FORUM SYSTEMS SENTRY™ VERSION 8.3 LOGGING GUIDE

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2014 Forum Systems, Inc. – All Rights Reserved.

Forum Systems Sentry™ Version 8.3 Logging Guide, published Octboer, 2014.

D-ASF-SE-01876

Table of Contents

INTRODUCTION TO THE LOGGING GUIDE 1
Audience for the Logging Guide 1
SENTRY INTERNAL LOG TYPES 2
Audit Logs 2
System Logs 2
Access Logs 2
LOGGING SETTINGS 3
Log Configuration Settings Screen Terms 4
MANAGING INTERNAL LOGS 6
Accessing the Sentry Logs 6
Resetting the Sentry System Log 7
Searching and Filtering Logs 7
Internal Logs Screen Terms 7
Set Refresh Time for Logs 8
Archive Logs 9
SYSLOG LOGGING 11
Remote Syslogs Screen Terms 11
PACKET CAPTURES 13
Packet Capture Examples 13
Start and Stop a Packet Capture 13
Download a Packet Capture to the Local File System 14
DATA SOURCES (DATABASE ACCESS) 15
Supported Databases 15
Database Drivers Supported 15
Upgrading Database Drivers 16
Creating a Data Source 17
Data Source Screen Terms 17
ERROR CODES 20
APPENDIX 90
Appendix A - Constraints in Logging Guide 90
Appendix B - Specifications in Logging Guide 90
Appendix C - Database Dictionary for Logging Tables 91
Appendix D - Database Dictionary for Database Tables 94
Index 95

List of Figures

Figure 1: Creating a Data Source 17

INTRODUCTION TO THE LOGGING GUIDE

Audience for the Logging Guide

The *Forum Systems Sentry™ Version 8.3 Logging Guide* is for System Administrators who will:

- Manage log configuration settings.
- Manage Remote Syslog policies.
- Manage Packet Capturing.
- Perform database archiving.
- Review System and audit logs analysis on the product.

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: ********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 8.3 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

SENTRY INTERNAL LOG TYPES

There are three types of logs in Sentry: Audit Logs, System Logs, and Access Logs.

Audit Logs

Audit logs are a comprehensive view of user activities and policy additions, modifications or deletions. Each entry in the Audit logs includes a unique Document ID, Time (date and timestamp of each event), session number, event code number, log level flag and system process message. Most columns of data may be sorted.

System Logs

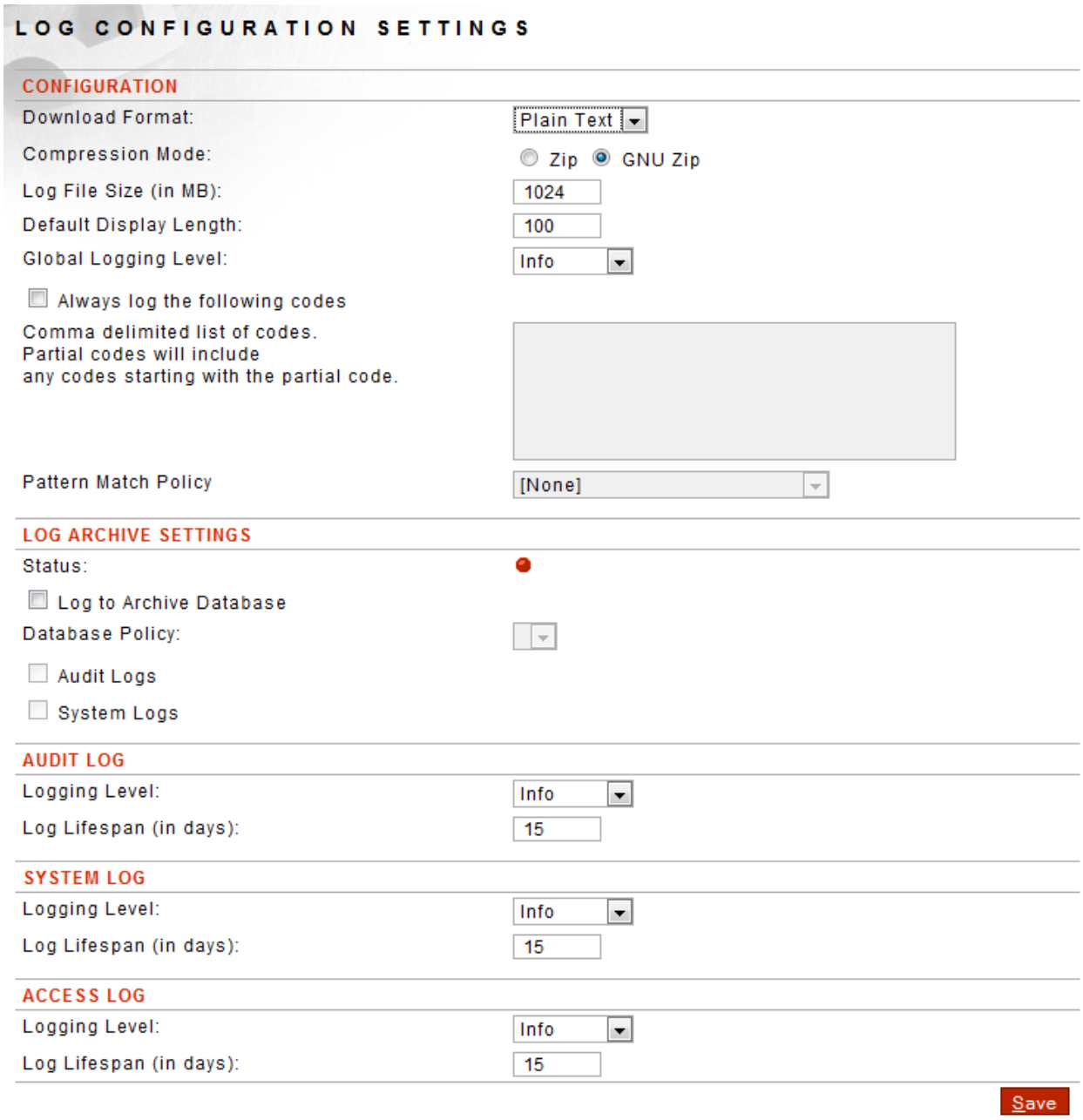
System logs capture the changes that occur in the life of a document as well as changes in movement for a document. As a request is received by the system and the document passes through various processes, tracking messages are written to the System log. Each entry in the System log includes a unique Document ID, Time (date and timestamp of each event), session number, event code number, log level flag and system process message. Most columns of data may be sorted.

Access Logs

Access logs capture a minimal amount of data for each document being processed. The data captured (columns in the log) are the Time (date and timestamp), Session ID, Client IP, TYPE (HTTP Method) HTTP Code, URI, and Length of each document that is processed by the system. They hyperlinked Session ID links to the same Session ID for this document in the System log.

LOGGING SETTINGS

The Settings screen manages individual settings for each category of logs. From the Navigator, select **SETTINGS** and the LOG CONFIGURATION SETTINGS screen appears.



Log Configuration Settings Screen Terms

While working with the Log Configuration Settings screen, please consider the following:

FIELD NAME	DEFINITION
CONFIGURATION	
Download Format	• With XML selected, your downloaded log will be in XML format. • With Plain Text selected, your downloaded log will be in plain text format. • With HTML selected, your downloaded log will be in HTML format. **Note**: The logs are stored in XML format. When downloading as Plain Text or HTML the system transforms the format of the document using an XSLT. Depending on the size of the documents, this transformation may slow down downloading the documents affect runtime traffic.
Compression Mode	• With the Zip radio button selected, all subsequently archived logs will be compressed in zip archives. • With the GNU zip radio button selected; all subsequently archived logs will be compressed in GNU zip archives. GNU zip is the default compression mode on the system.
Log File Size	Maximum size (in MB) for the log file. After the max file size for the log is reached, the system overwrites the content of the log with new messages.
Default Display Length	The number of log messages to display per page. The higher the number the longer it may take to load the page.
Global Logging Level	This setting allows an administrator to use a more permissive log level for syslogs or database logging. For example, to be able to configure the audit logs and system logs to log at Warning Level, but the syslogs log at Debug, this setting must be configured at Debug.
Always log the following codes.	When checked, allows an administrator to log certain messages regardless of the log level configured for the System or Audit log.
Comma delimited list of codes	List of codes to always be logged when the setting “Always log the following codes” is checked. The codes can partial, for example, using 001 will log all messages whose error codes start with 001.
Pattern Match Policy	Existing Pattern Match policies can be selected for use in logging specific messages based on defined pattern match policies (regex) on the system.
LOG ARCHIVE SETTINGS	
Status	The Status column represent the following states: • Green status light = enabled policy. • Yellow status light = a required functional element of this policy is disabled. • Red status light = disabled policy.
Log to Archive Database	When enabled, the Audit and / or System log information can be logged to a database via a Data Source (Data base) policy.
Audit Logs	When checked, the Audit Logs will be logged in the Archive Database if the Log to Archive Database checkbox is also checked.

