, [HIL-1403], <sequence-number>,, WARNING, <system-name>, All fan FRUs missing. Install fan FRUs immediately.
```

### Probable Cause

Indicates that all fan FRUs have been removed.

### Recommended Action

Install the missing fan FRUs immediately.

### Severity

WARNING

## HIL-1404

### Message

```
<timestamp>, [HIL-1404], <sequence-number>,, WARNING, <system-name>, <count> fan FRU(s) missing. Install fan FRU(s) immediately.
```

### Probable Cause

Indicates that one or more fan FRUs have been removed.

### Recommended Action

Install the missing fan FRUs immediately.

### Severity

WARNING

## HIL-1501

### Message

```
<timestamp>, [HIL-1501], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, high temperature (<measured temperature>).
```

### Probable Cause

Indicates that the temperature of this blade has risen above the warning threshold.

### Recommended Action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

### Severity

WARNING

## HIL-1502

### Message

```
<timestamp>, [HIL-1502], <sequence-number>,, CRITICAL, <system-name>, Slot <slot number>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.
```

### Probable Cause

Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

### Recommended Action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

**Severity** CRITICAL

## HIL-1503

### Message

```
<timestamp>, [HIL-1503], <sequence-number>,, CRITICAL, <system-name>, Slot <slot number>, unit shutting down.
```

**Probable Cause** Indicates that the temperature of this blade has risen above the maximum threshold for at least two minutes. The blade is shut down to prevent further damage. This usually follows a high-temperature warning message.

### Recommended Action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

**Severity** CRITICAL

## HIL-1504

### Message

```
<timestamp>, [HIL-1504], <sequence-number>,, INFO, <system-name>, System within normal temperature specifications (<measured temperature> C).
```

**Probable Cause** Indicates that temperatures in the system have returned to normal.

**Recommended Action** No action is required.

**Severity** INFO

## HIL-1505

### Message

```
<timestamp>, [HIL-1505], <sequence-number>,, WARNING, <system-name>, High temperature (<measured temperature> C) exceeds environmental specifications.
```

### Probable Cause

Indicates that temperatures in the system have risen above the warning threshold.

### Recommended Action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

### Severity

WARNING

## HIL-1506

### Message

```
<timestamp>, [HIL-1506], <sequence-number>,, CRITICAL, <system-name>, High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 2 minutes.
```

### Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

### Recommended Action

Run the **fanShow** command to verify that all fans are working properly. Replace any deteriorating fan FRUs.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

### Severity

CRITICAL

## HIL-1507

### Message

```
<timestamp>, [HIL-1507], <sequence-number>,, CRITICAL, <system-name>, High temperature warning time expired. System preparing for shutdown.
```

### Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

<b>Recommended Action</b>	Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.  Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
<b>Severity</b>	CRITICAL

## HIL-1508

### Message

```
<timestamp>, [HIL-1508], <sequence-number>,, CRITICAL, <system-name>, Fan faulty warning time expired. System preparing for shutdown.
```

### Probable Cause

Indicates that temperatures in the system have remained above the critical threshold too long.

### Recommended Action

Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

### Severity

CRITICAL

## HIL-1509

### Message

```
<timestamp>, [HIL-1509], <sequence-number>,, CRITICAL, <system-name>, High temperature (<measured temperature> C). Warning time expired. System preparing for shutdown.
```

### Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

### Recommended Action

Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

### Severity

CRITICAL



## HIL-1601

### Message

```
<timestamp>, [HIL-1601], <sequence-number>,, ERROR, <system-name>,  
Using backup temperature sensor. Service immediately.
```

### Probable Cause

Indicates that temperature readings from the primary sensor are out of range.

### Recommended Action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan FRUs.

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

### Severity

ERROR

## HIL-1602

### Message

```
<timestamp>, [HIL-1602], <sequence-number>,, CRITICAL, <system-  
name>, All temperature sensors failed. Service immediately.
```

### Probable Cause

Indicates that temperature readings from all sensors are out of range.

### Recommended Action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan FRUs.

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

### Severity

CRITICAL



# HLO Error Messages

---

## HLO-1001

### Message

```
<timestamp>, [HLO-1001], <sequence-number>,, ERROR, <system-name>,  
Incompatible Inactivity timeout <dead timeout> from port <port  
number>, correct value <value>
```

### Probable Cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

### Recommended Action

The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

**Severity** ERROR

## HLO-1002

### Message

```
<timestamp>, [HLO-1002], <sequence-number>,, ERROR, <system-name>,  
Incompatible Hello timeout <HLO timeout> from port <port number>,  
correct value <correct value>
```

### Probable Cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

### Recommended Action

The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

**Severity** ERROR

## HLO-1003

### Message

```
<timestamp>, [HLO-1003], <sequence-number>,, ERROR, <system-name>,  
Invalid Hello received from port <port number>, Domain = <domain  
ID>, Remote Port = <remote port ID>
```

### Probable Cause

Indicates that the HLO message received was invalid and the frame was dropped. The Brocade switch will not accept FSPF frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the Brocade switch is connected to a switch from another manufacturer.

### Recommended Action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

### Severity

ERROR

# HMON Error Messages

---

## HMON-1001

**Message**

```
<timestamp>, [HMON-1001], <sequence-number>,, CRITICAL, <system-name>, <Failure description>
```

**Probable Cause**

Indicates that there was a problem reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

**Recommended Action**

Run the **firmwareDownload** command to reinstall the firmware to your switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**

CRITICAL



# HTTP Error Messages

---

## HTTP-1001

**Message**

```
<timestamp>, [HTTP-1001], <sequence-number>, , INFO, <system-name>, Switch PIDformat has changed to <current PID format>.
```

**Probable Cause**

Indicates that the PID format was changed by the administrator.

**Recommended Action**

No action is required. For more information on PID, format refer to the *Fabric OS Procedures Guide*.

**Severity**

INFO





# KSWD Error Messages

---

## KSWD-1003

**Message**

```
<timestamp>, [KSWD-1003], <sequence-number>,, WARNING, <system-name>, kSWD: <Warning message>
```

**Probable Cause**

Indicates a warning state within the system.

**Recommended Action**

No action is required.

**Severity**

WARNING



# KTRC Error Messages

---

## KTRC-1001

**Message**

```
<timestamp>, [KTRC-1001], <sequence-number>,, WARNING, <system-name>, Dump memory size exceeds dump file size
```

**Probable Cause**

Indicates that the dump memory size has exceeded the dump file size.

**Recommended Action**

No action is required.

**Severity**

WARNING

## KTRC-1002

**Message**

```
<timestamp>, [KTRC-1002], <sequence-number>,, INFO, <system-name>, Concurrent trace dumping.
```

**Probable Cause**

Indicates that the initial background dump has not completed.

**Recommended Action**

No action is required.

**Severity**

INFO

## KTRC-1003

**Message**

```
<timestamp>, [KTRC-1003], <sequence-number>,, ERROR, <system-name>, Cannot open ATA dump device
```

**Probable Cause** Indicates that the ATA dump driver is not initialized properly.

**Recommended Action** No action is required.

**Severity** ERROR

## KTRC-1004

### Message

```
<timestamp>, [KTRC-1004], <sequence-number>, , ERROR, <system-name>,
Cannot write to ATA dump device
```

**Probable Cause** Indicates that the write boundry in the ATA dump device has been exceeded.

**Recommended Action** No action is required.

**Severity** ERROR

## LOG Error Messages

---

### LOG-1000

**Message**

```
<timestamp>, [LOG-1000], <sequence-number>,, INFO, <system-name>,
Previous message repeated <repeat count> time(s)
```

**Probable Cause**

Indicates that the previous message repeated the number of times specified by the repeat count.

**Recommended Action**

No action is required.

**Severity**

INFO

### LOG-1001

**Message**

```
<timestamp>, [LOG-1001], <sequence-number>,, CRITICAL, <system-
name>, A log message was dropped
```

**Probable Cause**

Indicates that a log message was dropped. A trace dump file is created.

**Recommended Action**

Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

Run the **saveCore** command to FTP core files to a server location.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**

CRITICAL

### LOG-1002

**Message**

```
<timestamp>, [LOG-1002], <sequence-number>,, CRITICAL, <system-
name>, A log message was dropped
```

**Probable Cause** Indicates that a message was not recorded by the error logging system. A trace dump file is created. The message might still be visible through SNMP or other management tools.

**Recommended Action** Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.  
Run the **saveCore** command to FTP core files to a server location.  
Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** CRITICAL

# LSDB Error Messages

---

## LSDB-1001

### Message

```
<timestamp>, [LSDB-1001], <sequence-number>,, ERROR, <system-name>,  
Link State ID <link state ID> out of range
```

### Probable Cause

Indicates that the link state database ID is out of the acceptable range. The valid *link state ID* is the same as the valid domain ID, whose range is from 1 through 239. The switch will discard the record because it is not supported.

### Recommended Action

No action is required.

### Severity

ERROR

## LSDB-1002

### Message

```
<timestamp>, [LSDB-1002], <sequence-number>,, INFO, <system-name>,  
Local Link State Record reached max incarnation#
```

### Probable Cause

Indicates that the local link state database reached the maximum incarnations.

An “incarnation” is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled.

### Recommended Action

No action is required. The incarnation count will begin again at 1 after reaching 239.

### Severity

INFO

## LSDB-1003

### Message

```
<timestamp>, [LSDB-1003], <sequence-number>,, CRITICAL, <system-name>,  
No database entry for local Link State Record, domain <local domain>
```

**Probable Cause** Indicates that there is no local link state record entry in the link state database. The switch should always generate its own local entry when starting up.

An “incarnation” is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled. By disabling and enabling the switch, a new local link state record is generated.

**Recommended Action** Run the **switchDisable** and **switchEnable** commands. A new local link state record is generated during the switch enable.

**Severity** CRITICAL

## LSDB-1004

### Message

```
<timestamp>, [LSDB-1004], <sequence-number>,, WARNING, <system-name>, No Link State Record for domain <local domain>
```

**Probable Cause** Indicates that there is no link state record for the specified *local domain*.

**Recommended Action** No action is required. The other switch will pass the LSD when the fabric has become stable.

**Severity** WARNING



# MFIC Error Messages

---

## MFIC-1001

### Message

```
<timestamp>, [MFIC-1001], <sequence-number>,, ERROR, <system-name>,  
failure at sysmod_scn registry rc= <failure reason>
```

### Probable Cause

Indicates that the system is temporarily out of resources.

### Recommended Action

This message is often transitory, and requires no action.

If the message persists, run a switch **reboot** or an **haFailover** (if applicable).

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## MFIC-1002

### Message

```
<timestamp>, [MFIC-1002], <sequence-number>,, INFO, <system-name>,  
Chassis FRU header not programmed for switch NID, using defaults  
(applies only to FICON environments).
```

### Probable Cause

Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR). The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

### Recommended Action

No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

### Severity

INFO

## MFIC-1003

### Message

```
<timestamp>, [MFIC-1003], <sequence-number>,, WARNING, <system-name>, Effective Insistent domain ID for the fabric changed from <state> to <state>
```

### Probable Cause

Indicates that one or more switches joined the fabric with a different insistent domain ID (IDID) mode setting than the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for state are:

- On
- Off

### Recommended Action

IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required. IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure Tab > Fabric Subtab > Insistent Domain ID Mode** checkbox. The switch must be disabled to change the IDID mode.

**Severity** WARNING

# MPTH Error Messages

---

## MPTH-1001

**Message**

```
<timestamp>, [MPTH-1001], <sequence-number>,, ERROR, <system-name>,  
Null parent, lsId = <number>
```

**Probable Cause**

Indicates that a null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

**Recommended Action**

No action is required.

**Severity**

ERROR

## MPTH-1002

**Message**

```
<timestamp>, [MPTH-1002], <sequence-number>,, ERROR, <system-name>,  
Null lsrP, lsId = <ls ID number>
```

**Probable Cause**

Indicates that a link state record is null.

**Recommended Action**

No action is required.

**Severity**

ERROR

## MPTH-1003

**Message**

```
<timestamp>, [MPTH-1003], <sequence-number>,, WARNING, <system-  
name>, No minimum cost path in candidate list
```

**Probable Cause**

Indicates that the FSPF module has determined that there is no minimum cost path (MPATH) available in the candidate list.

<b>Recommended Action</b>	No action is required.
<b>Severity</b>	WARNING

# MQ Error Messages

---

## MQ-1004

### Message

```
<timestamp>, [MQ-1004], <sequence-number>,, ERROR, <system-name>,  
mqRead, queue = <queue name>, queue ID = <queue ID>, type = <message  
type>
```

### Probable Cause

Indicates that an unexpected message has been received in the specified message queue. The *queue name* is always fspf\_q. The *queue ID* and *message type* can be any of the following:

- 2 - MSG\_TX
- 3 - MSG\_INTR
- 4 - MSG\_STR
- 6 - MSG\_ASYNC\_IU
- 7 - MSG\_LINIT\_IU
- 8 - MSG\_RSCN
- 9 - MSG\_IOCTL
- 10 - MSG\_ACCEPT
- 11 - MSG\_IU\_FREE
- 12 - MSG\_US
- 13 - MSG\_EXT\_RSCN
- 14 - MSG\_RDTS\_START
- 15 - MSG\_RDTS\_SENDEF
- 16 - MSG\_RDTS\_RESET

### Recommended Action

No action is required.

### Severity

ERROR



# MS Error Messages

---

## MS-1001

### Message

```
<timestamp>, [MS-1001], <sequence-number>, , WARNING, <system-name>,
MS Platform Segmented port=<port number>(<reason for segmentation>
<domain>)
```

### Probable Cause

Indicates that the management server (MS) has segmented from another switch *domain* at the specified *port number* due to errors or inconsistencies defined in the MS platform service.

### Recommended Action

Reboot or power cycle the switch.

### Severity

WARNING

## MS-1002

### Message

```
<timestamp>, [MS-1002], <sequence-number>, , INFO, <system-name>, MS
Platform Service Unstable(<message string><domain number>)
```

### Probable Cause

The MS platform service is unstable.

The *<message string>* can be one of the following:

- *<No Resp for GCAP from>*  
The switch did not respond to a request for GCAP (MS Get Capabilities) command.  
Recommended Action: No action is required.
- *<GCAP sup but not PL by>*  
The GCAP (MS Get Capabilities) is supported but the flag for MS platform service is not set.  
Recommended Action: Set the flag for the MS Platform Service.
- *<GCAP Rejected (reason =BUSY) by>*  
The GCAP (MS Get Capabilities) is not supported by another switch.  
Recommended Action: Upgrade the firmware level on the switch to a level that supports RCS.
- *<Reject EXGPLDB from>*  
The request to the exchange platform database was rejected. The remote switch might be busy.  
Recommended Action: Wait a few minutes and try the command again.

The *<domain number>* is the target domain that caused error.

<b>Recommended Action</b>	<p>The recommended actions are as follows:</p> <ul style="list-style-type: none"> <li>• &lt;No Resp for GCAP from&gt; No action is required.</li> <li>• &lt;GCAP sup but not PL by&gt; Set the flag for the MS Platform Service.</li> <li>• &lt;GCAP Rejected (reason =BUSY) by&gt; Run the <b>firmwareDownload</b> command to upgrade the firmware level on the switch to a level that supports RCS. RCS is supported in Fabric OS v2.6, v3.1 and greater, and v4.1 and greater.</li> <li>• &lt;Reject EXGPLDB from&gt; Wait a few minutes and try the command again.</li> </ul>
<b>Severity</b>	INFO

## MS-1003

### Message

```
<timestamp>, [MS-1003], <sequence-number>,, INFO, <system-name>, MS
detected Unstable Fabric(<message string><domain number>).
```

### Probable Cause

Indicates that MS detected an unstable fabric; the command or operation might not be successfully completed. This message is often transitory.

The *message string* can be one of the following:

- <DOMAIN\_INVALID for a req from>  
The domain is invalid for a request.
- <No WWN for>  
Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

### Recommended Action

The fabric might be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

INFO

## MS-1004

### Message

```
<timestamp>, [MS-1004], <sequence-number>,, INFO, <system-name>, MS
detected ONLY 1 Domain(d=<domain in local resource>).
```

### Probable Cause

Indicates that MS detected an unstable count of domains in its own local resource.



<b>Recommended Action</b>	<p>This message is often transitory.</p> <p>The fabric might be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.</p> <p>Run the <b>fabricShow</b> command or the <b>secFabricShow</b> command to verify that the number of domains matches the Management Server known domains.</p> <p>If the message persists, run <b>supportFtp</b> (as needed) to set up automatic FTP transfers; then run the <b>supportSave</b> command and contact your switch service provider.</p>
<b>Severity</b>	INFO

## MS-1005

### Message

```
<timestamp>, [MS-1005], <sequence-number>,, ERROR, <system-name>,
MS Invalid CT Response from d=<domain>
```

<b>Probable Cause</b>	Indicates that MS received an invalid common transport (CT) response from switch <i>domain</i> . MS expects either a CT accept IU or a reject IU; MS received neither response, which violates the Fibre Channel Generic Services (FS-GS) specification.
-----------------------	--

<b>Recommended Action</b>	Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-FS standard.
<b>Severity</b>	ERROR

## MS-1006

### Message

```
<timestamp>, [MS-1006], <sequence-number>,, ERROR, <system-name>,
MS Unexpected iu_data_sz=<number of bytes>
```

<b>Probable Cause</b>	Indicates that MS received IU data of unexpected size. The IU payload and the IU size might be inconsistent with each other or with the command that is currently being processed.
-----------------------	--

<b>Recommended Action</b>	<p>Wait a few minutes and try the operation again.</p> <p>If the message persists, run <b>supportFtp</b> (as needed) to set up automatic FTP transfers; then run the <b>supportSave</b> command and contact your switch service provider.</p>
<b>Severity</b>	ERROR

## MS-1007

### Message

```
<timestamp>, [MS-1007], <sequence-number>,, INFO, <system-name>, MS
CT cmd=0x<CT command>, RCS reason=0x<RCS reason code>( <RCS reason
code string>)
```

### Probable Cause

Usage of the reliable commit service (RCS) has failed in MS. All switches in the fabric must be RCS capable for RCS to be used in the fabric.

The specified MS *Command Transport command* for an RCS request failed for the specified *RCS\_reason* and is described in more detail in the *RCS\_reason\_code\_string*.

### Recommended Action

Run the **rctInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

INFO

## MS-1008

### Message

```
<timestamp>, [MS-1008], <sequence-number>,, ERROR, <system-name>,
MS Failure while initializing <action>
```

### Probable Cause

MS failed while initializing the specified *action*.

The following *actions* might be displayed:

- <while writing to ms\_els\_q>  
MS is unable to write a message to the MS Extended Link Service Queue.
- <while inserting timer to timer list>  
MS is unable to add a timer to a resource.

### Recommended Action

This message is often transitory.

If the error persists, check the available memory on the switch using **memShow**.

### Severity

ERROR

## MS-1021

### Message

```
<timestamp>, [MS-1021], <sequence-number>,, ERROR, <system-name>,
MS WARMBOOT failure(FSS_MS_WARMINIT failed. Reason=<failure
reason>)
```

**Probable Cause** Indicates that the FSS warm recovery failed during WARM INIT phase of a reboot.

**Recommended Action** If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR



# NBFS Error Messages

---

## NBFS-1001

### Message

```
<timestamp>, [NBFS-1001], <sequence-number>,, INFO, <system-name>,  
Duplicate E_Port SCN from port <portnumber> in state <state change  
name> (<state change number>)
```

### Probable Cause

Indicates that a duplicate E\_Port State Change Number was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

### Recommended Action

No action is required.

### Severity

INFO

## NBFS-1002

### Message

```
<timestamp>, [NBFS-1002], <sequence-number>,, ERROR, <system-name>,  
Wrong input: <state name> to neighbor FSM, state <current state  
name>, port <portnumber>
```

### Probable Cause

Indicates that the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait

- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, it means the protocol implementation between two connected switches has problems.

**Recommended Action** Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is FULL, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

**Severity** ERROR

## NBFS-1003

### Message

```
<timestamp>, [NBFS-1003], <sequence-number>,, WARNING, <system-name>, DB_XMIT_SET flag not set in state <current state name>, input <state name>, port <portnumber>
```

**Probable Cause** Indicates that the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

**Recommended Action** No action is required. The Fabric OS auto recovers from this problem.

**Severity** WARNING

# NS Error Messages

---

## NS-1001

### Message

```
<timestamp>, [NS-1001], <sequence-number>,, WARNING, <system-name>,  
The response for request 0x<CT command code> from remote switch  
0x<Domain Id> is larger than the max frame size the remote switch  
can support!
```

### Probable Cause

Indicates that the response payload exceeds the maximum frame size the remote switch can handle.

### Recommended Action

Run the **firmwareDownload** command to upgrade the remote switch with v4.3 or higher, or v3.2 or higher, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

### Severity

WARNING

## NS-1002

### Message

```
<timestamp>, [NS-1002], <sequence-number>,, WARNING, <system-name>,  
Remote switch 0x<Domain Id> has firmware revision lower than 2.2:  
<Firmware Revision 1st character><Firmware Revision 2nd  
character><Firmware Revision 3rd character><Firmware Revision 4th  
character> which is not supported!
```

### Probable Cause

Indicates that the local switch cannot interact with the remote switch due to incompatible or obsolete firmware.

### Recommended Action

Run the **firmwareDownload** command to upgrade the remote switch to the latest level of firmware.

### Severity

WARNING

## NS-1003

### Message

```
<timestamp>, [NS-1003], <sequence-number>,, INFO, <system-name>,  
Number of local devices <Current local device count>, exceeds the  
standby can support <Local device count that standby can support>,  
can't send update.
```

### Probable Cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

### Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

### Severity

INFO

## NS-1004

### Message

```
<timestamp>, [NS-1004], <sequence-number>,, INFO, <system-name>,  
Number of local devices <Current local device count>, exceeds the  
standby can support <Local device count that standby can support>,  
can't sync.
```

### Probable Cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

### Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

### Severity

INFO



# PDM Error Messages

---

## PDM-1001

### Message

```
<timestamp>, [PDM-1001], <sequence-number>,, WARNING, <system-name>, Failed to parse the pdm config
```

### Probable Cause

Indicates that the PDM process could not parse the configuration file. This might be caused by a missing configuration file during the installation.

### Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## PDM-1002

### Message