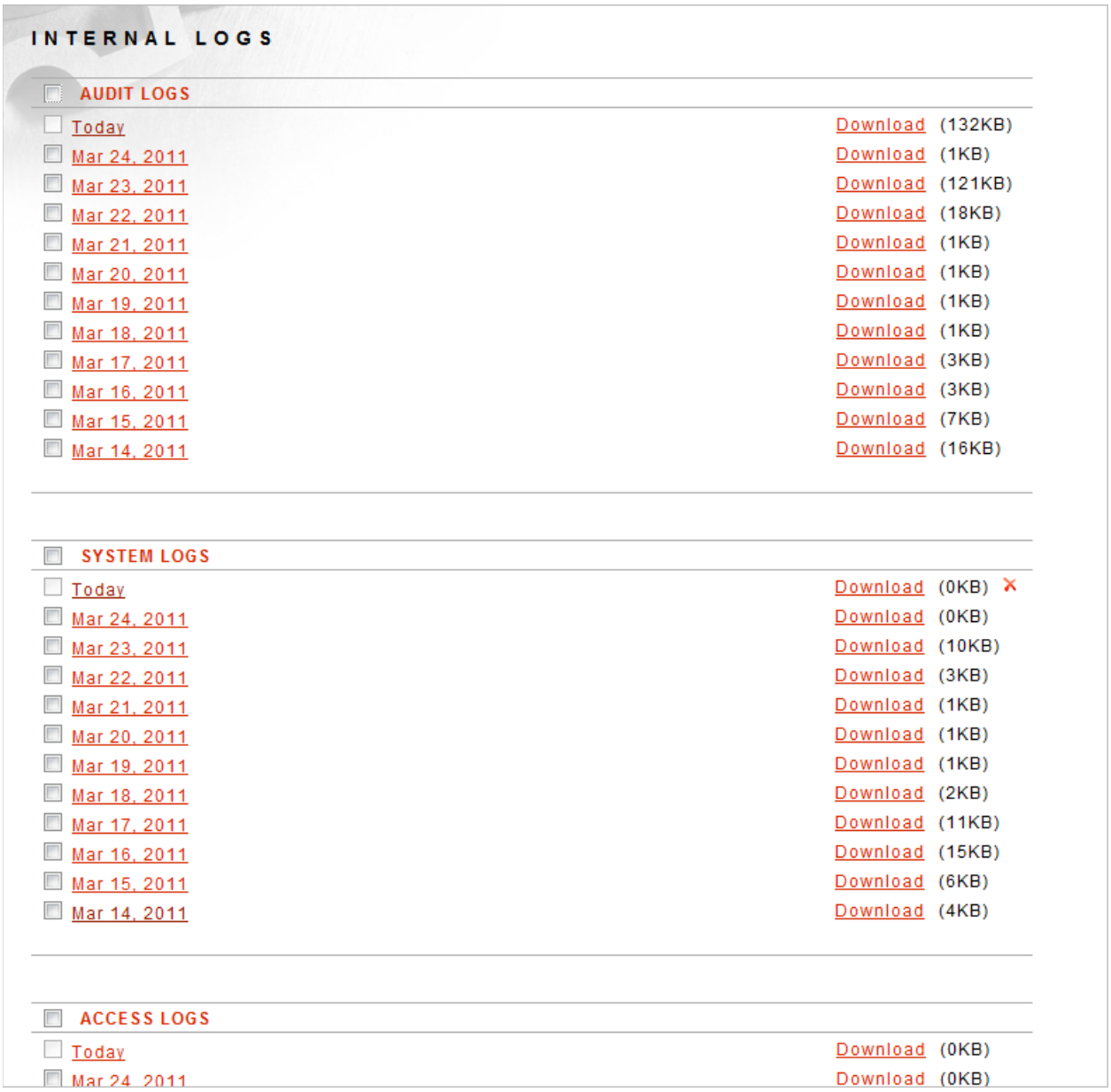
FIELD NAME	DEFINITION
System Logs	When checked, the System Logs will be logged in the Archive Database if the Log to Archive Database checkbox is also checked.
AUDIT LOG	
Logging Level	The Logging Level drop down list includes four categories which represent the level of detail for log messages; these are Error, Warning, Debug and Info log messages. Refer to the Log File Terms for information on log level thresholds.
Log Lifespan (in days)	The log lifespan is an indication of the number of days of logs which are kept resident on the system, after which logs are removed from the system. The default Log Lifespan (in days) is 15. The log lifespan may be configured to hold up to a maximum of 90 days of logs on the system.
SYSTEM LOG	
Logging Level	The Logging Level drop down list includes four categories which represent the level of detail for log messages; these are Error, Warning, Debug and Info log messages. Refer to the Log File Terms for information on log level thresholds.
Log Lifespan (in days)	The log lifespan is an indication of the number of days of logs which are kept resident on the system, after which logs are removed from the system. The default Log Lifespan (in days) is 15.
ACCESS LOG	
Logging Level	The Logging Level drop down list includes four categories which represent the level of detail for log messages; these are Error, Warning, Debug and Info log messages. Refer to the Log File Terms for information on log level thresholds.
Log Lifespan (in days)	The log lifespan is an indication of the number of days of logs which are kept resident on the system, after which logs are removed from the system. The default Log Lifespan (in days) is 15.

MANAGING INTERNAL LOGS

Accessing the Sentry Logs

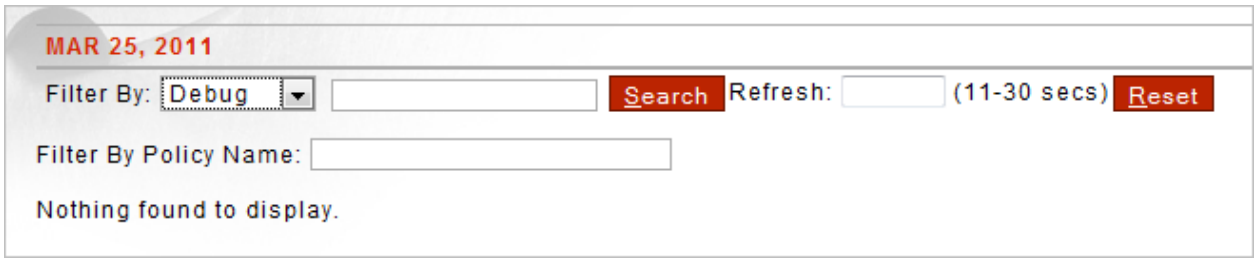
The Sentry logs are available through the WebAdmin on the Diagnostics >> Logging >> Internal Logs screen. The Today log is the current log. All logs can be downloaded or viewed through the WebAdmin interface.

Sentry log can also be viewed through the ForumOS CLI with the Forum Appliances.



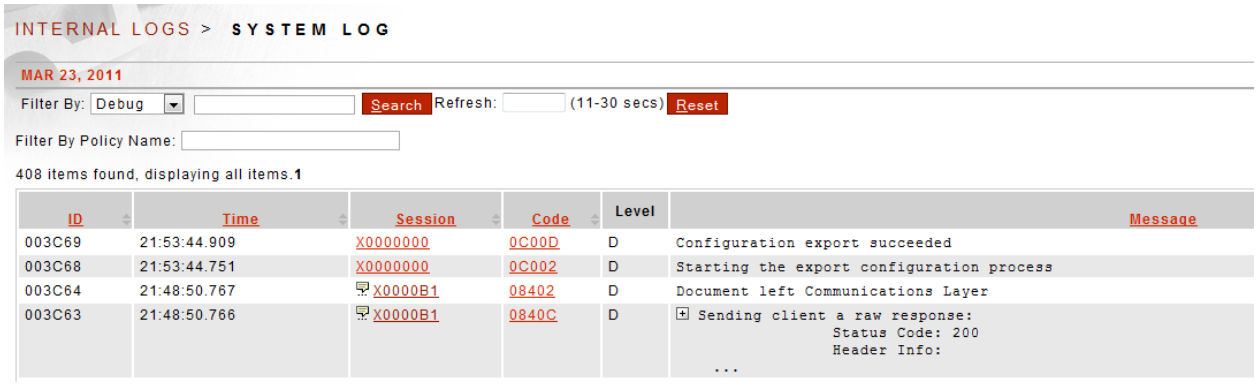
Resetting the Sentry System Log

The current “Today” Sentry System log can be reset from by clicking the X next to the current log or by clicking the Rest button while viewing the log.