```
<timestamp>, [PDM-1002], <sequence-number>,, WARNING, <system-name>, ipcInit failed
```

### Probable Cause

Indicates that the PDM process could not initialize the IPC mechanism.

### Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## PDM-1003

### Message

```
<timestamp>, [PDM-1003], <sequence-number>,, WARNING, <system-name>, pdm [-d] -S <service> -s <instance>
```

**Probable Cause** Indicates that a syntax error occurred when trying to launch the PDM process.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1004

### Message

```
<timestamp>, [PDM-1004], <sequence-number>,, WARNING, <system-name>, Memory shortage
```

**Probable Cause** Indicates that the PDM process ran out of memory.

**Recommended Action** Reboot or power cycle the switch.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1005

### Message

```
<timestamp>, [PDM-1005], <sequence-number>,, WARNING, <system-name>, FSS register failed
```

**Probable Cause** Indicates that the PDM failed to register to the FSS.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1006

### Message

```
<timestamp>, [PDM-1006], <sequence-number>,, WARNING, <system-name>, Too many files in sync.conf
```

**Probable Cause** Indicates that the configuration file *sync.conf* contains too many entries.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1007

### Message

```
<timestamp>, [PDM-1007], <sequence-number>,, WARNING, <system-name>, File not created: <file name>
```

**Probable Cause** Indicates that the PDM process failed to create the specified file name.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1008

### Message

```
<timestamp>, [PDM-1008], <sequence-number>,, WARNING, <system-name>, Failed to get the number of uports
```

**Probable Cause** Indicates that the PDM system call to `getcfg` failed.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1009

### Message

```
<timestamp>, [PDM-1009], <sequence-number>,, WARNING, <system-name>, Can't update Port Config Data
```

**Probable Cause** Indicates that the PDM system call to setcfg failed.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1010

### Message

```
<timestamp>, [PDM-1010], <sequence-number>,, WARNING, <system-name>, File open failed: <file name>
```

**Probable Cause** Indicates that the PDM process could not open the specified file name.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1011

### Message

```
<timestamp>, [PDM-1011], <sequence-number>,, WARNING, <system-name>, File read failed: <file name>
```

**Probable Cause** Indicates that the PDM process could not read data from the specified file name.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1012

### Message

```
<timestamp>, [PDM-1012], <sequence-number>,, WARNING, <system-name>, File write failed: <file name>
```

**Probable Cause** Indicates that the PDM process could not write data to the specified file name.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1013

### Message

```
<timestamp>, [PDM-1013], <sequence-number>,, WARNING, <system-name>, File empty: <File Name>
```

**Probable Cause** Indicates that the switch configuration file */etc/fabos/fabos.[0/1].conf* is empty.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1014

### Message

```
<timestamp>, [PDM-1014], <sequence-number>,, WARNING, <system-name>, Access sysmod failed
```

**Probable Cause** Indicates that a system call failed.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1017

### Message

```
<timestamp>, [PDM-1017], <sequence-number>,, CRITICAL, <system-name>, System (<Error Code>): <Command>
```

**Probable Cause** Indicates that a system call failed.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** CRITICAL

## PDM-1019

### Message

```
<timestamp>, [PDM-1019], <sequence-number>,, WARNING, <system-name>, File path or trigger too long
```

**Probable Cause** Indicates that one line of the *pdm.conf* file is too long.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## PDM-1020

### Message

```
<timestamp>, [PDM-1020], <sequence-number>,, WARNING, <system-name>, Long path name (<Path>/<File Name>), Skip
```

**Probable Cause** Indicates that the indicated file path name is too long. The limit is 49 characters.

**Recommended Action** Use short path name for the files to be replicated.

**Severity** WARNING

## PDM-1021

### Message

```
<timestamp>, [PDM-1021], <sequence-number>,, WARNING, <system-name>, Failed to download area port map
```

**Probable Cause** Indicates that a system call failed.

**Recommended Action** Run the **firmwareDownload** command to reinstall the firmware.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING





# PDTR Error Messages

---

## PDTR-1001

### Message

```
<timestamp>, [PDTR-1001], <sequence-number>,, INFO, <system-name>,  
< informational message >
```

### Probable Cause

Indicates that information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

### Recommended Action

Run the **pdShow** command to view the panic dump and core dump files.

### Severity

INFO

## PDTR-1002

### Message

```
<timestamp>, [PDTR-1002], <sequence-number>,, INFO, <system-name>,  
< informational message >
```

### Probable Cause

This message indicates that information has been written to the panic dump and core dump files and a trap generated. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

### Recommended Action

Run the **pdShow** command to view the panic dump and core dump files.

### Severity

INFO



# PLAT Error Messages

---

## PLAT-1000

### Message

```
<timestamp>, [PLAT-1000], <sequence-number>,, CRITICAL, <system-name>, <Function name> <Error string>
```

### Probable Cause

Indicates that nonrecoverable PCI errors have been detected.

### Recommended Action

The system will be faulted and might automatically reboot.

If the system does not reboot, then try issuing a **reboot** command from a command-line prompt.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

CRITICAL



# PORT Error Messages

---

## PORT-1003

### Message

```
<timestamp>, [PORT-1003], <sequence-number>,, WARNING, <system-name>, Port <port number> Faulted because of many Link Failures
```

### Probable Cause

Indicates that the specified port is now disabled because the link on this port had multiple failures that exceed an internally set threshold on the port. This problem is typically related to hardware.

### Recommended Action

Check and replace (if necessary) the hardware attached to both ends of the specified *port number*, including:

- the media (SFPs)
- the cable (fiber optic or copper ISL)
- the attached devices

When finished checking the hardware, perform **portEnable** to reenable the port.

### Severity

WARNING

## PORT-1004

### Message

```
<timestamp>, [PORT-1004], <sequence-number>,, INFO, <system-name>, Port <port number> could not be enabled because it is disabled due to long distance.
```

### Probable Cause

Indicates that the specified port could not be enabled because other ports in the same port group have used up the buffers available for this port group. This happens when other ports were configured to be long distance.

### Recommended Action

To enable this port, reconfigure the other E\_Ports so they are not long distance or change the other E\_Ports so they are not E\_Ports. This will free some buffers and allow this port to be enabled.

### Severity

INFO



# PS Error Messages

---

## PS-1000

**Message**

```
<timestamp>, [PS-1000], <sequence-number>,, CRITICAL, <system-name>, Failed to initialize Advanced Performance Monitoring.
```

**Probable Cause**

Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor has failed to initialize.

**Recommended Action**

The CP should reboot (or fail over) automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

**Severity**

CRITICAL

## PS-1001

**Message**

```
<timestamp>, [PS-1001], <sequence-number>,, INFO, <system-name>, Advanced Performance Monitoring configuration updated due to change in PID format
```

**Probable Cause**

Indicates that the PID format was changed.

**Recommended Action**

No action is required. Refer to the *Fabric OS Procedures Guide* for more information about the PID format.

**Severity**

INFO

## PS-1002

**Message**

```
<timestamp>, [PS-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize the tracing system for Advanced Performance Monitoring.
```

**Probable Cause** Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor tracing system has failed to initialize.

**Recommended Action** Tracing will not be available for Advanced Performance Monitoring, but other functions should function normally. To retry activating tracing, reboot (or fail over) the CP.

**Severity** ERROR

## PS-1003

### Message

```
<timestamp>, [PS-1003], <sequence-number>,, WARNING, <system-name>,
Failed to set end-to-end monitoring mask on ISL ports.
```

**Probable Cause** Indicates that the restoring configuration has attempted to set the end-to-end monitoring mask on at least one ISL port.

**Recommended Action** No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

**Severity** WARNING

## PS-1004

### Message

```
<timestamp>, [PS-1004], <sequence-number>,, WARNING, <system-name>,
Failed to add end-to-end monitors on ISL ports.
```

**Probable Cause** Indicates that the restoring configuration has attempted to add end-to-end monitors on at least one ISL port.

**Recommended Action** No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

**Severity** WARNING

## PS-1005

### Message

```
<timestamp>, [PS-1005], <sequence-number>,, WARNING, <system-name>,
ISL monitor on port <port> stopped counting because no hardware
resources are available
```

**Probable Cause** Indicates that ISL and end-to-end monitors have used up all the hardware resources.



<b>Recommended Action</b>	To resume counting, delete some end-to-end monitors sharing the same hardware resource pool.
<b>Severity</b>	WARNING



# PSWP Error Messages

---

## PSWP-1001

### Message

```
<timestamp>, [PSWP-1001], <sequence-number>,, INFO, <system-name>,  
Areas for port <wwn name corresponding to source port> and port <wwn  
name corresponding to destination port> are swapped. New area for  
port <wwn name corresponding to source port> is <wwn name  
corresponding to destination port> and port <new area corresponding  
to source wwn> is <new area corresponding to destination wwn>
```

### Probable Cause

Indicates that the **portSwap** command has been issued by the user.

### Recommended Action

No action is required.

### Severity

INFO

## PSWP-1002

### Message

```
<timestamp>, [PSWP-1002], <sequence-number>,, INFO, <system-name>,  
Port Swap feature enabled
```

### Probable Cause

Indicates that the **portSwap** feature has been enabled in the switch by the user.

### Recommended Action

No action is required.

### Severity

INFO

## PSWP-1003

### Message

```
<timestamp>, [PSWP-1003], <sequence-number>,, INFO, <system-name>,  
Port Swap feature disabled
```

### Probable Cause

Indicates that the **portSwap** feature has been disabled in the switch by the user.

### Recommended Action

No action is required.

### Severity

INFO

## PSWP-1004

### Message

```
<timestamp>, [PSWP-1004], <sequence-number>,, WARNING, <system-  
name>, Port Swap configuration does not match Chassis configuration  
for switch <switch number>. Erasing port swap tables...
```

### Probable Cause

Indicates that the **portSwap** configuration contradicts the chassis configuration.

### Recommended Action

Redefine the port swap configuration so that it matches the chassis configuration.

### Severity

WARNING

# RCS Error Messages

---

## RCS-1001

### Message

```
<timestamp>, [RCS-1001], <sequence-number>,, INFO, <system-name>,  
RCS has been disabled. Some switches in the fabric do not support  
this feature
```

### Probable Cause

Indicates that the RCS feature has been disabled on the local switch because not all switches in the fabric support RCS or the switch is in nonnative mode.

### Recommended Action

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

### Severity

INFO

## RCS-1002

### Message

```
<timestamp>, [RCS-1002], <sequence-number>,, INFO, <system-name>,  
RCS has been enabled.
```

### Probable Cause

Indicates that the RCS feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

### Recommended Action

No action is required.

### Severity

INFO

## RCS-1003

### Message

```
<timestamp>, [RCS-1003], <sequence-number>,, ERROR, <system-name>,
Failed to allocate memory: (<function name>)
```

### Probable Cause

Indicates that the specified RCS function failed to allocate memory.

### Recommended Action

This message is usually transitory. Wait a few minutes and retry the command.

Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

### Severity

ERROR

## RCS-1004

### Message

```
<timestamp>, [RCS-1004], <sequence-number>,, ERROR, <system-name>,
Application(<application name>) not registered.(<error string>)
```

### Probable Cause

Indicates that a specified application did not register with RCS.

### Recommended Action

Run the **haShow** command to view the HA state.

Run the **haDisable** and the **haEnable** commands.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

### Severity

ERROR

## RCS-1005

### Message

```
<timestamp>, [RCS-1005], <sequence-number>,, INFO, <system-name>,
State <RCS phase>, Application <Application ID> returned 0x<Reject
code>.
```

### Probable Cause

Indicates that a receiving switch is rejecting an RCS phase.

**Recommended Action** If the reject is in ACA phase, wait several minutes and then retry the operation from the sender switch.  
If the reject is in the SFC phase, check if the application license exists for the local domain and if the application data is compatible.

**Severity** INFO

## RCS-1006

### Message

```
<timestamp>, [RCS-1006], <sequence-number>,, INFO, <system-name>,  
State <RCS phase>, Application <Application ID>, RCS CM. Domain  
<Domain ID that sent the reject> returned 0x<Reject code>.
```

**Probable Cause** Indicates that a remote domain rejected an RCS phase initiated by an application on the local switch.

- If the reject phase is ACA, the remote domain might be busy and could not process the new request.
- If the reject phase is SFC, the data sent by the application might not be compatible or the domain does not have the license to support that application.

**Recommended Action** If the reject is in ACA phase, wait several minutes and then retry the operation.  
If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

**Severity** INFO





# RPCD Error Messages

---

## RPCD-1001

**Message**

```
<timestamp>, [RPCD-1001], <sequence-number>,, WARNING, <system-name>, Authentication Error: client \"<IP address>\" has bad credentials: <bad user name and password pair>
```

**Probable Cause**

Indicates that an authentication error was reported. The specified *client IP address* has faulty credentials.

**Recommended Action**

Enter the correct user name and password from the Fabric Access API host.

**Severity**

WARNING

## RPCD-1002

**Message**

```
<timestamp>, [RPCD-1002], <sequence-number>,, WARNING, <system-name>, Missing certificate file. Secure RPCd is disabled.
```

**Probable Cause**

Indicates that an SSL certificate is missing.

**Recommended Action**

To enable RPCD in secure mode, install a valid SSL certificate the switch.

**Severity**

WARNING

## RPCD-1003

**Message**

```
<timestamp>, [RPCD-1003], <sequence-number>,, WARNING, <system-name>, Permission denied accessing certificate file. Secure RPCd is disabled.
```

**Probable Cause** Indicates that the SSL certificate file configured on the switch could not be accessed because root did not have read access.

**Recommended Action** Change the file system access level for the certificate file to have root read-level access.

**Severity** WARNING

## RPCD-1004

### Message

```
<timestamp>, [RPCD-1004], <sequence-number>,, WARNING, <system-name>, Invalid certificate file. Secure RPCd is disabled.
```

**Probable Cause** Indicates that the SSL certificate file has been corrupted.

**Recommended Action** To enable RPCD in secure mode, install a valid SSL certificate the switch.

**Severity** WARNING

## RPCD-1005

### Message

```
<timestamp>, [RPCD-1005], <sequence-number>,, WARNING, <system-name>, Missing private key file. Secure RPCd is disabled.
```

**Probable Cause** Indicates that the private key file is missing.

**Recommended Action** Run the **pkiCreate** command to install a valid private key file.

**Severity** WARNING

## RPCD-1006

### Message

```
<timestamp>, [RPCD-1006], <sequence-number>,, WARNING, <system-name>, Permission denied accessing private key file. Secure RPCd is disabled.
```

**Probable Cause** Indicates that the private key file configured on the switch could not be accessed because root did not have read access.

**Recommended Action** Change the file system access level for the private key file to have root read-level access.

**Severity** WARNING

## RPCD-1007

### Message

```
<timestamp>, [RPCD-1007], <sequence-number>,, WARNING, <system-name>, Invalid private file. Secure RPCd is disabled.
```

**Probable Cause** Indicates that the private key file has been corrupted.

**Recommended Action** Run the **pkiCreate** command to install a valid private key file.

**Severity** WARNING



# RTWR Error Messages

---

## RTWR-1001

### Message

```
<timestamp>, [RTWR-1001], <sequence-number>,, ERROR, <system-name>,
RTWR <routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail
3>, 0x<detail 4>, 0x<detail 5>
```

### Probable Cause

Indicates that an error occurred in the RTWR. The message provides the name of the routine having the error, and more specific error information. Additionally, the values in details 1 through 5 might provide additional information.

### Recommended Action

No action is required.

### Severity

ERROR

## RTWR-1002

### Message

```
<timestamp>, [RTWR-1002], <sequence-number>,, WARNING, <system-
name>, RTWR <error message> 0x<detail1>, 0x<detail2>, 0x<detail3>,
0x<detail4>, 0x<detail5>
```

### Probable Cause

Indicates that the RTWR has exhausted the maximum number of retries sending data to the specified domain. Details are as follows:

- RTWRTransmit: Max retries exhausted
- detail1: Port
- detail2: Domain
- detail3: Retry Count
- detail4: Status
- detail5: Process ID

### Recommended Action

Run the **fabricShow** command to see if the specified domain ID is online.  
Enable the switch with the specified domain ID.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**    WARNING

# SCN Error Messages

---

## SCN-1001

### Message

```
<timestamp>, [SCN-1001], <sequence-number>,, CRITICAL, <system-name>, SCN queue overflow for process <daemon name>
```

### Probable Cause

Indicates that an attempt to write an SCN (state change notification) message to a specific queue has failed because the SCN queue for the specified *daemon name* is full. This might be caused by the daemon hanging or if the system is busy.

The valid values for *daemon name* are:

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

### Recommended Action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, run the **saveCore** command to send the core files using FTP to a secure server location.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** CRITICAL





# SEC Error Messages

---

## SEC-1001

### Message

```
<timestamp>, [SEC-1001], <sequence-number>,, ERROR, <system-name>,  
RCS process fails: <Reason text>
```

### Probable Cause

Indicates that the RCS (reliable commit service) process fails to complete. RCS is a reliable mechanism to transfer data from one switch to other switches within the fabric. This mechanism guarantees that either all switches commit to the new database or none of them update to the new database. This process can fail if one switch in the fabric is busy or in an error state that cannot accept the database.

### Recommended Action

RCS is used when the security database is changed by a command run by security (for example, **secPolicySave**, **secPolicyActivate**, or **secVersionReset**). If the switch is busy, the command might fail the first time only; retry after the first fail.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1002

### Message

```
<timestamp>, [SEC-1002], <sequence-number>,, ERROR, <system-name>,  
Security data fails: <Reason Text>
```

### Probable Cause

Indicates that the receiving switch fails to validate the security database sent from the primary FCS switch. This could result from the data package being corrupted, the time stamp on the package is out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure might be due to an internal error, such as losing the primary public key or an invalid database.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. The error might also be a result of an internal corruption or a hacker attack to the secure fabric.

**Severity** ERROR

## SEC-1003

### Message

```
<timestamp>, [SEC-1003], <sequence-number>,, WARNING, <system-name>, Fail to download security data to domain <Domain number> after <Number of retries> retries
```

**Probable Cause** Indicates that the specified domain number failed to download security data after the specified number of attempts. The primary switch will segment the failed switch after 30 tries. The failed switch might have had some internal error and failed to accept the database download.

**Recommended Action** Reset the version stamp on the switch to 0 and then rejoin the switch to the fabric.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## SEC-1005

### Message

```
<timestamp>, [SEC-1005], <sequence-number>,, INFO, <system-name>, Primary FCS receives data request from domain <Domain number>
```

**Probable Cause** Indicates that the primary FCS received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

**Recommended Action** Check the fabric status, using **secFabricShow** to verify that the fabric is not being attacked by unauthorized users.

**Severity** INFO

## SEC-1006

### Message

```
<timestamp>, [SEC-1006], <sequence-number>,, WARNING, <system-name>, Security statistics error: Failed to reset due to invalid <data>.
```

**Probable Cause** Indicates that invalid data has been received for any statistic-related command for security (**secStatsShow** or **secStatsReset**). The counter is updated automatically when a security violation occurs. This message might also occur if the updating counter fails.

**Recommended Action** If the message is the result of a user command, retry the statistic command.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## SEC-1007

### Message

```
<timestamp>, [SEC-1007], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address
of the violating host> tries to establish API connection.
```

**Probable Cause** Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

**Recommended Action** Check for unauthorized access to the switch through the API connection.

**Severity** INFO

## SEC-1008

### Message

```
<timestamp>, [SEC-1008], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address
of the violating host> tries to establish HTTP connection.
```

**Probable Cause** Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

**Recommended Action** Check for unauthorized access to the switch through the HTTP connection.

**Severity** INFO

## SEC-1009

### Message

```
<timestamp>, [SEC-1009], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address
of the violating host> tries to establish TELNET connection.
```

**Probable Cause** Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

**Recommended Action** Check for unauthorized access to the switch through the telnet connection.

**Severity** INFO

## SEC-1016

### Message

```
<timestamp>, [SEC-1016], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address
of the violating host> tries to establish SSH connection.
```

**Probable Cause** Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

**Recommended Action** Check for unauthorized access to the switch through the SSH connection.

**Severity** INFO

## SEC-1022

### Message

```
<timestamp>, [SEC-1022], <sequence-number>,, WARNING, <system-
name>, Failed to <operation> PKI objects.
```

**Probable Cause** Indicates that the security server failed to generate or validate either the public or private key pair or the CSR.

**Recommended Action** Run the **pkiShow** command and verify that all PKI objects exist on the switch. If the private key does not exist, follow the steps for re-creating PKI objects, outlined in the *Secure Fabric OS User's Guide*. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

**Severity** WARNING

## SEC-1024

### Message

```
<timestamp>, [SEC-1024], <sequence-number>,, INFO, <system-name>,
The <DB name> security database is too large to fit in flash.
```

**Probable Cause** Indicates that the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

**Recommended Action** Reduce the size of the security database by reducing the number of entries within each policy.

**Severity** INFO

## SEC-1025

### Message

```
<timestamp>, [SEC-1025], <sequence-number>,, ERROR, <system-name>,
Invalid IP <IP address>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1026

### Message

```
<timestamp>, [SEC-1026], <sequence-number>,, ERROR, <system-name>,
Not a valid format [<switch member ID>] for switch member.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1028

### Message

```
<timestamp>, [SEC-1028], <sequence-number>,, ERROR, <system-name>,
No name is specified.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1029

### Message

```
<timestamp>, [SEC-1029], <sequence-number>,, ERROR, <system-name>,
Invalid character in <policy name>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1030

### Message

```
<timestamp>, [SEC-1030], <sequence-number>,, ERROR, <system-name>,
The length of the name invalid.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1031

### Message

```
<timestamp>, [SEC-1031], <sequence-number>,, WARNING, <system-
name>, Current security policy DB cannot be supported by standby.
CPs will go out of sync.
```

**Probable Cause** The security database size is not supported by the standby CP.

**Recommended Action** Reduce the databas size by reducing the security policy size.

**Severity** WARNING

## SEC-1032

### Message

```
<timestamp>, [SEC-1032], <sequence-number>,, ERROR, <system-name>,
Empty FCS list is not allowed.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1033

### Message

```
<timestamp>, [SEC-1033], <sequence-number>,, ERROR, <system-name>,
The * symbol is only used to create the policy. Command terminated
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1034

### Message

```
<timestamp>, [SEC-1034], <sequence-number>,, ERROR, <system-name>,
Invalid member <policy member>.
```

**Probable Cause** Indicates that the input list has an invalid member.

**Recommended Action** Verify your member names, and input the correct information.

**Severity** ERROR

## SEC-1035

### Message

```
<timestamp>, [SEC-1035], <sequence-number>,, ERROR, <system-name>,
Invalid device WWN <Device WWN>.
```

**Probable Cause** Indicates that the specified WWN is invalid.

**Recommended Action** Enter the correct WWN value.

**Severity** ERROR

## SEC-1036

### Message

```
<timestamp>, [SEC-1036], <sequence-number>,, ERROR, <system-name>,
Invalid device name <device name>. Missing colon
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1037

### Message

```
<timestamp>, [SEC-1037], <sequence-number>,, ERROR, <system-name>,
Invalid WWN format <Invalid WWN>.
```



**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1038

### Message

```
<timestamp>, [SEC-1038], <sequence-number>,, ERROR, <system-name>,
Invalid domain <Domain ID>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1040

### Message

```
<timestamp>, [SEC-1040], <sequence-number>,, ERROR, <system-name>,
Invalid portlist (<port list>). Cannot combine * with port member in
the same portlist.
```

**Probable Cause** Indicates that the port list contains the wildcard asterisk (\*) character.

**Recommended Action** You cannot use the asterisk in a port list. Enter the port list values without any wildcards.

**Severity** ERROR

## SEC-1041

### Message

```
<timestamp>, [SEC-1041], <sequence-number>,, ERROR, <system-name>,  
Invalid port member <port member> in portlist (<port list>).  
<Reason>.
```

### Probable Cause

Indicates that the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

### Recommended Action

Use valid syntax when entering port members.

### Severity

ERROR

## SEC-1042

### Message

```
<timestamp>, [SEC-1042], <sequence-number>,, ERROR, <system-name>,  
Invalid area member <port member> in portlist (<Port list>). Out of  
range (<Minimum value> - <Maximum value>).
```

### Probable Cause

Indicates that the specified area member is not within the minimum and maximum values.

### Recommended Action

Use valid syntax when entering area numbers.

### Severity

ERROR

## SEC-1043

### Message

```
<timestamp>, [SEC-1043], <sequence-number>,, ERROR, <system-name>,  
Invalid port range <Minimum> - <Maximum>.
```

### Probable Cause

Indicates that the specified port is not within the minimum and maximum range.

### Recommended Action

Use valid syntax when entering port ranges.

### Severity

ERROR

## SEC-1044

### Message

```
<timestamp>, [SEC-1044], <sequence-number>,, ERROR, <system-name>,
Duplicate member <member ID> in (<List>).
```

### Probable Cause

Indicates that the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

### Recommended Action

Do not specify any duplicates.

### Severity

ERROR

## SEC-1045

### Message

```
<timestamp>, [SEC-1045], <sequence-number>,, ERROR, <system-name>,
Too many port members.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1046

### Message

```
<timestamp>, [SEC-1046], <sequence-number>,, ERROR, <system-name>,
Empty list.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1049

### Message

```
<timestamp>, [SEC-1049], <sequence-number>,, ERROR, <system-name>,  
Invalid switch name <switch name>.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1050

### Message

```
<timestamp>, [SEC-1050], <sequence-number>,, ERROR, <system-name>,  
There are more than one switches with the same name <switch name> in  
the fabric.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1051

### Message

```
<timestamp>, [SEC-1051], <sequence-number>,, ERROR, <system-name>,  
Missing brace for port list <port list>.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1052

### Message

```
<timestamp>, [SEC-1052], <sequence-number>,, ERROR, <system-name>,
Invalid input.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1053

### Message

```
<timestamp>, [SEC-1053], <sequence-number>,, ERROR, <system-name>,
Invalid pFCS list <pFCS list>
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1054

### Message

```
<timestamp>, [SEC-1054], <sequence-number>,, ERROR, <system-name>,
Invalid FCS list length <list length>
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1055

### Message

```
<timestamp>, [SEC-1055], <sequence-number>,, ERROR, <system-name>,
Invalid FCS list <WWN list>
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1056

### Message

```
<timestamp>, [SEC-1056], <sequence-number>,, ERROR, <system-name>,
Invalid postion <New position>. Only <Number of members in FCS list>
members in list.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1057

### Message

```
<timestamp>, [SEC-1057], <sequence-number>,, ERROR, <system-name>,
No change. Both positions are the same.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1059

### Message

```
<timestamp>, [SEC-1059], <sequence-number>,, ERROR, <system-name>,
Fail to <operation, e.g., save, delete, etc.,> <named item> to
flash.
```

**Probable Cause** Indicates that the operation failed when writing to flash.

**Recommended Action** Run the **saveCore** command to move files off the kernel flash.

**Severity** ERROR

## SEC-1062

### Message

```
<timestamp>, [SEC-1062], <sequence-number>,, ERROR, <system-name>,
Invalid number of Domains in Domain List.
```

**Probable Cause** Indicates either that no domains or domains more than the maximum are specified.

**Recommended Action** Enter the correct number of domains.

**Severity** ERROR

## SEC-1063

### Message

```
<timestamp>, [SEC-1063], <sequence-number>,, ERROR, <system-name>,
Failed to reset statistics.
```

**Probable Cause** Indicates that either the type or the domains specified are invalid.

**Recommended Action** Enter valid input.

**Severity** ERROR

## SEC-1064

### Message

```
<timestamp>, [SEC-1064], <sequence-number>,, ERROR, <system-name>,  
Failed to sign message.
```

**Probable Cause** Indicates that the PKI objects on the switch are not in a valid state and the signature operation failed.

**Recommended Action** Run the **pkiShow** command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

**Severity** ERROR

## SEC-1065

### Message

```
<timestamp>, [SEC-1065], <sequence-number>,, ERROR, <system-name>,  
Invalid character in list.
```

**Probable Cause** Indicates that the input list has an invalid character.

**Recommended Action** Enter valid input.

**Severity** ERROR

## SEC-1069

### Message

```
<timestamp>, [SEC-1069], <sequence-number>,, ERROR, <system-name>,  
Security Database is corrupted.
```

**Probable Cause** Indicates that the security database is corrupted for unknown reasons.



**Recommended Action** Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1071

### Message

```
<timestamp>, [SEC-1071], <sequence-number>,, ERROR, <system-name>,
No new data to apply.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1072

### Message

```
<timestamp>, [SEC-1072], <sequence-number>,, ERROR, <system-name>,
<Policy type> Policy List is Empty!
```

**Probable Cause** Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

**Recommended Action** Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1073

### Message

```
<timestamp>, [SEC-1073], <sequence-number>,, ERROR, <system-name>,
No FCS policy in list!
```

**Probable Cause** Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

**Recommended Action** Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1074

### Message

```
<timestamp>, [SEC-1074], <sequence-number>,, ERROR, <system-name>,  
Cannot execute the command on this switch. Please check the secure  
mode and FCS status.
```

**Probable Cause** Indicates that a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have required FCS privilege.

**Recommended Action** If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has required privilege, that is, either a backup FCS or primary FCS.

**Severity** ERROR

## SEC-1075

### Message

```
<timestamp>, [SEC-1075], <sequence-number>,, ERROR, <system-name>,  
Fail to <operation> new policy set on all switches.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1076

### Message

```
<timestamp>, [SEC-1076], <sequence-number>,, ERROR, <system-name>,  
NoNodeWWNZoning option has been changed.
```

**Probable Cause** Indicates that the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

**Recommended Action** Reenable the current zone configuration for the change to take effect.

**Severity** ERROR

## SEC-1077

### Message

```
<timestamp>, [SEC-1077], <sequence-number>,, ERROR, <system-name>,
Failed to activate new policy set on all switches.
```

**Probable Cause** Indicates that the policy could not be activated. Reasons can be no memory, switch busy, and so on.

**Recommended Action** Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

**Severity** ERROR

## SEC-1078

### Message

```
<timestamp>, [SEC-1078], <sequence-number>,, ERROR, <system-name>,
No new data to abort.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1079

### Message

```
<timestamp>, [SEC-1079], <sequence-number>,, ERROR, <system-name>,
Invalid policy name <Policy name>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1080

### Message

```
<timestamp>, [SEC-1080], <sequence-number>,, ERROR, <system-name>,
Operation denied. Please, use secModeEnable command.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1081

### Message

```
<timestamp>, [SEC-1081], <sequence-number>,, ERROR, <system-name>,
DCC_POLICY is not allowed without a unique identifier.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1082

### Message

```
<timestamp>, [SEC-1082], <sequence-number>,, ERROR, <system-name>,
Failed to create <policy name> policy.
```

**Probable Cause** Indicates that the security policy was not created due to faulty input or low resources.

**Recommended Action** Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

**Severity** ERROR

## SEC-1083

### Message

```
<timestamp>, [SEC-1083], <sequence-number>,, ERROR, <system-name>,
Name already exists.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1084

### Message

```
<timestamp>, [SEC-1084], <sequence-number>,, ERROR, <system-name>,
Name exists for different type <Policy name>.
```

**Probable Cause** Indicates that the specified policy already exists.

**Recommended Action** No action is required.

**Severity** ERROR

## SEC-1085

### Message

```
<timestamp>, [SEC-1085], <sequence-number>,, ERROR, <system-name>,
Failed to create <Policy name>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1086

### Message

```
<timestamp>, [SEC-1086], <sequence-number>,, ERROR, <system-name>,
The security database is too large to fit in flash.
```

**Probable Cause** Indicates that the security database has more data than the flash can accommodate.

**Recommended Action** Reduce the number of entries in some policies to decrease the security database size.

**Severity** ERROR

## SEC-1088

### Message

```
<timestamp>, [SEC-1088], <sequence-number>,, ERROR, <system-name>,
Cannot execute the command. Please try later.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1089

### Message

```
<timestamp>, [SEC-1089], <sequence-number>,, ERROR, <system-name>,
Policy name <Policy name> not found. Please, use secPolicyCreate.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1090

### Message

```
<timestamp>, [SEC-1090], <sequence-number>,, ERROR, <system-name>,
SCC list contains FCS member. Please remove member from the FCS
policy first.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1091

### Message

```
<timestamp>, [SEC-1091], <sequence-number>,, ERROR, <system-name>,
No policy to remove.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1092

### Message

```
<timestamp>, [SEC-1092], <sequence-number>,, ERROR, <system-name>,
<Policy name> Name not found.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1093

### Message

```
<timestamp>, [SEC-1093], <sequence-number>,, ERROR, <system-name>,  
New FCS list must have at least one member in common with current  
FCS list.
```

**Probable Cause** Indicates that the new FCS list does not have a common member with the existing FCS list.

**Recommended Action** Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

**Severity** ERROR

## SEC-1094

### Message

```
<timestamp>, [SEC-1094], <sequence-number>,, ERROR, <system-name>,  
Policy member not found.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1095

### Message

```
<timestamp>, [SEC-1095], <sequence-number>,, ERROR, <system-name>,  
Deleting FCS policy is not allowed.
```



**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1096

### Message

```
<timestamp>, [SEC-1096], <sequence-number>,, ERROR, <system-name>,
Failed to delete <Policy name>. <Reason text>
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1097

### Message

```
<timestamp>, [SEC-1097], <sequence-number>,, ERROR, <system-name>,
Cannot find <active or defined> policy set.
```

**Probable Cause** Indicates that the specified policy could not be found.

**Recommended Action** If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1098

### Message

```
<timestamp>, [SEC-1098], <sequence-number>,, ERROR, <system-name>,
No <active or defined> FCS list.
```

**Probable Cause** Indicates that the specified policy could not be found.

**Recommended Action** Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1099

### Message

```
<timestamp>, [SEC-1099], <sequence-number>,, ERROR, <system-name>,
Please enable your switch before running secModeEnable.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1100

### Message

```
<timestamp>, [SEC-1100], <sequence-number>,, ERROR, <system-name>,
FCS switch present. Command terminated.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1101

### Message

```
<timestamp>, [SEC-1101], <sequence-number>,, ERROR, <system-name>,
Failed to enable security on all switches. Please retry later.
```

**Probable Cause** Indicates that the security enable failed on the fabric because one or more switches in the fabric are busy.

**Recommended Action** Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

**Severity** ERROR

## SEC-1102

### Message

```
<timestamp>, [SEC-1102], <sequence-number>,, ERROR, <system-name>,
Fail to download <security data>.
```

**Probable Cause** Indicates that the switch failed to download certificate, security database, or policies. This can happen when switch does not get enough resources to complete the operation, fabric has not stabilized, or policy database is an invalid format.

**Recommended Action** Wait for fabric to become stable and then retry the operation. If the policy database is in an illegal format (with **configDownload**), correct the format and retry the operation.

**Severity** ERROR

## SEC-1104

### Message

```
<timestamp>, [SEC-1104], <sequence-number>,, ERROR, <system-name>,
Fail to get primary <Certificate or public key>.
```

**Probable Cause** Indicates that the switch failed to get either the primary certificate or a primary public key.

**Recommended Action** Verify that the primary switch has a valid certificate installed and retry the operation. If a valid certificate is not installed, install a certificate by following the procedure specified in the *Secure Fabric OS User's Guide*.

**Severity** ERROR

## SEC-1105

### Message

```
<timestamp>, [SEC-1105], <sequence-number>,, ERROR, <system-name>,
Fail to disable secure mode on all switches.
```

**Probable Cause** Indicates that the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

**Recommended Action** Run the **secFabricShow** to verify that all switches in the fabric are in the ready state. Retry the command when all switches are READY.

**Severity** ERROR

## SEC-1106

### Message

```
<timestamp>, [SEC-1106], <sequence-number>,, ERROR, <system-name>,
Failed to sign message data.
```

**Probable Cause** Indicates that some PKI objects on the switch are not in a valid state, and a signature operation failed.

**Recommended Action** Run the **pkiShow** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS User's Guide*.

**Severity** ERROR

## SEC-1107

### Message

```
<timestamp>, [SEC-1107], <sequence-number>,, INFO, <system-name>,
Stamp is 0.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1108

### Message

```
<timestamp>, [SEC-1108], <sequence-number>,, ERROR, <system-name>,
Fail to reset stamp on all switches.
```

**Probable Cause** Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

**Recommended Action** Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

**Severity** ERROR

## SEC-1110

### Message

```
<timestamp>, [SEC-1110], <sequence-number>,, ERROR, <system-name>,
FCS list must be the first entry in the [Defined Security policies]
section. Fail to download defined database.
```

**Probable Cause** Indicates that a security policy download is attempted with a defined policy that does not have the FCS policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

**Recommended Action** Download a correct configuration with the FCS policy as the first policy in the defined security database.

**Severity** ERROR

## SEC-1111

### Message

```
<timestamp>, [SEC-1111], <sequence-number>,, ERROR, <system-name>,
New defined FCS list must have at least one member in common with
current active FCS list. Fail to download defined database.
```

**Probable Cause** Indicates that the defined and active FCS policy list failed to have at least one member in common.

**Recommended Action** A new FCS policy list must have at least one member in common with the previous FCS policy.

**Severity** ERROR

## SEC-1112

### Message

```
<timestamp>, [SEC-1112], <sequence-number>,, ERROR, <system-name>,
FCS list must be the first entry in the Active Security policies,
and the same as the current active FCS list in the switch.
```

### Probable Cause

Indicates that either a security policy download is attempted with an active policy that does not have the FCS policy as the first policy or the FCS policy is not same as the current FCS policy on the switch.

### Recommended Action

Make sure that the new FCS policy is the same as the current FCS policy on the switch.

### Severity

ERROR

## SEC-1115

### Message

```
<timestamp>, [SEC-1115], <sequence-number>,, ERROR, <system-name>,
No primary FCS to failover.
```

### Probable Cause

Indicates that during an attempted **secFcsFailover**, no primary FCS is present in the fabric.

### Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

### Severity

ERROR

## SEC-1116

### Message

```
<timestamp>, [SEC-1116], <sequence-number>,, ERROR, <system-name>,
Fail to commit failover.
```

### Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1117

### Message

```
<timestamp>, [SEC-1117], <sequence-number>,, INFO, <system-name>,
Fail to set <data>.
```

### Probable Cause

Indicates that the switch failed to save the data received by the primary FCS switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

### Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

### Severity

INFO

## SEC-1118

### Message

```
<timestamp>, [SEC-1118], <sequence-number>,, INFO, <system-name>,
Fail to set SNMP string.
```

### Probable Cause

Indicates that the SNMP string could not be set.

### Recommended Action

Usually this problem is transient. Retry the command.

### Severity

INFO

## SEC-1119

### Message

```
<timestamp>, [SEC-1119], <sequence-number>,, INFO, <system-name>,
Secure mode has been enabled.
```

### Probable Cause

Indicates that the secure Fabric OS was enabled by the **secModeEnable** command.

### Recommended Action

Verify that the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1121

### Message

```
<timestamp>, [SEC-1121], <sequence-number>,, ERROR, <system-name>,
Time is out of range when <text>.
```

### Probable Cause

Indicates that the time on the switch is not synchronized with the primary FCS, the data packet is corrupted, or a replay attack is launched on the switch.

### Recommended Action

Verify that the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

### Severity

ERROR

## SEC-1122

### Message

```
<timestamp>, [SEC-1122], <sequence-number>,, INFO, <system-name>,
Error code: <Domain ID>, <Error message>.
```

### Probable Cause

Indicates that one of the switches in the fabric could not communicate with the primary FCS.

### Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

### Severity

INFO

## SEC-1123

### Message

```
<timestamp>, [SEC-1123], <sequence-number>,, INFO, <system-name>,
Security database downloaded by Primary FCS.
```

### Probable Cause

Indicates that the security database was successfully downloaded from the primary FCS.

### Recommended Action

No action is required.

### Severity

INFO



## SEC-1124

**Message**

```
<timestamp>, [SEC-1124], <sequence-number>,, INFO, <system-name>,  
Secure Mode is off.
```

**Probable Cause**

Indicates that a secure mode disable is attempted in a non-secure fabric.

**Recommended Action**

No action is required.

**Severity**

INFO

## SEC-1126

**Message**

```
<timestamp>, [SEC-1126], <sequence-number>,, INFO, <system-name>,  
Secure mode has been disabled.
```

**Probable Cause**

Indicates that a secure mode disable operation completed successfully.

**Recommended Action**

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity**

INFO

## SEC-1130

**Message**

```
<timestamp>, [SEC-1130], <sequence-number>,, INFO, <system-name>,  
The Primary FCS has failed over to a new switch.
```

**Probable Cause**

Indicates that an FCS failover operation was completed successfully.

**Recommended Action**

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity**

INFO

## SEC-1135

### Message

```
<timestamp>, [SEC-1135], <sequence-number>,, INFO, <system-name>,
Secure fabric version stamp has been reset.
```

### Probable Cause

Indicates that the version stamp of the secure fabric is reset.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1136

### Message

```
<timestamp>, [SEC-1136], <sequence-number>,, ERROR, <system-name>,
Failed to verify signature <data type, MUA, policy, etc.,>.
```

### Probable Cause

Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

### Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

### Severity

ERROR

## SEC-1137

### Message

```
<timestamp>, [SEC-1137], <sequence-number>,, ERROR, <system-name>,
No signature in <data type, MUA, policy, etc.,>.
```

### Probable Cause

Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

**Severity** ERROR

## SEC-1138

### Message

```
<timestamp>, [SEC-1138], <sequence-number>,, INFO, <system-name>,
Security database download received from Primary FCS.
```

**Probable Cause** Indicates that a non-primary FCS switch received a security database download.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-1139

### Message

```
<timestamp>, [SEC-1139], <sequence-number>,, ERROR, <system-name>,
The RSNMP_POLICY cannot exist without the WSNMP_POLICY.
```

**Probable Cause** Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

**Severity** ERROR

## SEC-1142

### Message

```
<timestamp>, [SEC-1142], <sequence-number>,, INFO, <system-name>,
Reject new policies. <reason text>.
```

**Probable Cause** Indicates that the new polices are rejected due to the reason specified.

**Recommended Action** Use proper syntax when entering policy information.

**Severity** INFO

## SEC-1145

### Message

```
<timestamp>, [SEC-1145], <sequence-number>,, INFO, <system-name>, A security admin event has occurred. This message is for information purpose only. The message for individual event is: <Event specific data>
```

**Probable Cause** Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-1146

### Message

```
<timestamp>, [SEC-1146], <sequence-number>,, INFO, <system-name>, PID changed: <State>.
```

**Probable Cause** Indicates that the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the DCC polices existed, all area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an area of 127 before changing to extended-edge PID, then the new area is 15, because of the wraparound.

**Recommended Action** No action is required.

**Severity** INFO

## SEC-1153

### Message

```
<timestamp>, [SEC-1153], <sequence-number>,, INFO, <system-name>,
Error in RCA: RCS is not supported
```

### Probable Cause

Indicates that RCS is not supported.

### Recommended Action

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the **firmwareDownload** command to upgrade the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

INFO

## SEC-1154

### Message

```
<timestamp>, [SEC-1154], <sequence-number>,, INFO, <system-name>,
PID change failed: <Reason> <defined status> <active status>.
```

### Probable Cause

Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

### Recommended Action

Reduce the size of the policy database.

### Severity

INFO

## SEC-1155

### Message

```
<timestamp>, [SEC-1155], <sequence-number>,, INFO, <system-name>,
PID change failed: <Reason> <defined status> <active status>.
```

### Probable Cause

Indicates that either the defined or active policy was too large after modifying the area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

**Recommended Action** Reduce the size of the specified policy database.

**Severity** INFO

## SEC-1156

### Message

```
<timestamp>, [SEC-1156], <sequence-number>,, INFO, <system-name>,
Change failed: <Reason> <defined status> <active status>.
```

**Probable Cause** Indicates that the security daemon is busy. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

**Recommended Action** For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

**Severity** INFO

## SEC-1157

### Message

```
<timestamp>, [SEC-1157], <sequence-number>,, INFO, <system-name>,
PID Change failed: <Reason> <defined status> <active status>.
```

**Probable Cause** Indicates that the provisioning resources for a security policy failed due to low memory or internal error. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

**Recommended Action** Retry the failed command.  
If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** INFO

## SEC-1158

### Message

```
<timestamp>, [SEC-1158], <sequence-number>,, INFO, <system-name>,
Invalid name <Policy or Switch name>.
```

**Probable Cause** Indicates that the specified name is invalid. The name can be a policy name or a switch name.

**Recommended Action** Enter a valid name.

**Severity** INFO

## SEC-1159

### Message

```
<timestamp>, [SEC-1159], <sequence-number>,, INFO, <system-name>,
Non_Reachable domain <Domain ID>.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1160

### Message

```
<timestamp>, [SEC-1160], <sequence-number>,, INFO, <system-name>,
Duplicate port <Port ID> in port list (<Port list>).
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1163

### Message

```
<timestamp>, [SEC-1163], <sequence-number>,, ERROR, <system-name>,
System is already in secure mode. Lockdown option cannot be applied.
```

**Probable Cause** Indicates that the lockdown option was attempted while the fabric is already in secure mode.

**Recommended Action** Do not use lockdown option with **secModeEnable**, when switch is already in secure mode.

**Severity** ERROR

## SEC-1164

### Message

```
<timestamp>, [SEC-1164], <sequence-number>,, ERROR, <system-name>,  
Lockdown option cannot be applied on a non-FCS switch.
```

**Probable Cause** Indicates that the attempt to enable security is made on a switch that is not present in the FCS list.

**Recommended Action** Add the switch into the FCS policy list when using the lockdown option to enable security.

**Severity** ERROR

## SEC-1165

### Message

```
<timestamp>, [SEC-1165], <sequence-number>,, ERROR, <system-name>,  
Low memory, failed to enable security on all switches.
```

**Probable Cause** Indicates that the system is low on memory.

**Recommended Action** Wait a few minutes and try the command again.

**Severity** ERROR

## SEC-1166

### Message

```
<timestamp>, [SEC-1166], <sequence-number>,, ERROR, <system-name>,  
Non FCS tries to commit failover.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.