Searching and Filtering Logs

Sentry Logs can be filtered by log level and by Policy Name. Clicking a hyperlinked Session ID will display only the logs messages associated to that Session. Clicking a hyperlinked Code will display all occurrences of that Error Code. Logs can also be searched and set to auto refresh.



Internal Logs Screen Terms

The following table includes terms found on the Internal Logs screen and their definitions:

FIELD NAME	DEFINITION
ID	A unique document ID which identifies this logged event.
Time	The hour, minute, second and millisecond that the event was logged in the system, displayed in military time.
Session	The session number includes a prefacing letter that indicates the type of user that triggered the log:

	• A = connected through the WebAdmin UI. • A9999999 = No user is associated with the log message. • S = connected through SSH. • C = connected through a serial port. • X = connected through the system. • X0000000 = No user ID is associated with the transaction.
Code	The event code number associated with a common log event on the system.
Level	The log level flag designates during which state an event was logged. • I = Information identifies a general system activity message that has occurred in system. • E = Error Identifies a severe system error that has occurred in system. • W = Warning identifies system activity that has reached a serious threshold in system • D = Debug identifies a system debugging message (available in log level Debug). Data which designates an Error or Warning state is highlighted with a yellow background and in a red font.
Message	The system process message displays the summary event being logged.

Internal Logs Examples

Examples for Internal Logs include:

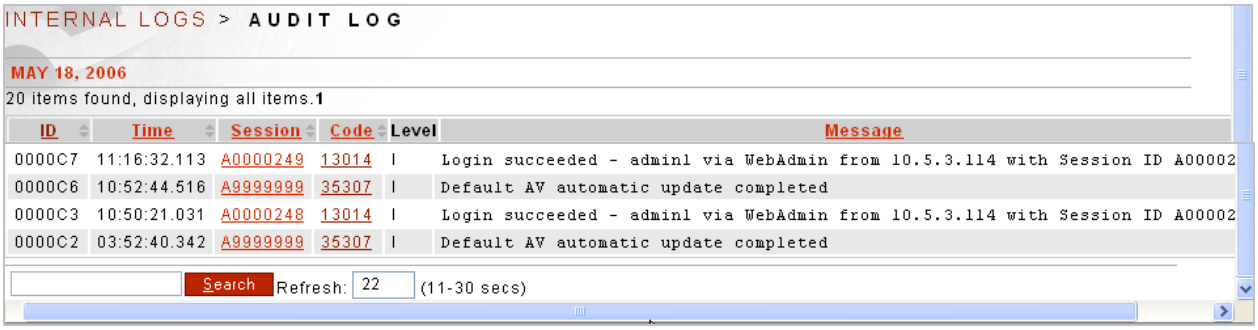
- Set Refresh Time for Logs.
- Archive Logs.

Set Refresh Time for Logs

You may wish to set, or later edit, the refresh time for updating logs visible on the screen.

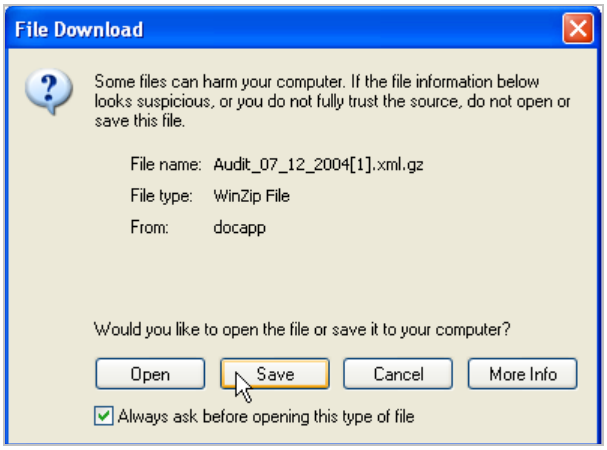
The first time users select a log, there will be no value in the Refresh field. Adding a value to one log will cascade that same value to all other logs. Changing the Refresh value in any log will also cascade the change to all other logs.

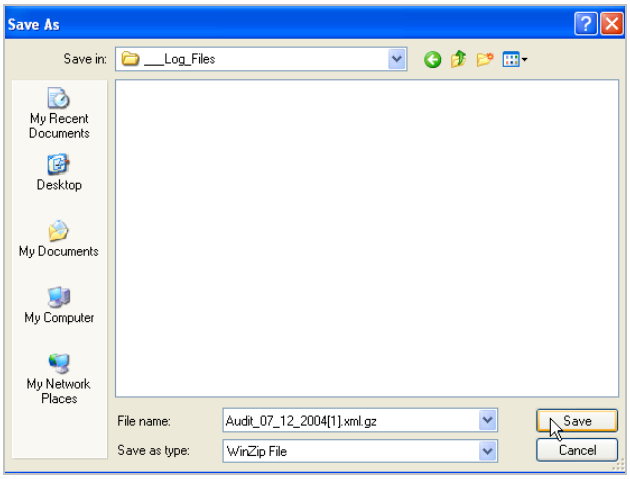
The refresh time may be from 11 to 30 seconds. With a log open, enter or overwrite the current value in the Refresh field with **another value** (22). Click **anywhere** else on the screen to accept the value



Archive Logs

Logs may be archived for off-system storage at any time.

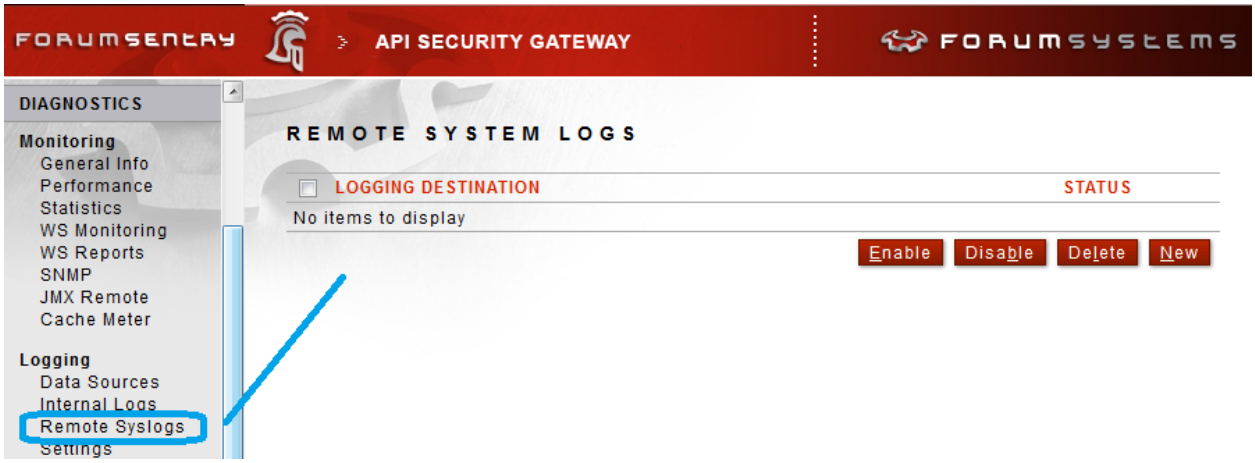




- Navigate to the **Internal Logs** screen.
- On the INTERNAL LOGS screen, click the **Download** link aligned with a log. The File Download screen appears.
- Click **Save**, and the Save As screen appears.
- Navigate your system to a desired directory, and click **Save**. When downloaded, the Download complete screen appears.
- Click **Close**.

SYSLOG LOGGING

The system uses the syslog protocol to send messages in real-time to a remote system capable of handling incoming syslog messages. These policies are configured under the Diagnostics->Logging->Remote Syslogs section



Note that the log levels specified in the Syslog policies do not need to match the log levels set for the Internal Logs. So it is possible to log only Info messages to the Internal Logs while sending Debug level messages to the Syslog server.