**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1167

### Message

```
<timestamp>, [SEC-1167], <sequence-number>,, ERROR, <system-name>,
Another FCS failover is in process. Command terminated.
```

**Probable Cause** Indicates that because another failover is already in progress, this failover attempt cannot proceed.

**Recommended Action** Verify that the security event was planned. If the security event was planned, retry FCS failover after current failover has completed, if this switch should become primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** ERROR

## SEC-1168

### Message

```
<timestamp>, [SEC-1168], <sequence-number>,, ERROR, <system-name>,
Primary FCS failover is busy. Please retry later.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** ERROR

## SEC-1170

### Message

```
<timestamp>, [SEC-1170], <sequence-number>,, INFO, <system-name>,
This command must be executed on the Primary FCS switch, the first
reachable switch in the FCS list.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1171

### Message

```
<timestamp>, [SEC-1171], <sequence-number>,, ERROR, <system-name>,
Disabled secure mode due to invalid security object.
```

**Probable Cause** Indicates that the switch is segmented, and secure mode is disabled on the switch because there was no license present or no PKI objects.

**Recommended Action** Run the **pkiShow** command to check if all PKI objects exist. If they do not exist, run the **pkiCreate** command to create them for the switch.

Run the **licenseAdd** command to install the required license key. Refer to your switch supplier to obtain a license if you do not have one.

**Severity** ERROR

## SEC-1172

### Message

```
<timestamp>, [SEC-1172], <sequence-number>,, ERROR, <system-name>,
Failed to identify role.
```

**Probable Cause** Indicates that the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

**Recommended Action** Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

**Severity** ERROR

## SEC-1173

### Message

```
<timestamp>, [SEC-1173], <sequence-number>,, ERROR, <system-name>,
Lost contact with Primary FCS switch.
```

**Probable Cause** Indicates that the switch has lost contact with the primary FCS switch in the secure fabric. This could be due to the primary FCS being disabled.

**Recommended Action** If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

**Severity** ERROR

## SEC-1174

### Message

```
<timestamp>, [SEC-1174], <sequence-number>,, ERROR, <system-name>,
Failed to set <FCS or non-FCS> password.
```

**Probable Cause** Indicates that the FCS or non-FCS password could not be set.

**Recommended Action** Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

**Severity** ERROR

## SEC-1175

### Message

```
<timestamp>, [SEC-1175], <sequence-number>,, ERROR, <system-name>,
Failed to install zone data.
```

**Probable Cause** Indicates that the zone database could not be installed on the switch.

**Recommended Action** Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

**Severity** ERROR

## SEC-1176

### Message

```
<timestamp>, [SEC-1176], <sequence-number>,, ERROR, <system-name>,
Failed to generate new version stamp.
```

**Probable Cause** Indicates that the primary FCS failed to generate a new version stamp due to the fabric not being stable.

**Recommended Action** Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

**Severity** ERROR

## SEC-1180

### Message

```
<timestamp>, [SEC-1180], <sequence-number>,, INFO, <system-name>,  
Added account <user name> with <role name> authorization.
```

**Probable Cause** Indicates that the specified new account has been created.

**Recommended Action** No action is required.

**Severity** INFO

## SEC-1181

### Message

```
<timestamp>, [SEC-1181], <sequence-number>,, INFO, <system-name>,  
Deleted account <user name>
```

**Probable Cause** Indicates that the specified account has been deleted.

**Recommended Action** No action is required.

**Severity** INFO

## SEC-1182

### Message

```
<timestamp>, [SEC-1182], <sequence-number>,, INFO, <system-name>,  
Recovered <number of> accounts.
```

**Probable Cause** Indicates that the specified number of accounts have been recovered from backup.

**Recommended Action** No action is required.

**Severity** INFO

## SEC-1183

### Message

```
<timestamp>, [SEC-1183], <sequence-number>,, ERROR, <system-name>,
Policy to binary conversion error: Port <port number> is out range.
```

### Probable Cause

Indicates that a security database conversion has failed because of an invalid value.

### Recommended Action

Retry the command with a valid value.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## SEC-1184

### Message

```
<timestamp>, [SEC-1184], <sequence-number>,, INFO, <system-name>,
Radius config change, action <action>, server ID <server>.
```

### Probable Cause

Indicates that the specified action is applied to the specified RADIUS server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

### Recommended Action

No action is required.

### Severity

INFO

## SEC-1185

### Message

```
<timestamp>, [SEC-1185], <sequence-number>,, INFO, <system-name>,
<action> switch DB.
```

### Probable Cause

Indicates that the switch database was enabled or disabled as the secondary AAA when RADUIS is the primary AAA mechanism.

### Recommended Action

No action is required.

### Severity

INFO

## SEC-1186

### Message

```
<timestamp>, [SEC-1186], <sequence-number>,, INFO, <system-name>,
<action> Radius Configuration.
```

### Probable Cause

Indicates that the RADIUS configuration was enabled or disabled as the primary AAA mechanism.

### Recommended Action

No action is required.

### Severity

INFO

## SEC-1187

### Message

```
<timestamp>, [SEC-1187], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized switch <switch wwn> tries to join
secure fabric.
```

### Probable Cause

Indicates that an SCC security violation was reported. The specified unauthorized switch attempts to join the secure fabric.

### Recommended Action

Check the switch connection control policy (SCC policy specifies the WWNs of switches allowed in the fabric) to verify which switches are allowed in the fabric. If the switch should be allowed in the fabric but not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

## SEC-1188

### Message

```
<timestamp>, [SEC-1188], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized device <device node name> tries to
flogin to area <port number> of switch <switch wwn>.
```

### Probable Cause

Indicates that a DCC security violation was reported. The specified device attempted to login using FLOGI to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, the device will not be allowed to login.

### Recommended Action

Check DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy. If the specified device not included in the policy, add it to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1189

### Message

```
<timestamp>, [SEC-1189], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address>
tries to do SNMP write operation.
```

**Probable Cause** Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

**Recommended Action** Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1190

### Message

```
<timestamp>, [SEC-1190], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address>
tries to do SNMP read operation.
```

**Probable Cause** Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

**Recommended Action** Check the RSNMP policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1191

### Message

```
<timestamp>, [SEC-1191], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <Ip address>
tries to establish HTTP connection.
```

**Probable Cause** Indicates that an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

**Recommended Action** Check if the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1192

### Message

```
<timestamp>, [SEC-1192], <sequence-number>,, INFO, <system-name>,
Security violation: Login failure attempt via <connection method>.
```

**Probable Cause** Indicates that a serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

**Recommended Action** Use the correct password.

**Severity** INFO

## SEC-1193

### Message

```
<timestamp>, [SEC-1193], <sequence-number>,, INFO, <system-name>,
Security violation: Login failure attempt via <connection method>.
IP Addr: <IP address>
```

**Probable Cause** Indicates that a specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

**Recommended Action** The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

**Severity** INFO

## SEC-1194

### Message

```
<timestamp>, [SEC-1194], <sequence-number>,, WARNING, <system-
name>, This switch does not have all the required PKI objects
correctly installed.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.



**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** WARNING

## SEC-1195

### Message

```
<timestamp>, [SEC-1195], <sequence-number>,, WARNING, <system-name>, This switch has no <component> license.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** WARNING

## SEC-1196

### Message

```
<timestamp>, [SEC-1196], <sequence-number>,, WARNING, <system-name>, Switch does not have all default account names.
```

**Probable Cause** Indicates that the default switch accounts admin and user do not exist on the switch when enabling security.

**Recommended Action** Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

**Severity** WARNING

## SEC-1197

### Message

```
<timestamp>, [SEC-1197], <sequence-number>,, INFO, <system-name>, Changed account <user name>.
```

**Probable Cause** Indicates that the specified account has changed.

**Recommended Action** No action is required.

**Severity** INFO

## SEC-1198

### Message

```
<timestamp>, [SEC-1198], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized host with IP address <IP address>
tries to establish API connection.
```

**Probable Cause** Indicates that an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

**Recommended Action** Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1199

### Message

```
<timestamp>, [SEC-1199], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized access to serial port of switch
<switch instance>.
```

**Probable Cause** Indicates that a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

**Recommended Action** Check to see if an authorized access attempt is being made on the console. If so, add the switch WWN to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1200

### Message

```
<timestamp>, [SEC-1200], <sequence-number>,, INFO, <system-name>,
Security violation: MS command is forwarded from non-primary FCS
switch.
```

**Probable Cause** Indicates that an MS forward security violation was reported. A management server command was forwarded from a non-primary FCS switch.

**Recommended Action** Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1201

### Message

```
<timestamp>, [SEC-1201], <sequence-number>,, INFO, <system-name>,
Security violation: MS device <device wwn> operates on non-primary
FCS switch.
```

**Probable Cause** Indicates that an MS operation security violation was reported. An MS device operation occurred on a non-primary FCS switch.

**Recommended Action** Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1202

### Message

```
<timestamp>, [SEC-1202], <sequence-number>,, INFO, <system-name>,
Security violation: Unauthorized access from MS device node name
<device node name>, device port name <device port name>.
```

**Probable Cause** Indicates that a MS security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

**Recommended Action** Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

**Severity** INFO

## SEC-1250

### Message

```
<timestamp>, [SEC-1250], <sequence-number>,, WARNING, <system-name>, DCC enforcement API failed: <failed action> err=<status>, key=<data>
```

### Probable Cause

Indicates that an internal error caused the DCC policy enforcement to fail.

### Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## SEC-1251

### Message

```
<timestamp>, [SEC-1251], <sequence-number>,, ERROR, <system-name>, Policy to binary conversion error: <text message> <value>.
```

### Probable Cause

Indicates that the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and faulty value is printed in *value* variable.

### Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## SEC-1253

### Message

```
<timestamp>, [SEC-1253], <sequence-number>,, ERROR, <system-name>, Bad DCC interface state during <Phase>, state=<state>.
```

### Probable Cause

Indicates that an internal error has caused the DCC policy update to fail in the provision, commit, or cancel phases.

### Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## SEC-1300

### Message

```
<timestamp>, [SEC-1300], <sequence-number>,, INFO, <system-name>,
This switch is in VcEncode mode. Security is not supported.
```

**Probable Cause** Indicates that the switch is set up with VC-encoded mode.

**Recommended Action** Turn off VC-encoded mode before enabling security.

**Severity** INFO

## SEC-1301

### Message

```
<timestamp>, [SEC-1301], <sequence-number>,, INFO, <system-name>,
This switch is in interop mode. Security is not supported.
```

**Probable Cause** Indicates that the switch is interop-mode enabled.

**Recommended Action** Disable interop-mode using the **interopMode** command before enabling the Secure Fabric OS feature.

**Severity** INFO

## SEC-1302

### Message

```
<timestamp>, [SEC-1302], <sequence-number>,, INFO, <system-name>,
This switch does not have all the required PKI objects correctly
installed.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1303

### Message

```
<timestamp>, [SEC-1303], <sequence-number>,, INFO, <system-name>,  
This software version does not support security.
```

**Probable Cause** Indicates that the currently installed software version does not support the Brocade Secure Fabric OS feature.

**Recommended Action** Run the **firmwareDownload** command to update the firmware to the latest version for your specific switch. Verify that the firmware you are installing supports the Brocade Secure Fabric OS feature.

**Severity** INFO

## SEC-1304

### Message

```
<timestamp>, [SEC-1304], <sequence-number>,, INFO, <system-name>,  
This switch has no security license.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1305

### Message

```
<timestamp>, [SEC-1305], <sequence-number>,, INFO, <system-name>,  
This switch has no zoning license.
```

**Probable Cause** Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

**Recommended Action** Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

**Severity** INFO

## SEC-1306

### Message

```
<timestamp>, [SEC-1306], <sequence-number>,, INFO, <system-name>,
Failed to verify certificate with root CA.
```

**Probable Cause** Indicates that the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

**Recommended Action** Run the **pkiShow** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS User's Guide*. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

**Severity** INFO

## SEC-1307

### Message

```
<timestamp>, [SEC-1307], <sequence-number>,, INFO, <system-name>,
Got response from Radius server <Radius server identity>.
```

**Probable Cause** Indicates that after some servers timed out, the specified RADIUS server responded to a switch request.

**Recommended Action** If the message appears frequently, move the specified server to the top of the server configuration list.

**Severity** INFO

## SEC-1308

### Message

```
<timestamp>, [SEC-1308], <sequence-number>,, INFO, <system-name>,
All Radius servers have failed to respond.
```

**Probable Cause** Indicates that all servers in the RADIUS configuration have failed to respond to a switch request within the specified timeout.

**Recommended Action** Verify that the switch has proper network connectivity to the specified RADIUS servers, and the servers are correctly configured.

**Severity** INFO

## SEC-3001

### Message

```
<timestamp>, [SEC-3001], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: security mode <State change: Enabled or Disabled>.
```

### Probable Cause

Indicates that the security mode of the fabric was either enabled or disabled.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3002

### Message

```
<timestamp>, [SEC-3002], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: NONE
```

### Probable Cause

Indicates that the specified security event has occurred. The event can be:

- There has been an FCS failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.
- A temporary password was set or reset.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3003

### Message

```
<timestamp>, [SEC-3003], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Create <Policy Name> policy, with <Member List> entries.
```



**Probable Cause** Indicates that a new security policy with entries has been created. When you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event info field.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3004

### Message

```
<timestamp>, [SEC-3004], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Create <Policy name> policy.
```

**Probable Cause** Indicates that a new security policy has been created. When you use a wildcard (for example, an asterisk) in creating member for a policy, the audit report displays the wildcard in the event info field.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3005

### Message

```
<timestamp>, [SEC-3005], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Add members [<Members added>] to policy <Policy name>.
```

**Probable Cause** Indicates that new member(s) have been added to a security policy. When you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event info field.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3006

### Message

```
<timestamp>, [SEC-3006], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Remove members [<Members removed>] from policy <Policy name>.
```

### Probable Cause

Indicates that a user has removed the specific members from the security policy. When you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event info field.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3007

### Message

```
<timestamp>, [SEC-3007], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Delete policy <Deleted policy name>.
```

### Probable Cause

Indicates that the user deleted the specified security policy.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3008

### Message

```
<timestamp>, [SEC-3008], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: FCS moved from position [<Old FCS position>] to [<New FCS position>].
```

### Probable Cause

Indicates that the FCS list has been modified. One of the members of the list has been moved to a new position in the list.

### Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3009

### Message

```
<timestamp>, [SEC-3009], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Security Transaction aborted.
```

**Probable Cause** Indicates that the pending security transaction is aborted.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3010

### Message

```
<timestamp>, [SEC-3010], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Reset [<Event specific information>] security stat(s).
```

**Probable Cause** Indicates that the user has reset all the security statistics.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3011

### Message

```
<timestamp>, [SEC-3011], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Reset <Stat name> stat on domains <Domain IDs>.
```

**Probable Cause** Indicates that the user has reset a security statistic on the specified domains.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3012

### Message

```
<timestamp>, [SEC-3012], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Passwd set/reset on domain [<Domain ID>] for account(s) <Account name>.
```

**Probable Cause** Indicates that the user has reset the password for the specified user accounts.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3013

### Message

```
<timestamp>, [SEC-3013], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Version is reset.
```

**Probable Cause** Indicates that the specified user has reset the security version stamp.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3014

### Message

```
<timestamp>, [SEC-3014], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: <Event option> server <Event data>.
```

**Probable Cause** Indicates that the specified user has changed the RADIUS configuration.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3015

### Message

```
<timestamp>, [SEC-3015], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: <Event option> server <Server name> to position <New position>.
```

**Probable Cause** Indicates that the specified user has changed the RADIUS configuration.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3016

### Message

```
<timestamp>, [SEC-3016], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: <Event option> server <server ID> attributes. New values: <Changed values>
```

**Probable Cause** Indicates that the specified user has changed the RADIUS configuration.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

## SEC-3017

### Message

```
<timestamp>, [SEC-3017], <sequence-number>, AUDIT, INFO, <system-name>, User: <User Name>, role: <User Role>, Event: <Event Name>, status: <Event Status>, Info: Radius <Server state>
```

**Probable Cause** Indicates that the specified user has changed the RADIUS configuration.

**Recommended Action** Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

**Severity** INFO

# SNMP Error Messages

---

## SNMP-1001

**Message**

```
<timestamp>, [SNMP-1001], <sequence-number>, , ERROR, <system-name>,
SNMP service is not available <Reason>.
```

**Probable Cause**

Indicates that the SNMP service could not be started because of the specified *Reason*. You will not be able to query the switch through SNMP.

**Recommended Action**

Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified *Reason* is an initialization failure, the switch requires a reboot.

**Severity**

ERROR

## SNMP-1002

**Message**

```
<timestamp>, [SNMP-1002], <sequence-number>, , ERROR, <system-name>,
SNMP <Error Details> initialization failed.
```

**Probable Cause**

Indicates that the initialization of the SNMP service failed and you will not be able to query the switch through SNMP.

**Recommended Action**

Reboot or power cycle the switch. This will automatically initialize SNMP.

**Severity**

ERROR

## SNMP-1003

**Message**

```
<timestamp>, [SNMP-1003], <sequence-number>, , ERROR, <system-name>,
Distribution of Community Strings to Secure Fabric failed.
```

**Probable Cause**

Indicates that the changes in the SNMP community strings could not be propagated to other switches in the secure fabric.

**Recommended Action**     Retry changing the SNMP community strings from the primary switch.

**Severity**     ERROR

## SNMP-1004

### Message

```
<timestamp>, [SNMP-1004], <sequence-number>, , ERROR, <system-name>,
Incorrect SNMP configuration.
```

**Probable Cause**     Indicates that the SNMP configuration is incorrect and the SNMP service will not work correctly.

**Recommended Action**     Try changing the SNMP configuration back to the default.

**Severity**     ERROR



# SS Error Messages

---

## SS-1000

### Message

```
<timestamp>, [SS-1000], <sequence-number>,, INFO, <system-name>,
supportSave has ftp'ed support information to the host with IP
address <host ip>.
```

### Probable Cause

Indicates that the **supportSave** command was used to transfer support information to a remote FTP location.

### Recommended Action

No action is required.

### Severity

INFO

## SS-1001

### Message

```
<timestamp>, [SS-1001], <sequence-number>,, WARNING, <system-name>,
supportSave's ftp operation to host IP address <host ip> aborted.
```

### Probable Cause

Indicates that an FTP error occurred during execution of the **supportSave** command.

### Recommended Action

Check the FTP server and settings. Run the **supportFtp** command to set the FTP parameters. After the FTP problem is corrected, rerun the **supportSave** command.

### Severity

WARNING



# SULB Error Messages

---

## SULB-1001

### Message

```
<timestamp>, [SULB-1001], <sequence-number>,, WARNING, <system-name>, Firmwaredownload command has started.
```

### Probable Cause

Indicates that the **firmwareDownload** command has started. This process can take some time; wait until the process is complete before initiating any new commands to the system.

### Recommended Action

Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption. No action is required.

Run the **firmwareDownloadStatus** command for more information.

### Severity

WARNING

## SULB-1002

### Message

```
<timestamp>, [SULB-1002], <sequence-number>,, INFO, <system-name>, Firmwaredownload command has completed successfully.
```

### Probable Cause

Indicates that the **firmwareDownload** command has completed successfully and loaded firmware to both the CPs.

### Recommended Action

No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information.

### Severity

INFO

## SULB-1003

### Message

```
<timestamp>, [SULB-1003], <sequence-number>,, INFO, <system-name>, Firmwarecommit has started.
```

**Probable Cause** Indicates the **FirmwareCommit** command has started to update the secondary partition.

**Recommended Action** No action is required. Run the **firmwareDownloadStatus** command for more information.

**Severity** INFO

## SULB-1005

### Message

```
<timestamp>, [SULB-1005], <sequence-number>,, INFO, <system-name>,
Current Active CP is preparing to failover.
```

**Probable Cause** Indicates that the forced failover was successful and the standby CP is now the active CP.

**Recommended Action** No action is required. The **firmwareDownload** command is progressing as expected.  
Run the **firmwareDownloadStatus** command for more information.

**Severity** INFO

## SULB-1006

### Message

```
<timestamp>, [SULB-1006], <sequence-number>,, INFO, <system-name>,
Forced failover succeeded. New Active CP is running new firmware.
```

**Probable Cause** Indicates that the previous standby has now become the active CP and is running the new firmware version.

**Recommended Action** No action is required. The **firmwareDownload** command is progressing as expected.  
Run the **firmwareDownloadStatus** command for more information.

**Severity** INFO

## SULB-1007

### Message

```
<timestamp>, [SULB-1007], <sequence-number>,, INFO, <system-name>,
Standby CP reboots.
```

**Probable Cause** Indicates that the standby CP will reboot.

**Recommended Action** No action is required. The **firmwareDownload** command is progressing as expected.  
Run the **firmwareDownloadStatus** command for more information.

**Severity** INFO

## SULB-1008

### Message

```
<timestamp>, [SULB-1008], <sequence-number>,, INFO, <system-name>,
Standby CP booted successfully with new firmware.
```

**Probable Cause** Indicates that the standby CP has rebooted successfully.

**Recommended Action** No action is required. The **firmwareDownload** command is progressing as expected.  
Run the **firmwareDownloadStatus** command for more information.

**Severity** INFO

## SULB-1009

### Message

```
<timestamp>, [SULB-1009], <sequence-number>,, INFO, <system-name>,
Firmwaredownload command failed (0x<firmwaredownload error code>).
```

**Probable Cause** Indicates that the firmware download failed. The additional *error message* information provides debugging information.

The **firmwareDownload** error code contains two bytes. The first byte contains the upgrade error message code, as indicated in [Table 49-1 on page 49-4](#), while the second byte might contain either the reason code (what caused the failure) or the state code (where the failure occurs), as indicated in the [Table 49-2 on page 49-8](#). The error code can be retrieved either by running the **firmwareDownloadStatus** command or through the **errShow** and **errDump** commands.

For example, the following entry indicates that the **firmwareDownload** failed in SUS\_SBY\_FS\_CHECK (0x2e) state because the "Standby CP failed to reboot" (0x66):

```
Switch: 0, Info SULIB-FWDL_FAIL, 4, Firmwaredownload command failed
(status=0x662e).
```

The following entry indicates that the **firmwareDownload** failed (0x44) because firmware has not been committed (0x1e):

```
Switch: 0, Info SULIB-FWDL_FAIL, 4, Firmwaredownload command failed (status=0x441e)
```

The following table lists the upgrade message and the associated code for that message.

**Table 49-1** Upgrade Messages and Code Values

Upgrade Messages	Code
"Image is up-to-date. No need to download."	0xF
"Boot environment variable is inconsistent."	0x10
"Bootenv OSRootPartition is inconsistent."	0x11
"Can't access package list (.plist) file."	0x12
"RPM database is inconsistent."	0x13
"Ran out of memory."	0x14
"Firmwaredownload failed due to out of disk space or timeout."	0x15
"Failed to create firmware version file."	0x16
"Unexpected system error."	0x17
"Error in getting lock device."	0x18
"Error in releasing lock device."	0x19
"Firmwarecommit failed."	0x1a
"Firmware directory structure is not compatible."	0x1b
"Failed to load kernel image."	0x1c
"Bootenv OSLoader is inconsistent."	0x1d
"Firmwaredownload failed because new image has not been committed."	0x1e
"Firmwarerestore failed."	0x1f
"Both images are mounted to the same device."	0x20
"Error in removing packages."	0x21
"Firmwaredownload is already in progress."	0x22
"Firmwaredownload timeout."	0x23
"Firmwaredownload sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because <b>firmwareDownload</b> is already in progress."	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34
"Sanity check failed because <b>firmwareDownload</b> is already in progress."	0x35

Upgrade Messages	Code
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
"Firmwaredownload failed on Standby CP."	0x40
"Firmwaredownload failed on Standby CP."	0x41
"Firmwaredownload failed on Standby CP."	0x42
"Firmwarecommit failed on Standby CP."	0x43
"Firmwaredownload failed."	0x44
"Firmwaredownload failed due to Standby CP timeout."	0x50
"Unable to check firmware version due to Standby CP timeout."	0x51
"Firmwaredownload failed due to Standby CP timeout."	0x52
"Firmwaredownload failed due to Standby CP timeout."	0x53
"Standby CP failed to reboot and was not responding."	0x54
"Firmwarecommit failed due to Standby CP timeout."	0x55
"Unable to check firmware version due to Standby CP timeout."	0x56
"Unable to restore the original firmware due to Standby CP timeout."	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check firmware version due to Standby CP timeout."	0x59
"Sanity check failed because <b>firmwareDownload</b> is already in progress."	0x60
"Sanity check failed because <b>firmwareDownload</b> is already in progress."	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Standby CP failed to reboot."	0x66

Upgrade Messages	Code
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
"Firmwarecommit has started to restore the secondary partition."	0x69
"Local CP is restoring its secondary partition."	0x6a
"Unable to restore the secondary partition. Please use firmwaredownloadstatus and firmwareshow to see firmware status."	0x6b
"Firmwaredownload has started on Standby CP. It might take up to 10 minutes."	0x6c
"Firmwaredownload has completed successfully on Standby CP."	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
"Firmwaredownload has completed successfully on Standby CP."	0x72
"Firmwaredownload has started on Standby CP. It might take up to 10 minutes. "	0x73
"Firmwaredownload has completed successfully on Standby CP."	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
"Firmwarecommit has started on Standby CP."	0x77
"Firmwarecommit has completed successfully on Standby CP."	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
"Firmwarecommit has started on both Active and Standby CPs."	0x7b
"Firmwarecommit has completed successfully on Active CP."	0x7c
"Firmwarecommit failed on Active CP."	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e



Upgrade Messages	Code
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
"There was an unexpected reboot during <b>firmwareDownload</b> . The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"Firmwarecommit has started on both CPs. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x86
"Firmwarecommit has started on the local CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x87
"Firmwarecommit has started on the remote CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x88
"Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x89
"Firmwaredownload command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
"Firmwaredownload has started."	0x8f
"Firmwarecommit has started."	0x90
"Firmwaredownload has completed successfully."	0x91
"Firmwarecommit has completed successfully."	0x92
"Firmwarecommit has started to restore the secondary partition."	0x93
"Firmwarecommit failed."	0x94
"The secondary partition has been restored successfully."	0x95

The following table lists the upgrade state and the associated code value for that state.

**Table 49-2** Upgrade State and Code Values

Upgrade State	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

**Recommended Action**

Run the **firmwareDownload** status command for more information.

Refer to the *Fabric OS Procedures Guide* for troubleshooting information.

**Severity**

INFO

**SULB-1010**

**Message**

```
<timestamp>, [SULB-1010], <sequence-number>,, INFO, <system-name>,
Firmwarecommit failed (status=0x<firmwarecommit error code>).
```

**Probable Cause** Indicates that a firmware commit failed to update the secondary partition.

**Recommended Action** Run the **firmwareCommit** command with "-d" option.

**Severity** INFO



# SWCH Error Messages

---

## SWCH-1001

### Message

```
<timestamp>, [SWCH-1001], <sequence-number>,, ERROR, <system-name>,  
Switch is not in ready state - Switch enable failed switch status=  
0x<switch status>, c_flags = 0x<switch control flags>
```

### Probable Cause

Indicates that the switch is enabled before it is ready.

### Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## SWCH-1002

### Message

```
<timestamp>, [SWCH-1002], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized device <wwn name of device> tries  
to flogin to port <port number>
```

### Probable Cause

Indicates that the device is not present in the authorized profile list.

### Recommended Action

Verify that the device is authorized to log in to the switch. If the device is authorized, run the **secPolicyDump** command to verify whether the specified device WWN is listed. If it is not listed, run the **secPolicyAdd** command to add this device to an existing policy.

### Severity

INFO

## SWCH-1003

### Message

```
<timestamp>, [SWCH-1003], <sequence-number>,, ERROR, <system-name>,  
Slot ENABLED but Not Ready during recovery, disabling slot = <slot  
number>(<return value>)
```

### Probable Cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

### Recommended Action

On a SilkWorm 12000 or 24000 switch, run first the **slotPowerOff** and then the **slotPowerOn** commands.

On a SilkWorm 3250, 3850, 3900, or 4100 switch, reboot or power cycle the switch.

### Severity

ERROR

## SWCH-1004

### Message

```
<timestamp>, [SWCH-1004], <sequence-number>,, ERROR, <system-name>,  
Blade attach failed during recovery, disabling slot = <slot number>
```

### Probable Cause

Indicates that a blade has failed during failover or recovery.

### Recommended Action

On a SilkWorm 12000 or 24000 switch, run first the **slotPowerOff** and then the **slotPowerOn** commands.

On a SilkWorm 3250, 3850, 3900, or 4100 switch, reboot or power cycle the switch.

### Severity

ERROR

## SWCH-1005

### Message

```
<timestamp>, [SWCH-1005], <sequence-number>,, ERROR, <system-name>,  
Diag attach failed during recovery, disabling slot = <slot number>
```

### Probable Cause

Indicates that the Diag blade attach has failed during failover or recovery.

### Recommended Action

On a SilkWorm 12000 or 24000 switch, run first the **slotPowerOff** and then the **slotPowerOn** commands.

On a SilkWorm 3250, 3850, 3900, or 4100 switch, reboot or power cycle the switch.

### Severity

ERROR

# SYSC Error Messages

---

## SYSC-1001

### Message

```
<timestamp>, [SYSC-1001], <sequence-number>,, CRITICAL, <system-name>, Failed to run <Name of program that could not be run (string)>:<System internal error message (string)>
```

### Probable Cause

Indicates that during the boot sequence, one of the programs would not run on the system. The *error information* field indicates the source of the error.

### Recommended Action

If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the **firmwareDownload** command.

If the message persists, there might be a conflict between the two versions of firmware or the nonvolatile storage might be corrupted.

Run supportFtp (as needed) to set up automatic FTP transfers; then run the supportSave command and contact your switch service provider.

### Severity

CRITICAL

## SYSC-1002

### Message

```
<timestamp>, [SYSC-1002], <sequence-number>,, CRITICAL, <system-name>, Switch bring-up timed out
```

### Probable Cause

Indicates that the system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

### Recommended Action

The switch is in an inconsistent state and can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch (or CP) and run the **haDump** command. If this is a dual-CP switch, then gather the output from the CP in which this log message appeared.

### Severity

CRITICAL





# SYSM Error Messages

---

## SYSM-1001

### Message

```
<timestamp>, [SYSM-1001], <sequence-number>,, CRITICAL, <system-name>, No memory
```

### Probable Cause

Indicates that the switch has run out of system memory.

### Recommended Action

Run the **memShow** command to view the switch memory usage.  
Reboot or power cycle the switch.

### Severity

CRITICAL

## SYSM-1002

### Message

```
<timestamp>, [SYSM-1002], <sequence-number>,, INFO, <system-name>, <number>, Switch: <Switch number>
```

### Probable Cause

Indicates that a user has executed either the **switchShutdown** or **switchReboot** command. All services are brought down for a logical switch.

### Recommended Action

No action is required if the **switchShutdown** or **switchReboot** command was executed intentionally. If the **switchShutdown** command was run, you must run the **switchStart** command to restart traffic on the logical switch.

### Severity

INFO

## SYSM-1003

### Message

```
<timestamp>, [SYSM-1003], <sequence-number>,, INFO, <system-name>, <number>, Switch: <start reason>
```

**Probable Cause** Indicates that the user executed the **switchStart** or **switchReboot** command. This indicates that all services are brought back up after a temporary shutdown of that logical switch.

**Recommended Action** No action is required if the **switchStart** command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

**Severity** INFO

## SYSM-1004

### Message

```
<timestamp>, [SYSM-1004], <sequence-number>,, ERROR, <system-name>,  
Failed to retrieve current chassis configuration option, ret=%d
```

**Probable Cause** Indicates that there was a failure to read configuration data from the WWN card.

**Recommended Action** Verify that the WWN card is present and operational and that the affected CP is properly seated in its slot.

**Severity** ERROR

# TRCE Error Messages

---

## TRCE-1001

### Message

```
<timestamp>, [TRCE-1001], <sequence-number>,, WARNING, <system-name>, Trace dump available< optional slot indicating on which slot the dump occurs >! (reason: <Text explanation of what triggered the dump. (PANIC DUMP, WATCHDOG EXPIRED, MANUAL, TRIGGER)>)
```

### Probable Cause

Indicates that trace dump files have been generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump:

- PANICDUMP generated by panic dump
- WATCHDOG EXPIRED generated by hardware watchdog expiration
- MANUAL generated by the **tracedump -n** command
- TRIGGER when triggered by a specific Message ID generated by CRITICAL RASLog message or RASLog message trigger setup using the **traceTrig** command

### Recommended Action

Run **supportFtp** and **traceFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## TRCE-1002

### Message

```
<timestamp>, [TRCE-1002], <sequence-number>,, INFO, <system-name>, Trace dump< optional slot indicating on which slot the dump occurs > automatically transferred to FTP address ' <FTP target designated by user> '.
```

### Probable Cause

Indicates that a trace dump has occurred on the switch or the indicated slot and is successfully transferred from the switch automatically.

### Recommended Action

No action is required.

**Severity** INFO

## TRCE-1003

### Message

```
<timestamp>, [TRCE-1003], <sequence-number>,, ERROR, <system-name>,  
Trace dump< optional slot indicating on which slot the dump occurs >  
was not transferred due to FTP error.
```

### Probable Cause

Indicates that a trace dump has been created on the switch or the indicated slot but is not automatically transferred from the switch due to an FTP error, such as wrong FTP address, FTP site down, network down, and so on.

### Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## TRCE-1004

### Message

```
<timestamp>, [TRCE-1004], <sequence-number>,, WARNING, <system-  
name>, Trace dump< optional slot indicating on which slot the dump  
occurs > was not transferred because trace auto-FTP disabled.
```

### Probable Cause

Indicates that trace dump files have been created on the switch or the indicated slot but are not automatically transferred from the switch because auto-FTP is disabled.

### Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

WARNING

## TRCE-1005

### Message

```
<timestamp>, [TRCE-1005], <sequence-number>,, ERROR, <system-name>,  
FTP Connectivity Test failed due to error.
```

### Probable Cause

Indicates that the connectivity test to the FTP host fails, because of a wrong FTP address, an FTP site down, or the network being down, and so on.

### Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## TRCE-1006

### Message

```
<timestamp>, [TRCE-1006], <sequence-number>,, INFO, <system-name>,
FTP Connectivity Test succeeded to FTP site ' <FTP target configured
by users.> '.
```

### Probable Cause

Indicates that a connectivity test to the FTP host has succeeded.

### Recommended Action

No action is required.

### Severity

INFO

## TRCE-1007

### Message

```
<timestamp>, [TRCE-1007], <sequence-number>,, ERROR, <system-name>,
Notification of this CP has failed. Parameters temporarily out of
synch with other CP.
```

### Probable Cause

Indicates that the active CP is unable to alert the standby CP of a change in trace status. This message is only applicable to the SilkWorm 12000 and 24000.

### Recommended Action

This message is often transitory. Wait a few minutes and try the command again.

If the problem persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## TRCE-1008

### Message

```
<timestamp>, [TRCE-1008], <sequence-number>,, CRITICAL, <system-
name>, Unable to load trace parameters.
```

### Probable Cause

Indicates that the active CP is unable to read stored trace parameters.

### Recommended Action

Reboot the CP (dual-CP system) or restart the switch.

Run **traceFtp** to set up for automatic FTP transfers.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** CRITICAL

## TRCE-1009

### Message

```
<timestamp>, [TRCE-1009], <sequence-number>,, ERROR, <system-name>,
Unable to alert active CP that a dump has occurred.
```

**Probable Cause** Indicates that the standby CP is unable to communicate trace information to active CP. This message is only applicable to the SilkWorm 12000 and 24000.

**Recommended Action** Run the **haShow** command to verify that the current CP is standby and the active CP is active.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## TRCE-1010

### Message

```
<timestamp>, [TRCE-1010], <sequence-number>,, ERROR, <system-name>,
Traced fails to start
```

**Probable Cause** Indicates that the trace daemon (traced), used for transferring trace files, failed to start. The trace capability within the switch is unaffected.

**Recommended Action** Reboot the CP (dual-CP system) or restart the switch.

Run **traceFtp** to set up for automatic FTP transfers.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** ERROR

## TRCE-1011

### Message

```
<timestamp>, [TRCE-1011], <sequence-number>,, INFO, <system-name>,
Trace dump manually transferred to target ' <optional string to
indicate which slot the dump is ftped out.> ': <result>.
```

**Probable Cause** Indicates that a manual transfer of trace dump files has occurred.

<b>Recommended Action</b>	No action is required.
<b>Severity</b>	INFO





# TRCK Error Messages

---

## TRCK-1001

**Message**

```
<timestamp>, [TRCK-1001], <sequence-number>,, INFO, <system-name>, Successful login by user <User>.
```

**Probable Cause**

Indicates that the track change feature recorded a successful login.

**Recommended Action**

No action is required.

**Severity**

INFO

## TRCK-1002

**Message**

```
<timestamp>, [TRCK-1002], <sequence-number>,, INFO, <system-name>, Unsuccessful login by user <User>.
```

**Probable Cause**

Indicates that the track change feature recorded a failed login. This occurs if the user name or password is entered incorrectly.

**Recommended Action**

Normally, this message indicates a typing error by an authorized user. If this message occurs repeatedly, it might indicate an unauthorized user trying to gain access to a switch. When secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

**Severity**

INFO

## TRCK-1003

**Message**

```
<timestamp>, [TRCK-1003], <sequence-number>,, INFO, <system-name>, Logout by user <User>.
```

**Probable Cause** Indicates that the track change feature recorded a successful logout.

**Recommended Action** No action is required.

**Severity** INFO

## TRCK-1004

### Message

```
<timestamp>, [TRCK-1004], <sequence-number>,, INFO, <system-name>,
Config file change from task:<task>
```

**Probable Cause** Indicates that the track change feature recorded a configuration change for the switch. The track change feature records any change to the configuration file in nonvolatile memory, including a **configDownload**. This message is not generated for a **configUpload**. All configuration changes occur through the PDM server, so the PDMIPC is the only task possible.

**Recommended Action** No action is required. Run the **configShow** command to view the configuration file.

**Severity** INFO

## TRCK-1005

### Message

```
<timestamp>, [TRCK-1005], <sequence-number>,, INFO, <system-name>,
Track-changes on
```

**Probable Cause** Indicates that the track change feature has been enabled.

**Recommended Action** No action is required. Run the **trackChangesSet 0** command to disable the track change feature.

**Severity** INFO

## TRCK-1006

### Message

```
<timestamp>, [TRCK-1006], <sequence-number>,, INFO, <system-name>,
Track-changes off
```

**Probable Cause** Indicates that the track change feature has been disabled.

<b>Recommended Action</b>	No action is required. Run the <b>trackChangesSet 1</b> command to enable the track changes feature.
<b>Severity</b>	INFO



# TS Error Messages

---

## TS-1001

### Message

```
<timestamp>, [TS-1001], <sequence-number>, , WARNING, <system-name>,
NTP Query failed: <error code>
```

### Probable Cause

Indicates that a network time protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary FCS switch is used for fabric synchronization.

This might be logged during temporary operational issues such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

### Recommended Action

Verify that the configured external clock server is available and functional. If that external clock server is not available, choose another.

### Severity

WARNING

## TS-1002

### Message

```
<timestamp>, [TS-1002], <sequence-number>, , WARNING, <system-name>,
< Type of clock server used > Clock Server used instead of < Type of
clock server configured >: locl: 0x<code> remote: 0x<code>
```

### Probable Cause

Indicates that the fabric time synchronization distributed from the principal or primary FCS switch was not sourced from the *Type of clock server configured*, instead, an alternate server was used, indicated by *Type of clock server used*. The type of clock server used or configured might be either:

- LOCL  
Local clock on the principal or primary FCS switch
- External  
External NTP server address configured

This might be logged during temporary operational issues such as IP network connection issues to the external clock server or if the fabric is configured for external time synchronization but the principal or primary FCS does not support the feature. If the message does not recur, it should be ignored.

**Recommended Action** Run the **tsClockServer** command to verify that the principal or primary FCS switch has the clock server IP configured correctly. Verify that this clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

**Severity** WARNING

## TS-1006

### Message

```
<timestamp>, [TS-1006], <sequence-number>, , INFO, <system-name>, <message>
```

**Probable Cause** Indicates that a time service event is occurring or has failed. The message might be one of the following:

- Init failed. Time Service exiting  
Probable Cause: Initialization error, Time Server exits.
- Synchronizing time of day clock  
Probable Cause: Usually logged during temporary operational issues when the clock goes out of synchronization: For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary FCS switch. If the message does not recur, it should be ignored.
- Validating time update  
Probable Cause: Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it should be ignored.

**Recommended Action** No action is required.

**Severity** INFO

# UCST Error Messages

---

## UCST-1003

### Message

```
<timestamp>, [UCST-1003], <sequence-number>,, INFO, <system-name>,  
Duplicate Path to Domain <domain ID>, Output Port = <port number>,  
PDB pointer = 0x<value>
```

### Probable Cause

Indicates that duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

### Recommended Action

No action is required.

### Severity

INFO

## UCST-1007

### Message

```
<timestamp>, [UCST-1007], <sequence-number>,, CRITICAL, <system-  
name>, Inconsistent route detected: Port = <port number>, should be  
<port number>
```

### Probable Cause

Indicates that the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

### Recommended Action

Run the **switchDisable** command and then the **switchEnable** command to reset the routing database. Run the **uRouteShow** command to display the new routing tables.

### Severity

CRITICAL





# UPTH Error Messages

---

## UPTH-1001

**Message**

```
<timestamp>, [UPTH-1001], <sequence-number>,, WARNING, <system-name>, No minimum cost path in candidate list
```

**Probable Cause**

Indicates that the specified switch is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

**Recommended Action**

No action is required. This will end the current SPF computation.

**Severity**

WARNING



# USWD Error Messages

---

## USWD-1006

**Message**

```
<timestamp>, [USWD-1006], <sequence-number>,, WARNING, <system-name>, uSWD: <Warning message>
```

**Probable Cause**

Indicates a warning state in the system. This is an internal use only message.