Remote Syslogs Screen Terms

While working with the Remote Syslogs screen, please consider the following:

TERM	DEFINITION
LOGGING POLICY	
Policy Name	The identifier for this Syslog policy.
INCLUDED LOGS	
Audit log	When checked, Audit logs are routed to the Syslog destination.
System log	When checked, System logs are routed to the Syslog destination.
Access Log	When checked, Access logs are routed to the Syslog destination.
LOG LEVELS	
Severe	Identifies a severe system error that has occurred in system.
Warning	Identifies system activity that has reached a serious threshold in system.
Info	Identifies a general system activity message that has occurred in system.
Debug	Identifies a system debugging message (available in log level Debug).

FIELD NAME	DEFINITION
REMOTE SYSLOG DAEMON	
Server	Server IP address must be a valid IPv4 address or valid host name. (DNS Servers must be added to the Network screen to resolve host names).
Port	The Syslog Port default is 514, but you may assign another port number.
Facility Code	Facility codes are indicators of a syslog utility or service area within the system that has logged the error. The Facility code refers to the name of the facility that the message is tagged as coming from. The following is a list of each facility codes and its definition: • General User handles messages generated by any system user. • Daemon handles messages as if logged by your system daemon. • Local 0 handles messages the same way your system would handle messages from a local user designated as 0. • Local 1 handles messages the same way your system would handle messages from a local user designated as 1. • Local 2 handles messages the same way your system would handle messages from a local user designated as 2. • Local 3 handles messages the same way your system would handle messages from a local user designated as 3. • Local 4 handles messages the same way your system would handle messages from a local user designated as 4. • Local 5 handles messages the same way your system would handle messages from a local user designated as 5. • Local 6 handles messages the same way your system would handle messages from a local user designated as 6. • Local 7 handles messages the same way your system would handle messages from a local user designated as 7.

PACKET CAPTURES

The PACKET CAPTURES screen provides a method of capturing, downloading and deleting packet captures that include full TCP packets. Users may capture up to 100,000 packets per capture on the Packet Capture screen.

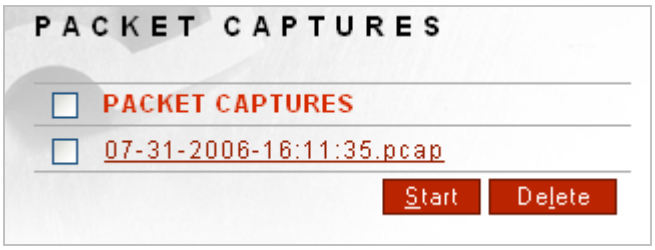
Packet Capture Examples

The examples for Packet Captures include:

- Start and Stop a Packet Capture.
- Download a Packet Capture.
- Delete a Packet Capture.

Start and Stop a Packet Capture

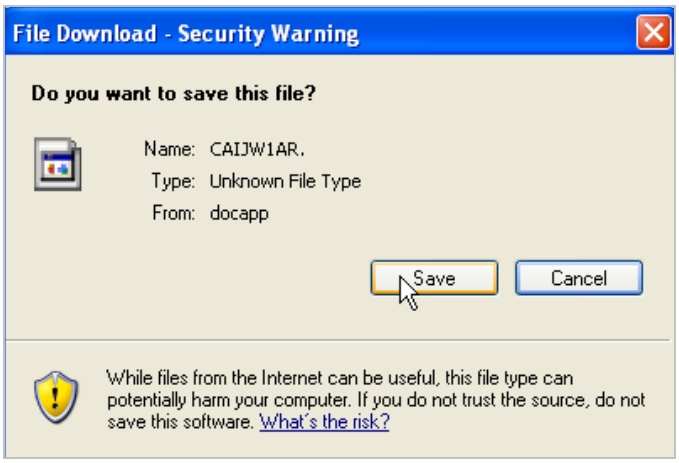
Follow these steps to start and stop capturing packets:

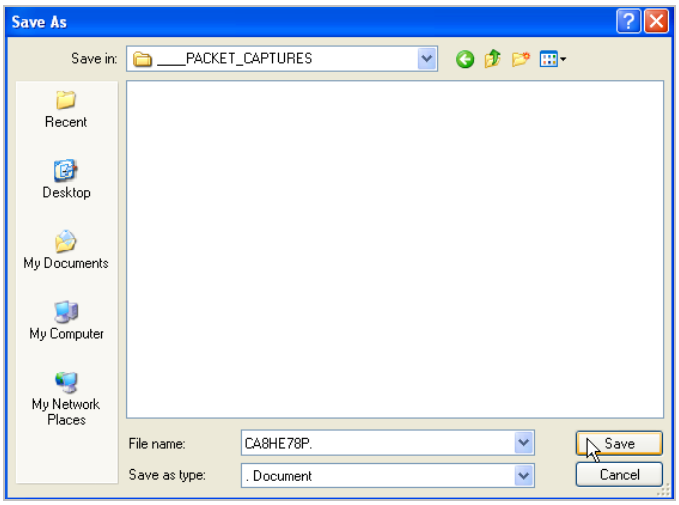


- Navigate to the **Packet Captures** screen.
- Select **Start**.
- On the PACKET CAPTURES screen, select **Stop** to end this packet capturing session.

Download a Packet Capture to the Local File System

Follow these steps to download a packet capture to a local file system:





- Navigate to the **Packet Captures** screen and click on one of the listed **Packet Captures**.
- On the File Download screen, select **Save**.
- On the Save As screen, navigate to a desired location and select **Save**.

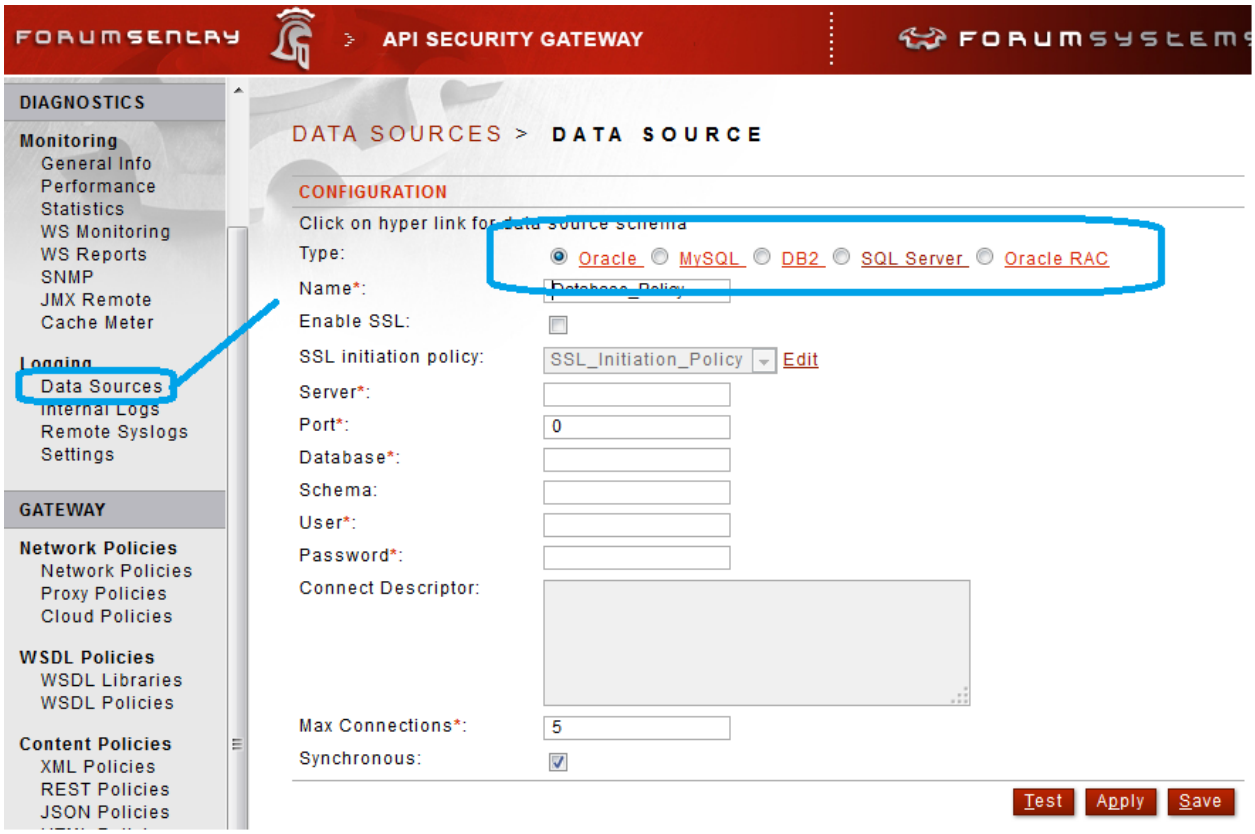
DATA SOURCES (DATABASE ACCESS)

The Data Sources screen allows users to set up JDBC connections (data sources) for accessing databases for architving, session storage, identity provider storage, and many other persistent storage access features of Forum Sentry.