**Recommended Action**

No action is required.

**Severity**

WARNING



# WEBD Error Messages

---

## WEBD-1001

### Message

```
<timestamp>, [WEBD-1001], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Certificate file -- HTTPS is configured to be enabled but could not be started.
```

### Probable Cause

Indicates that the SSL certificate file is either invalid or absent.

### Recommended Action

Run the **configure** command to disable HTTPS. Install a valid key file and enable HTTPS again. For more information on the **configure** command, refer to the *Fabric OS Command Reference Manual*.

### Severity

WARNING

## WEBD-1002

### Message

```
<timestamp>, [WEBD-1002], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Key file -- HTTPS is configured to be enabled but could not be started.
```

### Probable Cause

Indicates that the SSL key file is either invalid or absent.

### Recommended Action

Run the **configure** command to disable HTTPS. Install a valid key file and enable HTTPS again. For more information on the **configure** command, refer to the *Fabric OS Command Reference Manual*.

### Severity

WARNING

## WEBD-1003

### Message

```
<timestamp>, [WEBD-1003], <sequence-number>,, INFO, <system-name>, HTTP/HTTPS interface disabled
```

**Probable Cause** Indicates that the HTTP/HTTPS interface is disabled. This is logged when HTTP/HTTPS is disabled through the **configure** command.

**Recommended Action** Run the **configure** command to enable HTTP/HTTPS. For more information on the **configure** command, refer to the *Fabric OS Command Reference Manual*.

**Severity** INFO

## WEBD-1004

### Message

```
<timestamp>, [WEBD-1004], <sequence-number>,, INFO, <system-name>,
HTTP server will be restarted due to configuration change
```

**Probable Cause** Indicates that the HTTP server configuration has changed.

**Recommended Action** No action is required.

**Severity** INFO

## WEBD-1005

### Message

```
<timestamp>, [WEBD-1005], <sequence-number>,, WARNING, <system-
name>, HTTP server will be restarted for logfile truncation
```

**Probable Cause** Indicates that the size of HTTP logfile exceeded the maximum limit.

**Recommended Action** No action is required.

**Severity** WARNING

## WEBD-1006

### Message

```
<timestamp>, [WEBD-1006], <sequence-number>,, INFO, <system-name>,
HTTP server restarted due to logfile truncation
```

**Probable Cause** Indicates that the size of HTTP logfile exceeded the maximum limit.

**Recommended Action** No action is required.

**Severity** INFO

## WEBD-1007

### Message

```
<timestamp>, [WEBD-1007], <sequence-number>,, INFO, <system-name>,  
HTTP server will be restarted due to change of IP Address
```

**Probable Cause** Indicates that the IP address of the switch changed and the HTTP server is restarted.

**Recommended Action** No action is required.

**Severity** INFO





# ZOLB Error Messages

---

## ZOLB-1001

### Message

```
<timestamp>, [ZOLB-1001], <sequence-number>, , ERROR, <system-name>, ZONELIB <error message>
```

### Probable Cause

Indicates that there was an internal timeout on the IPC between the name server (NS) and the zoning modules. This usually indicates that the system was busy.

### Recommended Action

This message generates core dump files of the related modules (zoned, nsd, rcsd). Copy these core files using the **saveCore** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR



## ZONE Error Messages

---

### ZONE-1002

**Message**

```
<timestamp>, [ZONE-1002], <sequence-number>,, WARNING, <system-name>, WWN zoneTypeCheck or zoneGroupCheck warning(<warning string>) at port(<port number>)
```

**Probable Cause**

Indicates that a zone filter or zone group check failure occurred. The frame filter logic reported a failure when creating or adding zone groups during PLOGI trap processing. This messages usually indicates problems when adding CAM entries before the filter setup.

**Recommended Action**

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity**

WARNING

### ZONE-1003

**Message**

```
<timestamp>, [ZONE-1003], <sequence-number>,, WARNING, <system-name>, zone(<current zone>) contains (<domain id>, <port number>) which does not exist.
```

**Probable Cause**

Indicates that the port zone member that is targeted for the local switch contains a non-existent port. The effective zoning configuration (displayed in the error message) contains a port number that is out of range.

**Recommended Action**

Edit the zone database and change the port number to a viable value in the effective configuration.

**Severity**

WARNING

## ZONE-1004

### Message

```
<timestamp>, [ZONE-1004], <sequence-number>,, INFO, <system-name>,
port <port number> enforcement changed to Session Based HARD
Zoning.
```

### Probable Cause

Indicates that the zoning enforcement changed to session-based hard zoning. When a device is zoned using both WWN in one zone and <domain, portarea> in another, this will cause that port to go session based hard zoning.

In session-based zoning, the zone enforcement is checked by the software. In hardware-enforced zoning, zone or alias members are defined using <domain, portarea> exclusively or using WWNs exclusively: that is, using one method or the other to define all objects in the zoning database. If the devices on the port are defined by a mixture of port IDs and WWNs, the zone enforcement is session based. If the S\_ID list of the hardware-enforced zoning overflows (over the S\_ID limit), the hardware zone enforcement changes to session-based zoning.

### Recommended Action

No action is required.

### Severity

INFO

## ZONE-1005

### Message

```
<timestamp>, [ZONE-1005], <sequence-number>,, INFO, <system-name>,
HARD & SOFT zones(<zone name>, <zone name>) definitions overlap.
```

### Probable Cause

Indicates that a port is zoned with mixed devices (WWN and <domain, portarea>). During zoning database cross checking, it is detected that either:

- A port zone member is also listed as a member of a Mixed zone,
- A WWN zone member is also specified as a member of a Mixed zone.

You should use hard zone enforcement whenever possible. Hard zones are more secure than "session-based hard zones". Both types of zones will trap a PLOGI, but hard zones will filter out the I/O frames which "session-based" hard zones do not.

### Recommended Action

If hard zone enforcement is preferred, edit the zoning database to have the port zoned with devices defined as either WWN or defined as <domain, portarea> but do not mix the methods used to define these zone members.

### Severity

INFO

## ZONE-1006

### Message

```
<timestamp>, [ZONE-1006], <sequence-number>,, WARNING, <system-name>, WARNING - WWN(<WWN number>) in HARD PORT zone <zone_name>.
```

**Probable Cause** Indicates that one or more devices are zoned as WWN devices and also zoned as <domain, portarea> devices. The device(s) are used to specify zone members over separate zones.

**Recommended Action** If hardware zoning enforcement is preferred, edit the zoning database to have the device zoned using only one specification type, either WWN or <domain, portarea>.

**Severity** WARNING

## ZONE-1007

### Message

```
<timestamp>, [ZONE-1007], <sequence-number>,, INFO, <system-name>, Ioctl(<function>) in (<error message>) at port (<port number>) returns code (<error string>) and reason string (<reason string>)
```

**Probable Cause** Indicates that frame filter logic reported a failure during one of the IOCTL calls. The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding CAM entries before the filter setup.

**Recommended Action** There are two ways to avoid this problem.

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

**Severity** INFO

## ZONE-1008

### Message

```
<timestamp>, [ZONE-1008], <sequence-number>,, WARNING, <system-name>, WARNING - port <port number> Out of CAM entries
```

**Probable Cause** Indicates that the total number of entries of S\_ID CAM is above the limit while creating or adding a zone group. The maximum number of CAM entries allowed depends on the ASIC.

**Recommended Action** If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

**Severity** WARNING

## ZONE-1010

**Message**

```
<timestamp>, [ZONE-1010], <sequence-number>,, WARNING, <system-name>, WARNING - Duplicate entries in zone(<zone name>) specification.
```

**Probable Cause**

Indicates that there are duplicate entries in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

**Recommended Action**

Check the members of the zone and delete the duplicate member.

**Severity**

WARNING

## ZONE-1012

**Message**

```
<timestamp>, [ZONE-1012], <sequence-number>,, WARNING, <system-name>, WARNING - All ports are offline.
```

**Probable Cause**

Indicates that all the ports in a zone are offline.

**Recommended Action**

Check the device connection.

**Severity**

WARNING

## ZONE-1013

**Message**

```
<timestamp>, [ZONE-1013], <sequence-number>,, WARNING, <system-name>, Quick Loop not supported.
```

**Probable Cause**

Indicates that the QuickLoop feature is not supported in the current code release. If the QuickLoop zoning configuration is enabled on the switch, it will not be supported.

**Recommended Action**

Edit the zone database to remove the QuickLoop zoning definition in the effective configuration.

**Severity**

WARNING

## ZONE-1014

### Message

```
<timestamp>, [ZONE-1014], <sequence-number>,, ERROR, <system-name>,
Missing required license - <license name>.
```

### Probable Cause

Indicates that the required zoning license is missing.

### Recommended Action

Install the zoning license using the **licenseAdd** command. Refer to your switch supplier to obtain a zoning license if you do not have one.

### Severity

ERROR

## ZONE-1015

### Message

```
<timestamp>, [ZONE-1015], <sequence-number>,, WARNING, <system-
name>, Not owner of the current transaction <transaction ID>
```

### Probable Cause

Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administrators.

### Recommended Action

Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

### Severity

WARNING

## ZONE-1017

### Message

```
<timestamp>, [ZONE-1017], <sequence-number>,, ERROR, <system-name>,
FA Zone(<zone name>) contains incorrect number of Initiator and
Target devices
```

### Probable Cause

Indicates that the Fabric Assist (FA) zoning configuration has more than one initiator. The probable cause is incorrect entries in the FA zoning configuration.

### Recommended Action

Edit the zone database to ensure that only one initiator is set for each FA zone configuration.

### Severity

ERROR

## ZONE-1018

### Message

```
<timestamp>, [ZONE-1018], <sequence-number>,, ERROR, <system-name>,
Incorrect zoning enforcement type(<zone type>) at port(<port
number>)
```

### Probable Cause

Indicates that an incorrect zoning enforcement type was reported on the specified port. This is a software error. A QuickLoop zone type (value = 4) or an uninitialized type (value = 0) are invalid. The valid zone type values are:

- hard port zone (value = 1)
- hard wwn zone (value = 2)
- session based hard zoning (value = 3)
- FA zone (value = 5)

QuickLoop zones are not supported in Fabric OS v4.x.

### Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR

## ZONE-1019

### Message

```
<timestamp>, [ZONE-1019], <sequence-number>,, ERROR, <system-name>,
Transaction Commit failed. Reason code <reason code> (<Application
reason>) - \"<reason string>\"
```

### Probable Cause

Indicates that the Reliable Commit Service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

### Recommended Action

Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure that your changes to the zone database are not overwriting the work of another admin.

Run the **cfgTransShow** command to find out if there is any outstanding transaction running on the local switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

ERROR



## ZONE-1022

### Message

```
<timestamp>, [ZONE-1022], <sequence-number>,, INFO, <system-name>,
The effective configuration has changed
```

### Probable Cause

Indicates that the effective zone configuration has changed.

### Recommended Action

Verify that this zone configuration change was done on purpose. If the new effective zone configuration is correct, no action is necessary.

### Severity

INFO

## ZONE-1023

### Message

```
<timestamp>, [ZONE-1023], <sequence-number>,, INFO, <system-name>,
Switch connected to port (<port number>) is busy. Retry zone merge
```

### Probable Cause

Indicates that the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

### Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

### Severity

INFO

## ZONE-1024

### Message

```
<timestamp>, [ZONE-1024], <sequence-number>,, INFO, <system-name>,
<Information message>
```

### Probable Cause

Indicates that the **cfgSave** command ran successfully.

### Recommended Action

No action is required.

### Severity

INFO

## ZONE-1026

### Message

```
<timestamp>, [ZONE-1026], <sequence-number>,, INFO, <system-name>,
port <port number> Out of CAM entries
```

### Probable Cause

Indicates that the total number of S\_ID entries while creating or adding a zone group exceeds the limit.

### Recommended Action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

### Severity

INFO

## ZONE-1027

### Message

```
<timestamp>, [ZONE-1027], <sequence-number>,, ERROR, <system-name>,
Zoning transaction aborted - <error reason>
```

### Probable Cause

Indicates that the zoning transaction was aborted due to a variety of potential errors. The *error reason* variable can be one of the following:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new config is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

### Recommended Action

Many of the causes of this error message are transitory: for example because two admins are working with the zoning database concurrently. If you receive this error, wait a few minutes and try again. Verify that no one else is currently modifying the zone database.

### Severity

ERROR

## ZONE-1028

### Message

```
<timestamp>, [ZONE-1028], <sequence-number>,, WARNING, <system-
name>, Commit zone DB larger than supported - <zone db size> greater
than <max zone db size>
```

**Probable Cause** Indicates that the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

**Recommended Action** Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. Refer to the *Fabric OS Procedures Guide* for information on the zone database sizes supported for each switch.

**Severity** WARNING

## ZONE-1029

### Message

```
<timestamp>, [ZONE-1029], <sequence-number>,, WARNING, <system-name>, Restoring zone cfg from flash failed - bad config saved to <config file name> [<return code>]
```

**Probable Cause** Indicates that the zone configuration restored from the flash was faulty.

**Recommended Action** This error will save the bad zone configuration in the zoned core file directory. Run the **saveCore** command to save the file.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

**Severity** WARNING

## ZONE-1030

### Message

```
<timestamp>, [ZONE-1030], <sequence-number>,, WARNING, <system-name>, Converting the zone db for PID format change failed
```

**Probable Cause** Indicates that the current zone database could not be converted to reflect the PID format change. Most likely this is caused by the size of the database.

**Recommended Action** Change the PID format back to its original format. Then, correct the zone database. Usually this involves reducing the size of the database. Then, change the PID format back to the PID format you requested.

**Severity** WARNING



# Glossary

---

## A

- AL\_PA** Arbitrated-loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop. Alternately, “arbitrated-loop parameters.”
- alias** A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices, used to simplify the entry of port numbers and WWNs when creating zones.
- ARB** Arbitrative primitive signal. Applies only to an arbitrated-loop topology. Transmitted as the fill word by an L\_Port to indicate that the port is arbitrating access to the loop.
- area number** In Fabric OS v4.0 and above, ports on a switch are assigned a logical area number. Port area numbers can be viewed by entering the **switchshow** command. They are used to define the operative port for many Fabric OS commands: for example, area numbers can be used to define the ports within an alias or zone.
- ASIC** Application-specific integrated circuit.
- authentication** The process of verifying that an entity in a fabric (such as a switch) is what it claims to be. *See also* [digital certificate](#).
- autocommit** A feature of the **firmwaredownload** command. Enabled by default, **autocommit** commits new firmware to both partitions of a control processor.
- autoreboot** Refers to the **-b** option of the **firmwaredownload** command. Enabled by default.

## B

- backbone fabric** An optional capability that enables scalable meta-SANs by allowing the networking of multiple FC routers, which connect to the backbone fabric via EB\_Port interfaces.
- backup FCS switch** Relates to the Secure Fabric OS feature. The backup fabric configuration server serves as a backup in case the primary FCS switch fails. *See also* [FCS switch](#), [primary FCS switch](#).
- BB fabric** A backbone fabric that connects FC Routers. The FC Routers communicate over the backbone fabric using FCRP (Fibre Channel Router Protocol).
- BB\_Credit** Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. *See also* [buffer-to-buffer flow control](#), [EE\\_Credit](#).

<b>beacon</b>	A tool in which all of the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by a CLI command or through Advanced Web Tools.
<b>BISR</b>	Built-in self-repair.
<b>BIST</b>	Built-in self-test.
<b>broadcast</b>	The transmission of data from a single source to all devices in the fabric, regardless of zoning. <i>See also <a href="#">multicast</a>.</i>
<b>buffer-to-buffer flow control</b>	Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. <i>See also <a href="#">BB_Credit</a>.</i>

## C

<b>cascade</b>	Two or more interconnected Fibre Channel switches. SilkWorm 2000 and later switches can be cascaded up to 239 switches, with a recommended maximum of seven interswitch links (no path longer than eight switches). <i>See also <a href="#">fabric</a>, <a href="#">ISL</a>.</i>
<b>CHAP</b>	Challenge-Handshake Authentication Protocol. Allows remote servers and clients to securely exchange authentication credentials. Both the server and client are configured with the same shared secret.
<b>chassis</b>	The metal frame in which the switch and switch components are mounted.
<b>Class 1 service</b>	The class of frame-switching service for a dedicated connection between two communicating ports (also called “connection-oriented service”). Includes acknowledgement of frame delivery or nondelivery.
<b>Class 2 service</b>	A connectionless class of frame-switching service that includes acknowledgement of frame delivery or nondelivery.
<b>Class 3 service</b>	A connectionless class of frame-switching service that does not include acknowledgement of frame delivery or nondelivery. Can be used to provide a multicast connection between the frame originator and recipients, with acknowledgement of frame delivery or nondelivery.
<b>Class 4 service</b>	A connection-oriented service that allows fractional parts of the bandwidth to be used in a virtual circuit.
<b>Class 6 service</b>	A connection-oriented multicast service geared toward video broadcasts between a central server and clients.
<b>Class F service</b>	The class of frame-switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports. Includes acknowledgement of data delivery or nondelivery.
<b>class of service</b>	A specified set of delivery characteristics and attributes for frame delivery.

<b>CLI</b>	Command line interface. An interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.
<b>client</b>	An entity that, using its common transport (CT), makes requests of a server.
<b>community (SNMP)</b>	A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. <i>See also</i> <a href="#">SNMP</a> .
<b>compact flash</b>	Flash (temporary) memory that is used in a manner similar to hard disk storage. It is connected to a bridging component that connects to the PCI bus of the processor. Not visible within the processor's memory space.
<b>configuration</b>	(1) A set of parameters that can be modified to fine-tune the operation of a switch. Run the <b>configshow</b> command to view the current configuration of your switch.  (2) In Zoning, a zoning element that contains a set of zones. The Configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. <i>See also</i> <a href="#">zone configuration</a> .
<b>congestion</b>	The realization of the potential of oversubscription. A congested link is one on which multiple devices are contending for bandwidth.
<b>core PID</b>	Core switch port identifier. The core PID must be set for v3.1 and earlier switches included in a fabric of v4.1 switches. This parameter is located in the <b>configure</b> command of firmware versions v3.1 and earlier. All v4.1 switches and above use the core PID format by default; this parameter is not present in the <b>configure</b> command for these switches.
<b>CSCN</b>	Common services connection framework.
<b>D</b>	
<b>defined zone configuration</b>	The set of all zone objects defined in the fabric. Can include multiple zone configurations. <i>See also</i> <a href="#">enabled zone configuration</a> , <a href="#">zone configuration</a> .
<b>deskew</b>	Related to the Trunking feature. The time difference between traffic traveling over each ISL other than the shortest ISL in the group and traffic traveling over that shortest ISL. The deskew number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.
<b>DH-CHAP</b>	Diffie-Hellman Challenge-Handshake Authentication Protocol. An implementation of CHAP using Diffie-Hellman encryption. <i>See also</i> <a href="#">CHAP</a> .
<b>digital certificate</b>	An electronic document issued by a CA (certificate authority) to an entity, containing the public key and identity of the entity. Entities in a secure fabric are authenticated based on these certificates. <i>See also</i> <a href="#">authentication</a> , <a href="#">public key</a> .
<b>director</b>	A SilkWorm 12000, or 24000 switch.
<b>domain ID</b>	A unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch but can be assigned manually. The domain ID for a SilkWorm switch can be any integer between 1 and 239.

## E

<b>E_Port</b>	Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. <i>See also</i> <a href="#">ISL</a> .
<b>edge fabric</b>	A Fibre Channel fabric connected to an FC router via an EX_Port (where hosts and storage are attached in a meta-SAN).
<b>EE_Credit</b>	End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage frame exchange across the fabric, between source and destination. <i>See also</i> <a href="#">BB_Credit</a> .
<b>ELS</b>	Fibre Channel - Extended Link Services Frame.
<b>EM</b>	Environmental monitor. Monitors FRUs and reports failures.
<b>enabled zone configuration</b>	The currently enabled configuration of zones. Only one configuration can be enabled at a time. <i>See also</i> <a href="#">defined zone configuration</a> , <a href="#">zone configuration</a> .
<b>error</b>	As it applies to the Fibre Channel industry, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors).
<b>Ethernet</b>	Popular protocols for LANs.
<b>EX_Port</b>	A type of E_Port that connects an FC router to an edge fabric. EX_Ports limit the scope of fabric services scope but provide device connectivity using FC-NAT.
<b>exchange</b>	The highest-level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, it can work in either one or both directions.

## F

<b>fabric</b>	A collection of Fibre Channel switches and devices, such as hosts and storage. Also referred to as a “switched fabric.” <i>See also</i> <a href="#">cascade</a> , <a href="#">SAN</a> , <a href="#">topology</a> .
<b>Fabric Manager</b>	An optionally licensed software feature. Fabric Manager is a GUI that allows for fabric-wide administration and management. Switches can be treated as groups, and actions such as firmware downloads can be performed simultaneously.
<b>fabric name</b>	The unique identifier assigned to a fabric and communicated during login and port discovery.
<b>fabric port count</b>	The number of ports available for connection by nodes in a fabric.
<b>Fabric Watch</b>	An optionally licensed software feature. Fabric Watch can be accessed through either the command line or Advanced Web Tools, and it provides the ability to set thresholds for monitoring fabric conditions.
<b>failover</b>	Describes the SilkWorm 12000 process of one CP passing active status to another CP. A failover is nondisruptive.