Supported Databases

The system supports Oracle, Oracle Real Application Cluster (RAC), MySQL, DB2, Microsoft SQL Server databases.

Forum Systems provides the database schema SQL scripts to create Oracle, MySQL, DB2 or SQL Server database tables by selecting the hyper-linked database name. These SQL scripts, accessible by selecting the database name link, are intended to be run by a user with enough privileges to create users, tables and sequences.

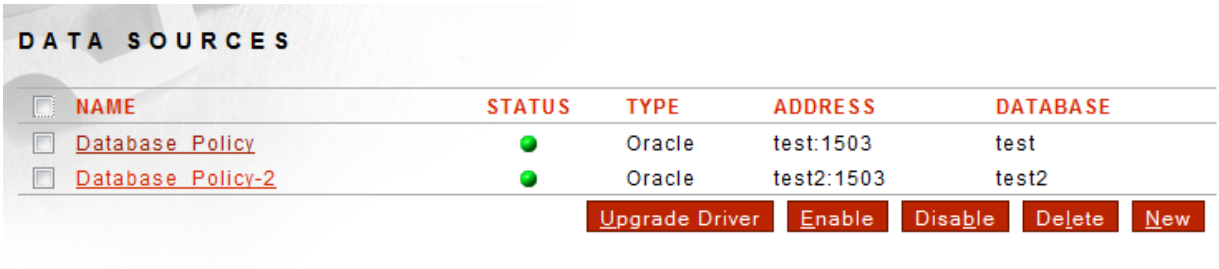


Database Drivers Supported

The following table displays the databases supported on the system, the versions of built-in database drivers supplied, and a listing of which database driver upgrades that required are after a system upgrade.

DATABASE TYPE	DATABASE DRIVER VERSION	DATABASE DRIVER UPGRADE REQUIRED
Oracle/Oracle RAC	9i and higher	Not applicable
MySQL	5.0 and higher	Yes, after system software upgrade.

DB2	7.2 and higher	Yes, after system software upgrade.
SQL Server	2005, 2008	Not applicable



Data Sources Screen

Functionality on the Data Sources screen includes:

- **Upgrade Driver** – Upgrade the JDBC drivers used to connect to the database.
- **Enable** – Enable the Data Source
- **Disable** – Disable the Data Source
- **Delete** – Delete the Data Source
- **New** – Create a new Data Source

Upgrading Database Drivers

Note: Every time the product software is upgraded, the database drivers are lost and the new database drivers installed are whichever drivers are on the upgraded product software.

However, with DB2 databases, the system leaves whatever drivers the system has currently. In other words, it does not overwrite the drivers that are currently in place with the drivers in the upgrade package.

- Navigate to the **Data Sources** screen.
- Select **Upgrade Driver**.
- Under UPGRADE INFORMATION, select the radio button prefacing your **database type**.
- Click **Browse**, and the Choose file screen appears.
- Navigate your local file system and select the **database driver jar** or **zip file.** .
- Click **Open**, and the Choose file closes while the UPGRADE DRIVER screen refreshes. The jar or zip file is now populated in the File field.
- Click **Upgrade**. The DATABASE CONFIGURATION screen refreshes with the “Reboot appliance for the changes to take effect” message visible at the top of the screen.
- Navigate to the **Control** screen. .
- Select **Reboot**. The “Are you sure you want to reboot the server?” message appears.
- Click **OK**, and the CONTROL SETTINGS screen refreshes with “The Server is rebooting” message visible.

Creating a Data Source

Data Sources can be created new and copied.

Once the Data Source is built, the user can Test the Data Source to ensure connectivity.

Forum Systems provides SQL scripts to create Oracle, MySQL, DB2 or SQL Server database tables and users for archiving, available by selecting the linked database name. These SQL scripts, accessible by selecting the database name link, are intended to be run by a user with enough privileges to create users, tables and sequences.

Note: In the sql script for an Oracle database, the database user is FSADMIN and the password is forumsys. Please substitute your own database user name and password in the script on the installation CD-ROM.

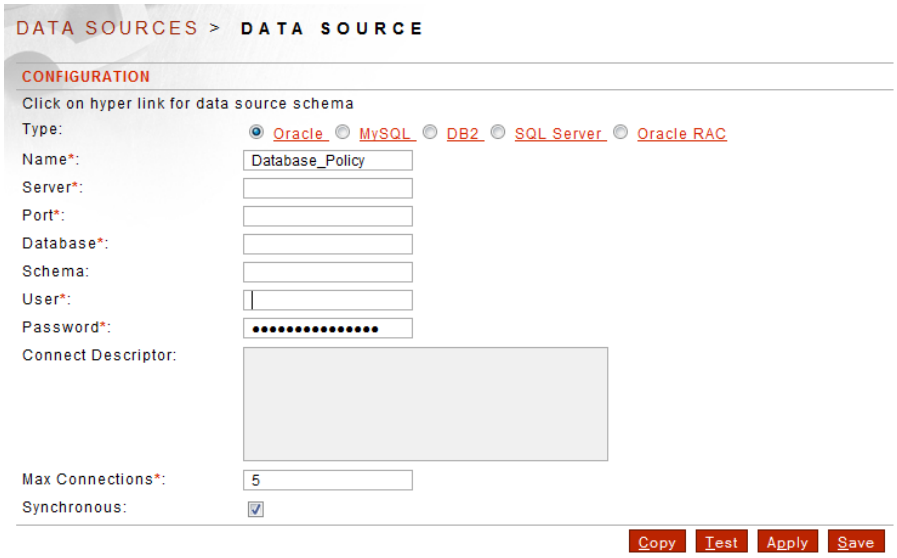


Figure 1: Creating a Data Source

Before creating your Data Source, confirm that you have:

- Database name
- Database port
- Created a database schema (for DB2 and Oracle databases only)
- Database schema name (for DB2 and Oracle databases only)
- Database user name and password

Data Source Screen Terms

When viewing the Archiving screen, consider the following:

TERM	DEFINITION

Type	Select Oracle (for 9i and 10g), MySQL, DB2, SQL Server or Oracle RAC (for Oracle RAC) as the database to configure.
Name	The name of your Data Source
Server	The IP address of your database server.
Port	The port for your database. **Note:** The product requires a DB2 JDBC proxy to facilitate communication with a DB2 server. The IP and Port values entered must correspond to those of your DB2 JDBC proxy. For information on how to set up a DB2 JDBC proxy, please refer to your DB2 documentation.
Database	The name of your database.
Schema	Your DB2 or Oracle database schema name. MySQL and SQL Server databases do not have schema names.
User	Your database user name.
Password	Your database password. Database Passwords must be unique, are case sensitive and may contain any ASCII character.

Connect Descriptor	The Connect Descriptor is a specially formatted string that specifies such details about the Oracle RAC as the service name, host name, port number, and failover configuration, among other parameters. For example, the following string describes the details for connecting to the test-server database on port 1521 with the service name “test.forumsys.com”:
	
	`(DESCRIPTION=`
	`  (ADDRESS=(PROTOCOL=tcp)(HOST=test-server)(PORT=1521)`
	`  (CONNECT_DATA=`
	`  (SERVICE_NAME=test.forumsys.com)))`
	
	The Connect Descriptor text field is enabled only by selecting the Oracle RAC radio button.

Max Connections	Default value is 5.