<b>FC router</b>	A platform running the Brocade Fibre Channel Routing Service or FC-to-FC routing (for instance, the SilkWorm Fabric AP7420) that enables two or more fabrics to share resources (such hosts or storage devices) without merging those fabrics. The platform could simultaneously be used as an FC router and as an FCIP tunnel or iSCSI gateway.
<b>FCIP</b>	Fibre Channel over IP.
<b>FCS switch</b>	Relates to the Brocade Secure Fabric OS feature. One or more designated switches that store and manage security parameters and configuration data for all switches in the fabric. They also act as a set of backup switches to the primary FCS switch. <i>See also</i> <a href="#">backbone fabric</a> , <a href="#">primary FCS switch</a> .
<b>FC-SW-2</b>	The second-generation Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches to create a multiswitch Fibre Channel fabric.
<b>FDDI</b>	Fibre Distributed Data Interface. An ANSI architecture for a metropolitan area network (MAN); a network based on the use of fiber-optic cable to transmit data at 100 Mbit/sec.
<b>FDMI</b>	Fabric-Device Management Interface. FDMI is a database service provided by the fabric for Nx_Ports. The primary use is by HBA devices that register information about themselves and their ports.
<b>FFFFF5</b>	Well-known Fibre Channel address for a Class 6 multicast server.
<b>FFFFF6</b>	Well-known Fibre Channel address for a clock synchronization server.
<b>FFFFF7</b>	Well-known Fibre Channel address for a security key distribution server.
<b>FFFFF8</b>	Well-known Fibre Channel address for an alias server.
<b>FFFFF9</b>	Well-known Fibre Channel address for a QoS facilitator.
<b>FFFFFA</b>	Well-known Fibre Channel address for a management server.
<b>FFFFFB</b>	Well-known Fibre Channel address for a time server.
<b>FFFFFC</b>	Well-known Fibre Channel address for a directory server.
<b>FFFFFD</b>	Well-known Fibre Channel address for a fabric controller.
<b>FFFFFE</b>	Well-known Fibre Channel address for a fabric F_Port.
<b>FFFFFF</b>	Well-known Fibre Channel address for a broadcast alias ID.
<b>Fibre Channel</b>	The primary protocol used for building SANs to transmit data between servers, switches, and storage devices. Unlike IP and Ethernet, Fibre Channel was designed to support the needs of storage devices of all types. It is a high-speed, serial, bidirectional, topology-independent, multiprotocol, and highly scalable interconnection between computers, peripherals, and networks.
<b>Fibre Channel transport</b>	A protocol service that supports communication between Fibre Channel service providers.

<b>FICON®</b>	A protocol used on IBM mainframes. Brocade SilkWorm switch FICON support enables a SilkWorm fabric to transmit FICON format data between FICON-capable servers and storage.
<b>FID</b>	Fabric ID. Unique identifier of a fabric in a meta-SAN.
<b>FIFO</b>	First in, first out. Refers to a data buffer that follows the first in, first out rule.
<b>fill word</b>	An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.
<b>firmware</b>	The basic operating system provided with the hardware.
<b>FL_Port</b>	Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated-loop capabilities. Can be used to connect an NL_Port to a switch. <i>See also</i> <a href="#">Fx_Port</a> .
<b>flash</b>	Programmable nonvolatile RAM (NVRAM) memory that maintains its contents without power.
<b>FLOGI</b>	Fabric login. The process by which an N_Port determines whether a fabric is present and, if so, exchanges service parameters with it. <i>See also</i> <a href="#">PLOGI</a> .
<b>frame</b>	The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements and so forth) and data frames.
<b>frame relay</b>	A protocol that uses logical channels, as used in X.25. Provides very little error-checking ability. Discards frames that arrive with errors. Allows a certain level of bandwidth between two locations (known as a "committed information rate": CIR) to be guaranteed by service provider. If CIR is exceeded for short periods (known as "bursts"), the network accommodates the extra data, if spare capacity is available. Frame relay is therefore known as "bandwidth on demand."
<b>FRU</b>	Field-replaceable unit. A component that can be replaced onsite.
<b>FSPF</b>	Fabric shortest path first. The Brocade routing protocol for Fibre Channel switches.
<b>FSS</b>	Fabric OS state synchronization. The FSS service is related to high availability (HA). The primary function of FSS is to deliver state update messages from active components to their peer standby components. FSS determines if fabric elements are synchronized (and thus FSS "compliant").
<b>FTP</b>	File Transfer Protocol.
<b>full fabric</b>	The Brocade software license that allows multiple E_Ports on a switch, making it possible to create multiple ISL links.
<b>full duplex</b>	A mode of communication that allows the same port to simultaneously transmit and receive frames. <i>See also</i> <a href="#">half duplex</a> .
<b>Fx_Port</b>	A fabric port that can operate as either an F_Port or FL_Port. <i>See also</i> <a href="#">FL_Port</a> .

## G

<b>G_Port</b>	Generic port. A port that can operate as either an E_Port or an F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.
<b>gateway</b>	Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.
<b>GBIC</b>	Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet.
<b>Gbit/sec</b>	Gigabits per second (1,062,500,000 bits/second).
<b>GB/sec</b>	Gigabytes per second (1,062,500,000 bytes/second).
<b>GLM</b>	Gigabit Link Module. A semitransparent transceiver that incorporates serializing/deserializing functions.
<b>GMT</b>	Greenwich Mean Time. An international time zone. Also known as "UTC."
<b>GUI</b>	A graphic user interface, such as Brocade Advanced Web Toolsarbitrated-loop topology and Brocade Fabric Manager.

## H

<b>HA</b>	High availability. A set of features in Brocade SilkWorm switches that is designed to provide maximum reliability and nondisruptive replacement of key hardware and software modules.
<b>half duplex</b>	A mode of communication that allows a port to either transmit or receive frames at any time except simultaneously (with the exception of link control frames, which can be transmitted at any time). <i>See also</i> <a href="#">full duplex</a> .
<b>hard address</b>	The AL_PA that an NL_Port attempts to acquire during loop initialization.
<b>Hardware Translative Mode</b>	A method for achieving address translation. There are two hardware translative modes available to a QuickLoop enabled switch: Standard Translative Mode and QuickLoop Mode.
<b>HBA</b>	Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.
<b>hop count</b>	The number of ISLs a frame must traverse to get from its source to its destination.
<b>host</b>	A computer system that provides end users with services like computation and storage access.
<b>hot swappable</b>	A hot swappable component can be replaced under power.
<b>HTTP</b>	Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

**hub** A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

## I

**ICT** Intracircuit test.

**ID\_ID** Insistent domain ID. A parameter of the **configure** command in the Brocade Fabric OS.

**Insistent Domain ID Mode** Sets the domain ID of a switch as insistent, so that it remains the same over reboots, power cycles, failovers, and fabric reconfigurations. This mode is required to support FICON® traffic.

**integrated fabric** The fabric created by a Brocade SilkWorm 6400, consisting of six SilkWorm 2250 switches cabled together and configured to handle traffic seamlessly as a group.

**IOCTL** I/O control.

**iSCSI** Internet Small Computer Systems Interface. A protocol that defines the processes for transferring block storage applications over TCP/IP networks by encapsulating SCSI commands into TCP and transporting them over the network via IP.

**iSCSI Gateway Service** The Brocade multiprotocol SAN routing service that maps the FCP protocol to the IP transport. This service projects iSCSI hosts onto the backbone fabric of a gateway switch.

**ISL** Interswitch link. A Fibre Channel link from the E\_Port of one switch to the E\_Port of another. *See also cascade, E\_Port.*

**ISP** Internet service provider.

## J

**JBOD** "Just a bunch of disks." Indicates a number of disks connected in a single chassis to one or more controllers. *See also RAID.*

**jitter** A deviation in timing for a bit stream as it flows through a physical medium.

## K

**key** A string of data (usually a numeric value) shared between two entities and used to control a cryptographic algorithm. Usually selected from a large pool of possible keys to make unauthorized identification of the key difficult. *See also key pair.*

**key pair** In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret.

## L

<b>L_Port</b>	Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated-loop capabilities. An L_Port can be in either Fabric Mode or Loop Mode.
<b>LAN</b>	Local area network. A network in which transmissions typically take place over fewer than 5 kilometers (3.4 miles).
<b>latency</b>	The time required to transmit a frame. Together, latency and bandwidth define the speed and capacity of a link or system.
<b>LED</b>	Light-emitting diode. Used to indicate the status of elements on a switch.
<b>login server</b>	The unit that responds to login requests.
<b>Loop Mode</b>	One of two possible modes for an L_Port, in which the L_Port is in an arbitrated loop, using loop protocol. An L_Port in Loop Mode can also be in Participating Mode or Nonparticipating Mode.
<b>LSAN</b>	Logical storage area network. An LSAN enables device and storage connectivity that spans two or more fabrics. The path between devices in an LSAN can be local to a fabric or cross one or more FC routers and one or more backbone fabrics.
<b>LSAN zone</b>	The mechanism by which LSANs are administered. An FC router attached to two fabrics will “listen” for the creation of matching LSAN zones on both fabrics. If this occurs, it will create phantom domains and FC-NAT entries as appropriate, and insert entries for them into the name servers on the fabrics. LSAN zones are compatible with all standard zoning mechanisms.

## M

<b>MALLOC</b>	Memory allocation. Usually relates to buffer credits.
<b>meta-SAN</b>	The collection of all devices, switches, edge and backbone fabrics, LSANs, and FC routers that make up a physically connected but logically partitioned storage network. LSANs span between edge fabrics using FC routers. In a data network, this would simply be called “the network.” However, an additional term is required to specify the difference between a single-fabric network (“SAN”), a multifabric network without cross-fabric connectivity (“dual-redundant fabric SAN”), and a multifabric network with connectivity (“meta-SAN”).
<b>MIB</b>	Management Information Base. An SNMP structure to help with device management, providing configuration and device information.
<b>MS</b>	Management Server. The Management Server allows a storage area network (SAN) management application to retrieve information and administer the fabric and interconnected elements, such as switches, servers, and storage devices. The MS is located at the Fibre Channel well-known address FFFFFAh.
<b>MTBF</b>	Mean time between failures. An expression of time, indicating the longevity of a device.
<b>multicast</b>	The transmission of data from a single source to multiple specified N_Ports (as opposed to all the ports on the network). <i>See also</i> <a href="#">broadcast</a> .

**multimode** A fiber optic cabling specification that allows up to 500 meters between devices.

## N

**N\_Port** Node port. A port on a node that can connect to a Fibre Channel port or to another N\_Port in a point-to-point connection. *See also* [NL\\_Port](#), [Nx\\_Port](#).

**Name Server** Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as "directory service."

**NAS** Network-attached storage. A disk array connected to a controller that gives access via a LAN.

**NIC** Network interconnect card.

**NL\_Port** Node loop port. A node port that has arbitrated-loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL\_Port. *See also* [N\\_Port](#), [Nx\\_Port](#).

**node** A Fibre Channel device that contains an N\_Port or NL\_Port.

**node count** The number of nodes attached to a fabric.

**node name** The unique identifier for a node, communicated during login and port discovery.

**NR\_Port** A normal E\_Port used to connect an FC Router to a backbone fabric.

**NS** Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also known as "Simple Name Server" or as a "directory service." *See also* [Simple Name Server \(SNS\)](#).

**Nx\_Port** A node port that can operate as either an N\_Port or NL\_Port.

## O

**oversubscription** A situation in which more nodes could potentially contend for a resource than the resource could simultaneously support (typically an ISL). Oversubscription could be a desirable attribute in fabric topology, as long as it does not produce unacceptable levels of congestion.

**OX\_ID** Originator ID or exchange ID. Refers to the exchange ID assigned by the originator port.

## P

**payload** A Fibre Channel frame has a header and a payload. The payload contains the information being transported by the frame; it is determined by the higher-level service or FC\_4 upper-level protocol. There are many different payload formats, based on protocol.

**PBC** Port bypass circuit. A circuit in hubs or a disk enclosure to open or close a loop to add or remove nodes.

**PCBA** Printed circuit board assembly.

<b>PCM</b>	Pulse-code modulation. A standard method of encoding analog audio signals in digital form.
<b>Performance Monitoring</b>	A Brocade SilkWorm switch feature that monitors port traffic and includes frame counters, SCSI read monitors, SCSI write monitors, and other types of monitors.
<b>phantom device</b>	A device that is not physically in an arbitrated-loop but is logically included through the use of a phantom address.
<b>phantom domain</b>	<i>See</i> <a href="#">xlate domain</a> .
<b>PID</b>	Port identifier. <i>See also</i> <a href="#">core PID</a> .
<b>PKI</b>	Public key infrastructure. An infrastructure that is based on public key cryptography and CA (certificate authority) and that uses digital certificates. <i>See also</i> <a href="#">digital certificate</a> .
<b>PKI certification utility</b>	Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and to load certificates to switches. <i>See also</i> <a href="#">digital certificate</a> , <a href="#">PKI</a> .
<b>PLOGI</b>	Port login. The port-to-port login process by which initiators establish sessions with targets. <i>See also</i> <a href="#">FLOGI</a> .
<b>port</b>	In a Brocade SilkWorm switch environment, an SFP or GBIC receptacle on a switch to which an optic cable for another device is attached.
<b>port address</b>	In Fibre Channel technology, the port address is defined in hexadecimal. In the Brocade Fabric OS, a port address can be defined by a domain and port number combination or by area number. In an ESCON Director, an address used to specify port connectivity parameters and to assign link addresses for attached channels and control units.
<b>port name</b>	A user-defined alphanumeric name for a port.
<b>port swapping</b>	Port swapping is the ability to redirect a failed port to another port. This feature is available in Fabric OS v4.1.0 and higher.
<b>port_name</b>	The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.
<b>POST</b>	Power-on self-test. A series of tests run by a switch after it is turned on.
<b>primary FCS switch</b>	Relates to the Brocade Secure Fabric OS feature. The primary fabric configuration server switch actively manages security and configurations for all switches in the fabric. <i>See also</i> <a href="#">backbone fabric</a> , <a href="#">FCS switch</a> .
<b>principal switch</b>	The first switch to boot up in a fabric. Ensures unique domain IDs among roles.
<b>private device</b>	A device that supports arbitrated-loop protocol and can interpret 8-bit addresses but cannot log in to the fabric.
<b>private key</b>	The secret half of a key pair. <i>See also</i> <a href="#">key</a> , <a href="#">key pair</a> .

<b>private loop</b>	An arbitrated loop that does not include a participating FL_Port.
<b>private loop device</b>	A device that supports a loop and can understand 8-bit addresses but does not log in to the fabric.
<b>private NL_Port</b>	An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to the fabric.
<b>protocol</b>	A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.
<b>pstate</b>	Port State Machine.
<b>public device</b>	A device that supports arbitrated-loop protocol, can interpret 8-bit addresses, and can log in to the fabric.
<b>public key</b>	The public half of a key pair. <i>See also</i> <a href="#">key</a> , <a href="#">key pair</a> .

## Q

<b>queue</b>	A mechanism for each AL_PA address that allows for collecting frames prior to sending them to the loop.
<b>QuickLoop</b>	A Brocade software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.
<b>QuickLoop Mode</b>	Allows initiator devices to communicate with private or public devices that are not in the same loop.

## R

<b>R_RDY</b>	Receiver ready. A primitive signal indicating that the port is ready to receive a frame.
<b>radius</b>	The greatest "distance" between any edge switch and the center of a fabric. A low-radius network is better than a high-radius network.
<b>RAID</b>	Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. <i>See also</i> <a href="#">JBOD</a> .
<b>RCS</b>	Reliable Commit Service. Refers to Brocade-specific ILS command code.
<b>RCS_SFC</b>	RCS Stage Fabric Config. Refers to Brocade-specific ILS command code.
<b>RLS</b>	Read Link Status.
<b>route</b>	As it applies to a fabric, the communication path between two switches. Might also apply to the specific path taken by an individual frame, from source to destination. <i>See also</i> <a href="#">FSPF</a> .
<b>routing</b>	The assignment of frames to specific switch ports, according to frame destination.



- RR\_TOV** Resource recovery timeout value. The minimum time a target device in a loop waits after an LIP before logging out an SCSI initiator.
- RSCN** Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes. The fabric controller issues RSCN requests to N\_Ports and NL\_Ports, but only if they have registered to be notified of state changes in other N\_Ports and NL\_Ports. This registration is performed via the State Change Registration (SCR) Extended Link Service. An N\_Port or NL\_Port can issue an RSCN to the fabric controller without having completed SCR with the fabric controller.
- RTWR** Reliable transport with response. Might appear as a task in **portlogdump** command output.
- RW** Read/write. Refers to access rights.
- RX** Receiving frames.

## S

- SAN** Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also* [fabric](#).
- SCC** SC connector. An SC connector is a fiber-optic cable connector that uses a push-pull latching mechanism similar to common audio and video cables. For bidirectional transmissions, two fiber cables and two SC connectors (dual SC) are generally used. SC is specified by the TIA as FOCIS-3.
- SCN** State change notification. Used for internal state change notifications, not external changes. This is the switch logging that the port is online or is an Fx\_Port, not what is sent from the switch to the Nx\_Ports.
- SCR** State change registration. Extended Link Service (ELS) requests the fabric controller to add the N\_Port or NL\_Port to the list of N\_Ports and NL\_Ports registered to receive the Registered State Change Notification (RSCN) Extended Link Service.
- SCSI** Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks to a distance of 15 to 25 meters.
- SCSI-2** An updated version of the SCSI bus architecture.
- SCSI-3** An SCSI standard that defines transmission of SCSI protocol data over different kinds of links.
- SDRAM** The main memory for a switch.
- sectelnet** A protocol similar to telnet but with encrypted passwords for increased security.
- Secure Fabric OS** An optionally licensed Brocade feature that provides advanced, centralized security for a fabric.
- security policy** Rules that determine how security is implemented in a fabric. Security policies can be customized through Brocade Secure Fabric OS or Brocade Fabric Manager.
- server** A computer that processes end-user applications or requests.

<b>SES</b>	SCSI Enclosure Services. A subset of the SCSI protocol used to monitor temperature, power, and fan status for enclosed devices.
<b>SFP</b>	Small-form-factor pluggable. A transceiver used on 2 GB/sec switches that replaces the GBIC.
<b>SilkWorm</b>	The brand name for the Brocade family of switches.
<b>Simple Name Server (SNS)</b>	A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as “directory service” or “name server.”
<b>SLAP</b>	Switch Link Authentication Protocol.
<b>SLP</b>	Service Location Protocol.
<b>SNMP</b>	Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. <i>See also</i> <a href="#">community (SNMP)</a> .
<b>SNS</b>	Simple Name Server.
<b>SOF</b>	Start of frame. A group of ordered sets that marks the beginning of a frame and indicates the class of service the frame will use.
<b>soft zone</b>	A zone consisting of zone members that are made visible to each other through client service requests. Typically, soft zones contain zone members that are visible to devices using Name Server exposure of zone members. The fabric does not enforce a soft zone. Note that well-known addresses are implicitly included in every zone.
<b>SSH</b>	Secure shell. Used starting in Brocade Fabric OS v4.1 to support encrypted telnet sessions to the switch. SSH encrypts all messages, including the client sending the password at login.
<b>SSL</b>	Secure sockets layer.
<b>Standard Translative Mode</b>	Allows public devices to communicate with private devices that are directly connected to the fabric.
<b>striping</b>	A RAID technique for writing a file to multiple disks on a block-by-block basis, with or without parity.
<b>switch</b>	A fabric device providing bandwidth and high-speed routing of data via link-level addressing.
<b>switch name</b>	The arbitrary name assigned to a switch.
<b>switch port</b>	A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.
<b>syslog</b>	Syslog daemon. Used to forward error messages.

## T

<b>target</b>	A storage device on a Fibre Channel network.
<b>TC</b>	Track changes.
<b>TCP/IP</b>	Transmission Control Protocol Internet Protocol.
<b>telnet</b>	A virtual terminal emulation used with TCP/IP. “Telnet” is sometimes used as a synonym for the Brocade Fabric OS CLI.
<b>throughput</b>	The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second or b/sec). <i>See also</i> <a href="#">BB fabric</a> .
<b>Time Server</b>	A Fibre Channel service that allows for the management of all timers.
<b>topology</b>	As it applies to Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies: <ul style="list-style-type: none"><li><b>Point to point.</b> A direct link between two communication ports.</li><li><b>Switched fabric.</b> Multiple N_Ports linked to a switch by F_Ports.</li><li><b>Arbitrated loop.</b> Multiple NL_Ports connected in a loop.</li></ul>
<b>track changes</b>	A Brocade Fabric OS feature that can be enabled to report specific activities (for example, logins, logouts, and configuration task changes). The output from the track-changes feature is dumped to the error log for the switch.
<b>transceiver</b>	A device that converts one form of signaling to another for transmission and reception; in fiber optics, optical to electrical.
<b>translate domain</b>	<i>See</i> <a href="#">xlate domain</a> .
<b>Translative Mode</b>	A mode in which private devices can communicate with public devices across the fabric.
<b>transmission character</b>	A 10-bit character encoded according to the rules of the 8b/10b algorithm.
<b>transmission word</b>	A group of four transmission characters.
<b>trap (SNMP)</b>	The message sent by an SNMP agent to inform the SNMP management station of a critical error. <i>See also</i> <a href="#">SNMP</a> .
<b>trunking</b>	In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.
<b>trunking group</b>	A set of up to four trunked ISLs.
<b>trunking ports</b>	The ports in a set of trunked ISLs.

**TS** Time Server.

**tunneling** A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network but are connected by a different type of network.

**TX** Transmit.

## U

**U\_Port** Universal port. A switch port that can operate as a G\_Port, E\_Port, F\_Port, or FL\_Port. A port is defined as a U\_Port when it is not connected or has not yet assumed a specific function in the fabric.

## V

## W

**WAN** Wide area network.

**WAN\_TOV** Wide area network timeout value.

**well-known address** As it pertains to Fibre Channel technology, a logical address defined by Fibre Channel standards as assigned to a specific function and stored on the switch.

**workstation** A computer used to access and manage the fabric. Also referred to as a “management station” or “host.”

**WWN** World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

## X

**xlate domain** Translate domain. A router virtual domain that represents an entire fabric. Device connectivity can be achieved from one fabric to another, over the router and through this virtual domain, without merging the two fabrics. Also known as “phantom domains.”

## Y

## Z

**zone** A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

**zone configuration** A specified set of zones. Enabling a configuration enables all zones in that configuration. *See also* [defined zone configuration](#), [enabled zone configuration](#).