TERM	DEFINITION
Synchronous	The system supports information that is stored synchronously and asynchronously. • With the Synchronous checkbox checked, when documents are processed through Tasks, information is not transferred until archiving has completed. • With the Synchronous checkbox unchecked, when documents are processed through Tasks, the data is placed in a queue for later archiving. The request will be transferred even if archiving has not completed. The size of the queue depends on system memory and number and size of messages in the queue. Once the queue is filled,

	messages are dropped. The client will not be notified on any errors occurred during archiving

ERROR CODES

The following table displays the Error Codes, Error Messages and Error Descriptions in the system.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
00001	Could not create server directory {0}	The system could not create the indicated directory during initialization.
00002	Reading log level failed - The value {0} pass to -logLevel is not one of the possible values	During initialization the server could not set the log level parameter passed in from the command line.
00003	Initialization failed - {0} could not be loaded	During initialization the server could not load the indicated system component.
00004	Error shutting down {0}	During shutdown the server could not stop the indicated system component.
00005	Starting server failed - Unknown error starting server	During initialization the server encountered an unknown error.
00006	Error stopping XmlServer	During shutdown the server encountered an unknown error.
00016	Shutdown failed - No server found to be running	Shutdown failed because the server was never properly initialized and thus wasn't found to be running at all.
00100	Could not retrieve SSL termination policy {0}	The server was unable to retrieve neither the user specified SSL termination policy nor the System default SSL termination policy.
00102	Could not retrieve factory default SSL termination policy	The server was unable to retrieve the factory SSL Termination policy.
00103	Unknown host while starting AdminServer	Server initialization failed because the hostname used to configure the Web administration server could not be recognized.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
00104	Could not start AdminServer	Server initialization failed because an SSL error occurred while configuring the Web admin server.
0010A	Failed to rebind listener	Failure while rebinding the interfaces after a network change.
00203	Web admin listener bind to {0}:{1} - failed	Failure during system initialization while binding Web Admin Server to the specified address and port.
00204	Servlet create failed for web admin server	Failure during system initializing the web admin server.
00503	GDM listener bind to {0}:{1} - failed	Failure during system initialization while binding GDM Server to specified address and port.
00504	Servlet create failed for GDM server	Failure during initialization when configuring the GDM server.
00601	Listener rebind failed	Unable to reset (to the current settings) one of the system's administration servers (WebAdmin, GDM) after the administration server was bounced.
00602	Error setting {0} port - {1}	Either a port conflict or an invalid port value was detected while setting the port for one of the system's administration servers (Web, GDM, etc). This is a generic port validation error when any one of the management port conflicts with another. A conflicting listener type will be inserted into the error message to provide more detail.
00605	Error setting SMTP address - SMTP server {0} is not a valid host name or IP address	Invalid host name or IP address used when setting SMTP address.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0060B	System policy load failed	An attempt to access the System Policy failed owing to an error when accessing the system store.
0060C	Port set failed	The specified port could not be set for one of the administration servers (such as the WebAdmin server, GDM, ISA, Generic API).
0060F	Failed to get system policies	The system failed to retrieve the system policy from storage.
None	Error Synchronizing with NTP Server	NTP server sync failed. An NTP server is synchronized when the NTP server IP has been set or changed.
00700	Loading policies failed - Managers policies could not be retrieved from the repository	Some system policies could not be loaded by the server from the system store (aka Preferences).
00702	Update failed - Object is null	A change to one of the policy objects could not be saved because the new placeholder object was not initialized properly.
00703	Update failed - {0} does not exist	A change to one of the policy objects could not be saved because the old object does not exist.
00705	Object is null	The name of the policy object to be removed is empty.
00706	Name conflict. Name already in use by system '{0}	The server was performing policy name checks and found a naming conflict.
00708	Loading objects failed - Objects policies could not be retrieved from the repository	Policy objects could not be loaded from the repository.
00709	Loading object failed - Could not retrieve {0} from the repository	The indicated policy object could not be loaded from

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		the repository.
0070B	Update failed - User {0} does not have permissions to modify {1}	The user attempted to modify a policy without having the proper permissions to do so.
0070C	Remove failed - User {0} does not have permissions to remove {1}	The user attempted to remove a policy without having the proper permissions to do so.
0070D	Add failed - User {0} does not have permissions to add {1}	The user attempted to add a policy without having the proper permissions to do so.
00711	Reload failed - {0}	The configuration data failed to reload while it was being imported either through the import/export process or through a GDM transaction.
00716	Directory has not been loaded: {0}	Could not load the indicated preferences directory when loading policy objects.
00717	Users can not add system default objects	Somehow an attempt was made to add a default policy to the preference. Only the system can add default policies (during initialization).
00718	Users can not unset system default status	A user cannot change the system default status of a policy. Only the system is allowed to do so.
00719	Users can not set system default status	A user cannot change the system default status of a policy. Only the system is allowed to do so.
0071D	Manager "{0}" accessed prematurely	When retrieving policy objects from the preferences the system was found in an illegal state.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0071E	Users can not change admin domain	The admin domain cannot be changed by users.
0200F	Exception during archiving	This is a generic error message thrown by the database API. It will help to turn on logging level to debug for further information.
02018	Unknown database requested	An invalid database product code was encountered by the database API. See Archiving help documentation for a list of supported database products.
03008	Failed to set logging configuration	There was an error while setting log configuration parameter (such as log level or lifespan).
0300B	LAN interface only available in two port mode	Error reported by the CLI command for configuring network management interface (which allows users to choose the interface where the management listeners are going to bind to). The error occurs when users attempt to configure the LAN interface while the network topology mode is not set to two-port.
03010	Invalid parameter was entered	The user entered an invalid parameter for a CLI command.
03108	Illegal value entered for the number of admin cards to create	When creating admin HSM cards the value entered for the number of cards to create is illegal.
03109	Invalid card number entry: {0}	The value entered for the number of HSM cards to create is invalid: it's either less than zero or greater than the allowed maximum value.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0310C	Slot is null	Card reader slot could not be detected. Check card reader connection.
0310D	Card reader device not found	Card reader slot could not be detected. Check card reader connection.
0310E	Card not found	Card could not be detected in the slot. Try reinserting.
03110	There was an error detecting the state of the card slot	Could not communicate with card reader. Check connection.
03114	There was an error while initializing the PKI repository	Could not initialize PKI Manager. Reboot appliance.
03115	Incorrect password	User entered an incorrect password.
03116	Could not erase card	Error while attempting to erase smart card.
04003	Failover transition failed - Unable to transition into {0} mode	The failover mechanism encountered an error when transitioning into a new mode ({0} indicates the new mode).
04004	Failover failed	An error occurred during the failover process causing the failover to fail.
04007	Failover scheduling failed - Cannot schedule a synchronization while a transition is in place	An error occurred while attempting to schedule a synchronization of the slave appliance with the master appliance because a transition between failover modes was taking place. Synchronization cannot take place during transition between failover modes.
04008	Failover failed - Could not transition to Master	An error occurred when sending failover command to the master appliance.
04009	Set failed - Could not set PPP configuration	PPP protocol configuration could not be saved for failover mechanism.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0400A	Failover synchronization failed - Server needs to be running in Master mode	The failover mechanism encountered an error when synchronizing the slave appliance with the master appliance. The error occurred because the current appliance was not running in master mode.
0400D	Unexpected exception happened	An unexpected error was thrown by the failover mechanism.
0400F	Socket creation failed - Could not create or open a connection	The failover mechanism could not create the server socket used to listen for connections.
04013	Reading socket failed - Socket timeout waiting for data	Socket timeout occurred when trying to setup connection to the master appliance.
04014	Reading socket failed	The failover mechanism encountered an error while reading data frames from the socket.
04015	Initiating handshake failed	The failover mechanism encountered a protocol handshake error when connecting to the master appliance.
04016	Thread interrupted	The failover mechanism encountered a threading error when connecting to the master appliance.
04017	Closing socket failed - Could not client close socket	The failover mechanism encountered an error when attempting to close the socket connection to the master appliance.
0401A	Failover synchronization failed - Could not import configuration	Failover mechanism encountered an error on the local appliance when importing configuration from the master appliance.
04020	Illegal mode: {0}	The failover policy was

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		initialized with an invalid failover mode.
04023	Connection failed - Unable to connect to server running in Master mode	Failover client (slave) could not establish a connection with the master appliance.
04026	Exporting configuration failed	Failover mechanism encountered an error when exporting the system configuration from the current appliance.
0402C	Failover failed - {0} is an invalid state to failover	The failover mechanism encountered an invalid state when it was expecting either the master or the standby state.
0402F	Failover input processing failed - The client closed the connection	Failover mechanism encountered an error when reading data over the network.
04030	Save failed - Cannot save configuration while a failover transition is in progress	An attempt was made to save the Failover policy to the system store (aka Preferences) while a failover transition was in progress.
05001	Export failed	Error occurred while exporting the local configuration and sending it to the target machine.
05004	GDM transaction to agent {0} at {1} failed	GDM transaction failed owing to an I/O error.
05006	Field override failed	GDM transaction failed to set an override value.
05007	Connection failed	GDM transaction could not create an HTTPS connection.
05014	Insufficient resources to perform export	The system does not have enough memory to perform a GDM export. This can be caused if the system is under load or if the configuration is extremely large.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
05026	Remote import to "{0}" at "{1}" failed - {2}	GDM transaction failed owing to a failure on the remote end. Possibly the remote side could not import the transferred configuration.
05061	GDM transaction to agent {0} at {1} failed	GDM transaction transfer to remote agent failed because of an SSL error.
0510A	Failed to handle dependency for {0}	While packaging the system configuration in preparation for a GDM partial transfer, the system was unable to handle dependencies for the indicated policy object.
06015	Database product is unknown	System could not recognize the database product. This is probably because of a programming error.
06018	Failed to start monitoring: '{0}'	The system failed to start collecting statistics for an operation or virtual directory.
06019	Failed to stop monitoring: '{0}'	The system failed to stop collecting statistics for an operation or virtual directory.
0601A	Failed to save sensor information	The system failed to store to disk IDP statistics for rate based IDP rules.
0601B	Failed to load sensor information	The system failed to load from disk IDP statistics for rate based IDP rules.
06231	Listener Policy is required when in Agent mode	The user tried to configure IDP Config in Policy Server Mode without a Listener Policy.
06232	Remote Policy is required when in Policy Server mode	The user tried to configure IDP Config in Agent Mode without a Remote Policy
06233	The virtual directory '{0} already exists	The virtual directory used in Policy Server Mode to listen for connections, /idp, is in used by the system on the same IP and port.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
06234	Failed to start IDP listener	The system failed to start the listener used in Policy Server Mode to listener for connections.
06235	Failed to contact IDP Policy Server continue processing	The system running in Agent Mode failed to contact the Policy Server, but it is configured to continue processing in this failure scenario.
06300	Failed to parse incoming IDP request	The system running in Policy Server Mode failed to parse the incoming XML request from a system running in Agent Mode. Or the system running in Agent Mode failed to parse the response from the system running in Policy Server Mode.
06301	Failed to convert incoming request to XML	The system running in Policy Server Mode failed to obtain the XML request from an Agent. The system running in Agent Mode failed to obtain the XML Response from the Policy Server
06302	Failed reading from the input stream	The system failed reading a request or response from an Agent or Policy Server respectively.
07302	Failed to authenticate user {0} using LDAP policy {1}	The indicated user does not have access to the LDAP server specified by the LDAP policy.
07305	Use of LDAP policy "{0}" disallowed: LDAP policies in FIPS mode must use SSL	While creating the LDAP directory context, the system detected that the indicated LDAP policy is not using SSL. Because the system is configured to use FIPS mode, all LDAP policies must use SSL.
07002	Could not authenticate to the LDAP server	The connection to the LDAP server failed due to an authentication error.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
07004	Could not connect to the LDAP server	The connection to the LDAP server failed due to an unexpected communication error.
07003	Could not find LDAP context	The connection to LDAP was established but we were unable to read the root directory context.
07044	Failed to find user that matches "{0}" equals "{1}". LDAP policy "{1}" is disabled.	Failed to find the LDAP user that matches the given criteria because the LDAP Policy is disabled.
07045	Found user "{0}" with DN "{1}" in cache for LDAP policy "{2}".	Found the indicated LDAP user using the cached DN for the particular LDAP Policy.
07047	Failed to find user that matches "{0}" equals "{1}" using LDAP policy "{2}"	Failed to find the LDAP user that matches the given criteria.
None	Policy not found: {0}	The indicated Network policy could not be retrieved, probably because the user has no access to that policy.
None	Policy cannot be used in this context: {0}	This is a runtime check and error for the case where the wrong type of network policy is associated with a particular listener. For example, when retrieving the indicated policy the system was expecting an HTTP type policy, but instead found a non-HTTP type policy.
None	Policy not found because no policy was specified	The system could not retrieve a policy because the policy name was empty.
None	Could not store policy: {0}	The indicated policy could not be store to the system repository. The cause of the error should be indicated in the log message.
None	Key {0} reused in Process State	This is an internal server

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		error. It indicates a programming error.
08200	SSL listeners are not a licensed feature	While creating an SSL listener, the system detected that it is not licensed to create SSL listeners.
08201	Got null policy	The SSL listener could not be created because no SSL termination policy was provided to be used by the listener.
08501	Remote Server for policy {0} not responding	One of the remote servers in the Group Remote Policy is not responding.
08502	Remote server for policy {0} responded initially then died	One of the remote servers in the Group Remote Policy was working and suddenly stop responding.
08503	None of the configured remote servers could be reached	The system was unable to choose a remote policy to handle an incoming request.
08505	Group remote policy "{0}" chose remote policy "{1}", but it has been deleted.	The Remote Policy chosen by the Group Remote Policy has been deleted from the system.
08506	Remote server for policy "{0}" returned status code 503 (Service Unavailable)	One of the Remote servers in the Group Remote Policy is unavailable
08507	Remote server for policy "{0}" returned status code 503 (Service Unavailable) and will be unavailable for the next {1} seconds.	One of the remote servers in the Group Remote Policy is unavailable and will be disabled for the specified amount of time.
08508	Remote server for policy "{0}" returned status code 503 (Service Unavailable) and will be unavailable until {1}.	One of the remote server in the Group Remote Policy is unavailable and will be disabled until the specified time.
08509	Remote server for policy "{0}" returned status code 503 (Service Unavailable) and reports that it will be unavailable until {1}, but THIS TIME HAS ALREADY PASSED. Using retry delay value of {2} seconds configured in Group Remote Policy "{3}".	One of the remote servers in the Group Remote Policy exceeded the amount of time it indicated it was going to be unavailable for. The system will retry ever nn seconds to re-establish contact with the server.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0850A	Remote server for policy "{0}" returned status code 503 (Service Unavailable) with a malformed Retry-After header "{1}". Using retry delay value of {2} seconds configured in Group Remote Policy "{3}".	One of the remote servers in the Group Remote Policy returned an invalid HTTP header in relation with the 503 error. The system will retry to establish connectivity every nn seconds.
0850B	Remote server for policy "{0}" returned status code 503 (Service Unavailable) with no Retry-After header. Using retry delay value of {1} seconds configured in Group Remote Policy "{2}".	One of the remoter servers in the Group Remote Policy is unavailable but failed to indicate when to retry it. The system will retry to establish connectivity every nn seconds.
0850E	The remote policy "{0}" selected for client "{1}" using server affinity has been disabled. A new remote policy will be chosen for this client.	The system selected a remote policy for the client using server affinity. However the selected remote policy has been disabled, the system will use a different remote policy.
0850F	The remote policy "{0}" selected for client "{1}" using server affinity has become unavailable. A new remote policy will be chosen for this client.	The system selected a remote policy for the client using server affinity. However the selected remote policy is not available. The system will use a different remote policy for the client.
08510	The remote policy "{0}" selected for client "{1}" using server affinity has been deleted. A new remote policy will be chosen for this client.	The system selected a remote policy for the client using server affinity. However the selected remote policy has been deleted from the system. The system will use a different policy for the client.
09002	Presenting certificates to remote server failed - No certificates found for SSL Initiation policy "{0}"	The system failed to present the SSL certificates to the remote server because the SSL Initiation policy did not contain any certificates.
09006	Failed to get authentication credentials for user "{0}"	The system failed to find authentication credentials for the specified user. The credentials are required for basic or digest authentication to the remote server.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
09007	Static auth credentials: user "{0}" does not exist	The authentication credential for the local user selected to authenticate to the remote server re missing.
0900B	Dynamic credentials not found for remote authentication	The client sending the request failed to present authentication credentials to the system to use for the remote server.
0900C	Not using remote authentication because the remote server does not require it	The system is not going to authenticate to the remote server because it is not required.
None	Runtime proxy not found for remote policy "{0}"	The system failed to locate the proxy required for sending traffic to the remote server.
09157	Client with IP address "{0}" was denied by IP ACL Policy "{1}"	The system denied the request because the IP address from the client is blocked by the specified IP ACL Policy.
09196	Connection rejected: Maximum number of licensed connections reached	The system rejected the connection because the maximum amount of connections allowed by the license has been exceeded.
None	The listener must be using HTTPS in FIPS mode	This is a runtime protection to ensure that only TLSv1 is used for communication.
None	Cannot start listener because no network interface policy was found	This is a runtime protection to ensure that the appliance has a network interface policy definition before listeners can be started. Any configured appliance should have a NIP defined before any listeners can be defined, so this would be an unexpected condition.
09300	Starting listener failed - Unknown host while starting listener	The listener could not be bound to the host name in the network interface