**zoning** A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.

# Index

---

## A

audit field 1-3  
AUTH-1001 2-1  
AUTH-1002 2-1  
AUTH-1003 2-1  
AUTH-1004 2-2  
AUTH-1005 2-2  
AUTH-1006 2-2  
AUTH-1007 2-3  
AUTH-1008 2-3  
AUTH-1010 2-3  
AUTH-1011 2-4  
AUTH-1012 2-4  
AUTH-1013 2-5  
AUTH-1014 2-5  
AUTH-1017 2-5  
AUTH-1018 2-6  
AUTH-1020 2-6  
AUTH-1022 2-7  
AUTH-1023 2-7  
AUTH-1025 2-8  
AUTH-1027 2-8  
AUTH-1028 2-8  
AUTH-1029 2-9  
AUTH-1030 2-9  
AUTH-1031 2-10  
AUTH-1032 2-10  
AUTH-1033 2-11  
AUTH-1034 2-11  
AUTH-1035 2-11  
AUTH-1036 2-12  
AUTH-1037 2-12  
AUTH-1038 2-13

## B

BL-1000 3-1  
BL-1001 3-1  
BL-1002 3-1  
BL-1003 3-2  
BL-1004 3-2  
BL-1006 3-3

BL-1007 3-3  
BL-1008 3-3  
BL-1009 3-4  
BL-1010 3-4  
BL-1011 3-5  
BL-1012 3-5  
BL-1013 3-6  
BL-1014 3-6  
BL-1015 3-7  
BL-1016 3-7  
BLL-1000 4-1

## C

CER-1001 5-1  
changes for this release of the Fabric OS 1-1  
clearing the system message log 1-10  
core dump files 1-5

## D

dual-CP systems 1-4  
dumping the system messages 1-9

## E

EM-1001 6-1  
EM-1002 6-1  
EM-1003 6-2  
EM-1004 6-2  
EM-1005 6-3  
EM-1006 6-4  
EM-1007 6-4  
EM-1008 6-4  
EM-1009 6-5  
EM-1010 6-5  
EM-1011 6-6  
EM-1012 6-6  
EM-1013 6-6  
EM-1014 6-7  
EM-1015 6-8

EM-1016 6-8  
 EM-1017 6-8  
 EM-1028 6-9  
 EM-1029 6-10  
 EM-1031 6-10  
 EM-1033 6-11  
 EM-1034 6-11  
 EM-1036 6-12  
 EM-1041 6-12  
 EM-1042 6-13  
 EM-1043 6-14  
 EM-1044 6-14  
 EM-1045 6-14  
 EM-1046 6-15  
 EM-1047 6-15  
 EM-1048 6-16  
 EM-1049 6-16  
 EM-1050 6-17  
 EM-1051 6-18  
 EM-1052 6-18  
 EM-1053 6-19  
 EM-1055 6-19  
 EM-1056 6-20  
 EVMD-1001 7-1  
 example system message 1-8

## F

FABR-1001 8-1  
 FABR-1002 8-1  
 FABR-1003 8-2  
 FABR-1004 8-2  
 FABR-1005 8-3  
 FABR-1006 8-3  
 FABR-1007 8-3  
 FABR-1008 8-4  
 FABR-1009 8-4  
 FABR-1010 8-4  
 FABR-1011 8-5  
 FABR-1012 8-5  
 FABR-1013 8-5  
 FABR-1014 8-6  
 FABR-1015 8-6  
 FABR-1016 8-7  
 FABR-1017 8-7  
 FABR-1018 8-7  
 FABR-1019 8-8  
 FABR-1020 8-8  
 FABR-1021 8-8  
 FABR-1022 8-9  
 FABR-1023 8-9

FABR-1024 8-10  
 FABR-1029 8-10  
 FABS-1001 9-1  
 FABS-1002 9-1  
 FABS-1004 9-1  
 FABS-1005 9-2  
 FABS-1006 9-2  
 FABS-1007 9-3  
 FABS-1008 9-3  
 FABS-1009 9-3  
 FABS-1010 9-4  
 FCMC-1001 10-1  
 FCPD-1001 11-1  
 FCPD-1002 11-1  
 FCPD-1003 11-2  
 FCPH-1001 12-1  
 Fibre Channel Association XXXIX  
 FICU-1001 13-1  
 FICU-1002 13-1  
 FICU-1003 13-2  
 FICU-1004 13-2  
 FICU-1005 13-2  
 FICU-1006 13-3  
 FICU-1007 13-3  
 FICU-1008 13-3, 13-4  
 FKLB-1001 14-1  
 FLOD-1001 15-1  
 FLOD-1003 15-1  
 FLOD-1004 15-1  
 FLOD-1005 15-2  
 FLOD-1006 15-2  
 FSPF-1001 16-1  
 FSPF-1002 16-1  
 FSPF-1003 16-1  
 FSPF-1005 16-2  
 FSPF-1006 16-2  
 FSS-1001 17-1  
 FSS-1002 17-1  
 FSS-1003 17-2  
 FSS-1004 17-2  
 FSS-1005 17-2  
 FSS-1006 17-3  
 FSSM-1002 18-1  
 FSSM-1003 18-1  
 FSSM-1004 18-2  
 FW-1001 19-1  
 FW-1002 19-1  
 FW-1003 19-2  
 FW-1004 19-2  
 FW-1005 19-2  
 FW-1006 19-3  
 FW-1007 19-3

FW-1008	19-3	FW-1140	19-22
FW-1009	19-4	FW-1141	19-23
FW-1010	19-4	FW-1142	19-23
FW-1011	19-4	FW-1143	19-23
FW-1012	19-5	FW-1144	19-24
FW-1033	19-5	FW-1160	19-24
FW-1034	19-5	FW-1161	19-24
FW-1035	19-6	FW-1162	19-25
FW-1036	19-6	FW-1163	19-25
FW-1037	19-6	FW-1164	19-26
FW-1038	19-7	FW-1165	19-26
FW-1039	19-7	FW-1166	19-26
FW-1040	19-7	FW-1167	19-27
FW-1041	19-8	FW-1168	19-27
FW-1042	19-8	FW-1169	19-27
FW-1043	19-8	FW-1170	19-28
FW-1044	19-9	FW-1171	19-28
FW-1045	19-9	FW-1172	19-29
FW-1046	19-10	FW-1173	19-29
FW-1047	19-10	FW-1174	19-29
FW-1048	19-10	FW-1175	19-30
FW-1049	19-11	FW-1176	19-30
FW-1050	19-11	FW-1177	19-30
FW-1051	19-11	FW-1178	19-31
FW-1052	19-12	FW-1179	19-31
FW-1113	19-12	FW-1180	19-31
FW-1114	19-12	FW-1181	19-32
FW-1115	19-13	FW-1182	19-32
FW-1116	19-13	FW-1183	19-32
FW-1117	19-13	FW-1184	19-33
FW-1118	19-14	FW-1185	19-33
FW-1119	19-14	FW-1186	19-33
FW-1120	19-15	FW-1187	19-34
FW-1121	19-15	FW-1188	19-34
FW-1122	19-15	FW-1189	19-34
FW-1123	19-16	FW-1190	19-35
FW-1124	19-16	FW-1191	19-35
FW-1125	19-17	FW-1192	19-35
FW-1126	19-17	FW-1193	19-36
FW-1127	19-18	FW-1194	19-36
FW-1128	19-18	FW-1195	19-36
FW-1129	19-19	FW-1216	19-37
FW-1130	19-19	FW-1217	19-37
FW-1131	19-19	FW-1218	19-38
FW-1132	19-20	FW-1219	19-38
FW-1133	19-20	FW-1240	19-38
FW-1134	19-20	FW-1241	19-39
FW-1135	19-21	FW-1242	19-39
FW-1136	19-21	FW-1243	19-40
FW-1137	19-21	FW-1244	19-40
FW-1138	19-22	FW-1245	19-40
FW-1139	19-22	FW-1246	19-41

FW-1247	19-41	FW-1339	19-61
FW-1248	19-41	FW-1340	19-61
FW-1249	19-42	FW-1341	19-62
FW-1250	19-42	FW-1342	19-62
FW-1251	19-42	FW-1343	19-63
FW-1272	19-43	FW-1344	19-63
FW-1273	19-43	FW-1345	19-63
FW-1274	19-44	FW-1346	19-64
FW-1275	19-44	FW-1347	19-64
FW-1296	19-44	FW-1348	19-65
FW-1297	19-45	FW-1349	19-65
FW-1298	19-45	FW-1350	19-66
FW-1299	19-46	FW-1351	19-66
FW-1300	19-46	FW-1352	19-66
FW-1301	19-46	FW-1353	19-67
FW-1302	19-47	FW-1354	19-67
FW-1303	19-47	FW-1355	19-68
FW-1304	19-48	FW-1356	19-68
FW-1305	19-48	FW-1357	19-68
FW-1306	19-48	FW-1358	19-69
FW-1307	19-49	FW-1359	19-69
FW-1308	19-49	FW-1360	19-70
FW-1309	19-50	FW-1361	19-70
FW-1310	19-50	FW-1362	19-70
FW-1311	19-50	FW-1363	19-71
FW-1312	19-51	FW-1364	19-71
FW-1313	19-51	FW-1365	19-71
FW-1314	19-51	FW-1366	19-72
FW-1315	19-52	FW-1367	19-72
FW-1316	19-52	FW-1368	19-72
FW-1317	19-52	FW-1369	19-73
FW-1318	19-53	FW-1370	19-73
FW-1319	19-53	FW-1371	19-73
FW-1320	19-54	FW-1372	19-74
FW-1321	19-54	FW-1373	19-74
FW-1322	19-54	FW-1374	19-75
FW-1323	19-55	FW-1375	19-75
FW-1324	19-55	FW-1376	19-75
FW-1325	19-56	FW-1377	19-76
FW-1326	19-56	FW-1378	19-76
FW-1327	19-56	FW-1379	19-77
FW-1328	19-57	FW-1400	19-77
FW-1329	19-57	FW-1401	19-77
FW-1330	19-57	FW-1402	19-78
FW-1331	19-58	FW-1403	19-78
FW-1332	19-58	FW-1424	19-78
FW-1333	19-59	FW-1425	19-79
FW-1334	19-59	FW-1426	19-79
FW-1335	19-59	FW-1427	19-79
FW-1336	19-60	FW-1428	19-80
FW-1337	19-60	FW-1429	19-80
FW-1338	19-61	FW-1430	19-80



FW-1431 19-81  
FW-1432 19-81  
FW-1433 19-81  
FW-1434 19-82  
FW-1435 19-82  
FW-1436 19-82  
FW-1437 19-83  
FW-1438 19-83  
FW-1439 19-83  
FW-1440 19-84  
FW-1441 19-84  
FW-1442 19-84  
FW-1443 19-85  
FW-1444 19-85

## G

gathering information about the problem 1-11

## H

HAM-1001 20-1  
HAM-1002 20-1  
HAM-1004 20-2  
HAM-1005 20-2  
HAMK-1001 21-1  
HAMK-1002 21-1  
HAMK-1003 21-2  
HIL-1101 22-1  
HIL-1102 22-1  
HIL-1103 22-2  
HIL-1104 22-2  
HIL-1105 22-2  
HIL-1106 22-3  
HIL-1107 22-3  
HIL-1108 22-4  
HIL-1201 22-4  
HIL-1202 22-5  
HIL-1203 22-5  
HIL-1204 22-5  
HIL-1205 22-6  
HIL-1206 22-6  
HIL-1301 22-7  
HIL-1302 22-7  
HIL-1303 22-7  
HIL-1304 22-8  
HIL-1305 22-8  
HIL-1306 22-8  
HIL-1307 22-9  
HIL-1308 22-9

HIL-1309 22-9  
HIL-1401 22-10  
HIL-1402 22-10  
HIL-1403 22-10  
HIL-1404 22-11  
HIL-1501 22-11  
HIL-1502 22-11  
HIL-1503 22-12  
HIL-1504 22-12  
HIL-1505 22-13  
HIL-1506 22-13  
HIL-1507 22-13  
HIL-1508 22-14  
HIL-1509 22-14  
HIL-1601 22-15  
HIL-1602 22-15  
HLO-1001 23-1  
HLO-1002 23-1  
HLO-1003 23-2  
HMON-1001 24-1  
HTTP-1001 25-1

## K

KSWD-1003 26-1  
KTRC-1001 27-1  
KTRC-1002 27-1  
KTRC-1003 27-1  
KTRC-1004 27-2

## L

LOG-1000 28-1  
LOG-1001 28-1  
LOG-1002 28-1  
looking up a system message 1-11  
LSDB-1001 29-1  
LSDB-1002 29-1  
LSDB-1003 29-1  
LSDB-1004 29-2

## M

message severity levels 1-2  
MFIC-1001 30-1  
MFIC-1002 30-1  
MFIC-1003 30-2  
MPH-1001 31-1

MPTH-1002 31-1  
MPTH-1003 31-1  
MQ-1004 32-1  
MS-1001 33-1  
MS-1002 33-1  
MS-1003 33-2  
MS-1004 33-2  
MS-1005 33-3  
MS-1006 33-3  
MS-1007 33-4  
MS-1008 33-4  
MS-1021 33-4

## N

NBFS-1001 34-1  
NBFS-1002 34-1  
NBFS-1003 34-2  
NS-1001 35-1  
NS-1002 35-1  
NS-1003 35-2  
NS-1004 35-2

## O

overview of the system messages 1-2

## P

panic dump files 1-5  
PDM-1001 36-1  
PDM-1002 36-1  
PDM-1003 36-1  
PDM-1004 36-2  
PDM-1005 36-2  
PDM-1006 36-2  
PDM-1007 36-3  
PDM-1008 36-3  
PDM-1009 36-3  
PDM-1010 36-4  
PDM-1011 36-4  
PDM-1012 36-4  
PDM-1013 36-5  
PDM-1014 36-5  
PDM-1017 36-5  
PDM-1019 36-6  
PDM-1020 36-6  
PDM-1021 36-6

PDTR-1001 37-1  
PDTR-1002 37-1  
PLAT-1000 38-1  
Port Logs 1-5  
PORT-1003 39-1  
PORT-1004 39-1  
PS-1000 40-1  
PS-1001 40-1  
PS-1002 40-1  
PS-1003 40-2  
PS-1004 40-2  
PS-1005 40-2  
PSWP-1001 41-1  
PSWP-1002 41-1  
PSWP-1003 41-2  
PSWP-1004 41-2

## R

RCS-1001 42-1  
RCS-1002 42-1  
RCS-1003 42-2  
RCS-1004 42-2  
RCS-1005 42-2  
RCS-1006 42-3  
reading a system message 1-8  
responding to a system message 1-11  
RPCD-1001 43-1  
RPCD-1002 43-1  
RPCD-1003 43-1  
RPCD-1004 43-2  
RPCD-1005 43-2  
RPCD-1006 43-2  
RPCD-1007 43-3  
RTWR-1001 44-1  
RTWR-1002 44-1

## S

SCN-1001 45-1  
SEC-1001 46-1  
SEC-1002 46-1  
SEC-1003 46-2  
SEC-1005 46-2  
SEC-1006 46-2  
SEC-1007 46-3  
SEC-1008 46-3  
SEC-1009 46-3  
SEC-1016 46-4  
SEC-1022 46-4

SEC-1024	46-4	SEC-1088	46-22
SEC-1025	46-5	SEC-1089	46-22
SEC-1026	46-5	SEC-1090	46-23
SEC-1028	46-5	SEC-1091	46-23
SEC-1029	46-6	SEC-1092	46-23
SEC-1030	46-6	SEC-1093	46-24
SEC-1031	46-6	SEC-1094	46-24
SEC-1032	46-7	SEC-1095	46-24
SEC-1033	46-7	SEC-1096	46-25
SEC-1034	46-7	SEC-1097	46-25
SEC-1035	46-8	SEC-1098	46-25
SEC-1036	46-8	SEC-1099	46-26
SEC-1037	46-8	SEC-1100	46-26
SEC-1038	46-9	SEC-1101	46-26
SEC-1040	46-9	SEC-1102	46-27
SEC-1041	46-10	SEC-1104	46-27
SEC-1042	46-10	SEC-1105	46-27
SEC-1043	46-10	SEC-1106	46-28
SEC-1044	46-11	SEC-1107	46-28
SEC-1045	46-11	SEC-1108	46-28
SEC-1046	46-11	SEC-1110	46-29
SEC-1049	46-12	SEC-1111	46-29
SEC-1050	46-12	SEC-1112	46-30
SEC-1051	46-12	SEC-1115	46-30
SEC-1052	46-13	SEC-1116	46-30
SEC-1053	46-13	SEC-1117	46-31
SEC-1054	46-13	SEC-1118	46-31
SEC-1055	46-14	SEC-1119	46-31
SEC-1056	46-14	SEC-1121	46-32
SEC-1057	46-14	SEC-1122	46-32
SEC-1059	46-15	SEC-1123	46-32
SEC-1062	46-15	SEC-1124	46-33
SEC-1063	46-15	SEC-1126	46-33
SEC-1064	46-16	SEC-1130	46-33
SEC-1065	46-16	SEC-1135	46-34
SEC-1069	46-16	SEC-1136	46-34
SEC-1071	46-17	SEC-1137	46-34
SEC-1072	46-17	SEC-1138	46-35
SEC-1073	46-17	SEC-1139	46-35
SEC-1074	46-18	SEC-1142	46-35
SEC-1075	46-18	SEC-1145	46-36
SEC-1076	46-18	SEC-1146	46-36
SEC-1077	46-19	SEC-1153	46-37
SEC-1078	46-19	SEC-1154	46-37
SEC-1079	46-19	SEC-1155	46-37
SEC-1080	46-20	SEC-1156	46-38
SEC-1081	46-20	SEC-1157	46-38
SEC-1082	46-20	SEC-1158	46-38
SEC-1083	46-21	SEC-1159	46-39
SEC-1084	46-21	SEC-1160	46-39
SEC-1085	46-21	SEC-1163	46-39
SEC-1086	46-22	SEC-1164	46-40

SEC-1165 46-40  
SEC-1166 46-40  
SEC-1167 46-41  
SEC-1168 46-41  
SEC-1170 46-41  
SEC-1171 46-42  
SEC-1172 46-42  
SEC-1173 46-42  
SEC-1174 46-43  
SEC-1175 46-43  
SEC-1176 46-43  
SEC-1180 46-44  
SEC-1181 46-44  
SEC-1182 46-44  
SEC-1183 46-45  
SEC-1184 46-45  
SEC-1185 46-45  
SEC-1186 46-46  
SEC-1187 46-46  
SEC-1188 46-46  
SEC-1189 46-47  
SEC-1190 46-47  
SEC-1191 46-47  
SEC-1192 46-48  
SEC-1193 46-48  
SEC-1194 46-48  
SEC-1195 46-49  
SEC-1196 46-49  
SEC-1197 46-49  
SEC-1198 46-50  
SEC-1199 46-50  
SEC-1200 46-50  
SEC-1201 46-51  
SEC-1202 46-51  
SEC-1250 46-52  
SEC-1251 46-52  
SEC-1253 46-52  
SEC-1300 46-53  
SEC-1301 46-53  
SEC-1302 46-53  
SEC-1303 46-54  
SEC-1304 46-54  
SEC-1305 46-54  
SEC-1306 46-55  
SEC-1307 46-55  
SEC-1308 46-55  
SEC-3001 46-56  
SEC-3002 46-56  
SEC-3003 46-56  
SEC-3004 46-57  
SEC-3005 46-57  
SEC-3006 46-58

SEC-3007 46-58  
SEC-3008 46-58  
SEC-3009 46-59  
SEC-3010 46-59  
SEC-3011 46-59  
SEC-3012 46-60  
SEC-3013 46-60  
SEC-3014 46-60  
SEC-3015 46-61  
SEC-3016 46-61  
SEC-3017 46-61  
security audit logging 1-3  
SNMP-1001 47-1  
SNMP-1002 47-1  
SNMP-1003 47-1  
SNMP-1004 47-2  
SS-1000 48-1  
SS-1001 48-1  
SULB-1001 49-1  
SULB-1002 49-1  
SULB-1003 49-1  
SULB-1005 49-2  
SULB-1006 49-2  
SULB-1007 49-2  
SULB-1008 49-3  
SULB-1009 49-3  
SULB-1010 49-8  
supportSave command 1-6  
SWCH-1001 50-1  
SWCH-1002 50-1  
SWCH-1003 50-2  
SWCH-1004 50-2  
SWCH-1005 50-2  
SYSC-1001 51-1  
SYSC-1002 51-1  
SYSM-1001 52-1, 52-2  
SYSM-1002 52-1  
SYSM-1003 52-1  
system console 1-6  
system logging daemon 1-4  
system message log (RASLog) 1-3  
system module descriptions 1-12

## T

Trace Logs 1-5  
TRCE-1001 53-1  
TRCE-1002 53-1  
TRCE-1003 53-2  
TRCE-1004 53-2  
TRCE-1005 53-2

TRCE-1006 53-3  
TRCE-1007 53-3  
TRCE-1008 53-3  
TRCE-1009 53-4  
TRCE-1010 53-4  
TRCE-1011 53-4  
TRCK-1001 54-1  
TRCK-1002 54-1  
TRCK-1003 54-1  
TRCK-1004 54-2  
TRCK-1005 54-2  
TRCK-1006 54-2  
TS-1001 55-1  
TS-1002 55-1  
TS-1006 55-2

## U

UCST-1003 56-1  
UCST-1007 56-1  
UPTH-1001 57-1  
USWD-1006 58-1

## V

view or configure the system message logs 1-6  
viewing system messages from Advanced Web Tools 1-9  
viewing the system messages with page breaks 1-10

## W

WEBD-1001 59-1  
WEBD-1002 59-1  
WEBD-1003 59-1  
WEBD-1004 59-2  
WEBD-1005 59-2  
WEBD-1006 59-2  
WEBD-1007 59-3

## Z

ZOLB-1001 60-1  
ZONE-1002 61-1  
ZONE-1003 61-1  
ZONE-1004 61-2  
ZONE-1005 61-2  
ZONE-1006 61-3

ZONE-1007 61-3  
ZONE-1008 61-3  
ZONE-1010 61-4  
ZONE-1012 61-4  
ZONE-1013 61-4  
ZONE-1014 61-5  
ZONE-1015 61-5  
ZONE-1017 61-5  
ZONE-1018 61-6  
ZONE-1019 61-6  
ZONE-1022 61-7  
ZONE-1023 61-7  
ZONE-1024 61-7  
ZONE-1026 61-8  
ZONE-1027 61-8  
ZONE-1028 61-8  
ZONE-1029 61-9  
ZONE-1030 61-9