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		policy.
None	Error template {0} does not exist	This is runtime protection for the case when an error is generated and the error formatting template associated with the HTTPS listener policy does not reference a known error template.
09210	0< MinThreads <= MaxThreads	This is runtime protection for the corner case where the minimum threads for the listener thread pool could somehow be set below zero or more than the max thread setting.
None	Remote server must be using HTTPS in FIPS mode	This is runtime protection to ensure that an outbound connection cannot be made without using FIPS restricted HTTPS when in FIPS mode.
09515	No parameter names match "{0}"	The system failed to find a parameter in the request that matches the configured parameter in the REST request filter.
09630	Invalid remote path "{0}"	The path presented by the remoter server in the digest challenge is invalid.
09631	Server challenge domains "{0}" do not include request URL "{1}"	The digest challenge by the remote server does not include the request URL.
09702	Presenting certificates to remote server failed - No certificates found for SSL initiation policy {0}	The trusted certificates from the SSL policy could not be retrieved and presented to the backend server.
None	SSL certificate did not match host name	SSL host name verification failed.
None	SSL Policy not found	An SSL policy that the remote communication policy depends on could not be retrieved from the repository.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
09701	HTTP Proxy init failed - server policy {0} does not exist	The HTTP policy that the listener is associated with / depends on, no longer exists.
None	Remote connection restricted to the TLS protocol	This is a runtime check to ensure that when in FIPS mode the remote server must always use TLSv1 to connect.
None	Wrong type of SSL policy	This would be displayed at runtime if a breakdown of integrity happened such that an SSL initiation policy was associated with a listener policy or an SSL Termination policy with a remote communication policy. The combinations are incompatible.
	The requested resource is not available	The remote policy is disabled.
0A137	Session for FTP user timed out	The system timed out the FTP user because the configured idle timeout has been exceeded.
None	The remote policy ""{0}"" cannot be used because it is disabled	The remote policy is disabled.
0B002	Compression failed - Could not compress {0} historic log {1}	The system could not compressed the specified audit or system log.
0B018	Failed to create log file handler	The system failed to create a handler to log audit or system events.
0B019	Invalid error code(s). Code must be a hex value from 0 to FFFFF. {0}	The specified error code for the message does not adhere to the standards.
0C001	Export preprocessing failed - {0}	This occurs if the GDM module is calling the export process and it is unable to overwrite configuration items such as IP addresses from the Managed machine settings.
0C011	Error notifying listener	When an import event happens, all of the managers in the appliance

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		need to be notified of the event so they can reload their state from the repository. In this case, the notification event failed.
0C02B	Export failed user {0} does not have permissions	The authenticated user does not have authorization to perform an export operation.
0C01A	Importing the keystore failed	One component of the import process is importing a Java KeyStore. The Java key store is not used on a FIA_Gateway appliance, but if the empty JKS file is not imported properly this message would be thrown.
0C01B	Importing the namespace failed	One component of the import process is importing the repository component called the namespace. If it cannot be imported, this message is thrown.
0C01C	Importing the OpenPGP keys failed	Although the FIA Gateway does not make any use of OpenPGP, the import file contains an OpenPGP keyring and if it can be read in the import it throws this message.
0C019	Import the repository failed	This is the primary component of the import and if it fails this message will be thrown.
0C02C	Import failed	This is the general error message header that will be appended with detail from 0C01A, 0C01B, 0C01C or OC019.
0C02A	Import failed user {0} does not have permissions	This gets generated when a user does not have sufficient privileges to run an import.
0C022	The security world key could not be found in the import	This happens if the encrypted security world

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		key cannot be found in the import file.
0C00E	Keystore is null	Even though the FIA Gateway does not make use of the software keystore, it is always expected to be initialized and at a minimum empty. If it is not initialized for some unexpected reason, this message is thrown.
0C00F	Namespace is null	At a minimum the namespace storage in the configuration file is expected to be initialized, if it is not for some unexpected reason this message will be thrown.
0E001	Failed to process task list "{0}" at "{1}" task "{2}"	The system failed to process the task list at the specified task.
0E02E	No Authenticated User	The system failed to find an authenticated user during processing.
0E02F	Transformation is not a licensed feature	The system cannot use XSLT transformations since it is not a licensed feature.
0E030	No matches found for xpath {0} during validate X.509 task.	The system failed to match an xpath during the validate X509 task.
0E031	Task "{0}" is not fully configured	The Validate X509 task is not fully configured, it is missing the Signer Group.
0E033	Unsupported token type: "{0}"	The STS task does not support the specified token type.
0E034	Unsupported request type: "{0}"	The STS task does not support the specified request type.
0E035	Unsupported AppliesTo target: "{0}"	The STS task does not support the specified applies to target.
0E105	Failed to identify incoming document:\n{0}	The system failed to match a document identification task to the incoming document.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0E10B	No TaskListGroup configured, document will not be processed	The system cannot map a Task List Group to the incoming document; therefore it will not process the document.
0E10C	Failed to identify incoming document with a TaskList using TaskListGroup "{0}", document will not be processed	The system failed to identify the incoming document with the specified Task List Group.
13009	Login failed - {0} has invalid credentials to log into enable mode	The authentication credentials for CLI enable mode were invalid.
13006	Login failed - Invalid credentials - {0} via {1,choice,0#CLI/ssh|1#CLI/serial|2#WebAdmin} from {2}	Management authentication failed - the message specifies the management interface (CLI or WebAdmin) and the source IP, if appropriate.
13007	Login failed - No permissions to access this module - {0} via {1,choice,0#CLI/ssh|1#CLI/serial|2#WebAdmin} from {2}	Authenticated user does not have access to the management interface. The error message specifies the interface they are attempting to access and the source IP, if appropriate.
13308	Failed to map cookie to user	The system failed to map the incoming session cookie to a local user.
13600	Failed to store cookie to database.	The system failed to store the session cookie in the database.
13601	Failed to retrieve cookie from database.	The system failed to retrieve the cookie from the database.
13602	Failed to update last seen field.	The system failed to update the last seen column in the database for the session cookie.
13603	Failed to delete cookie	The system failed to delete the row from the database containing the specified cookie.
13604	Failed to remove expired cookies	The system failed to remove the expired cookie from the database.
1402C	Failed to store CRL to database.	The system failed to store the CRL in the database

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
1402F	Failed to retrieve CRL from database.	The system failed to retrieve a cached CRL from the database.
14306	The X509CRLSelector does not contain an X.509 certificate.	The system could not find the X509 Certificate to check its revocation status.
14309	Error during XKMS CertStore processing	The system failed to locate the CRL in one of the configured distribution points in the certificate.
14507	Invalid or unsupported OCSP response type.	The system does not support the response it received from the OCSP server. The response is either invalid or not supported.
14508	The OCSP response contained an unsupported critical extension.	The system does not support an extension in the OCSP response that it is considered critical.
1450B	Unsupported OCSP response version: {0}	The system does not support the version indicated in the OCSP response.
1450D	Missing or incorrect nonce in OCSP response.	The system detected that the OCSP response is missing or have an incorrect nonce.
1451	OCSP returned unknown status.	The system does not understand the statys returned by the OCSP server.
14511	The OCSP response did not contain a response for the specified certificate.	The OCSP server did not respond to the request for the X509 Certificate passed on the request.
14513	The OCSP response signature does not contain a certificate for verification.	The signature of the OCSP response cannot be verified because the X509 Certificate for the verification was not provided.
14514	The OCSP response is not signed by the certificate issuer. Expected "{0}", found "{1}".	The OCSP response was not signed by the issuer; this might be a security problem.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
15411	Could not import Java Key Store entry {0}	The system could not import the specified entry from the Java Key Store(JKS)
15412	Could not import certificate. It already exists under alias {0}	The system found a duplicate certificate during the import.
16100	Task "{0}" is not fully configured	The system cannot process the specified XKMS task because a signer group was not configured for the task.
16101	XKMS "{0}" not supported.	The system does not support the specified XKMS request type.
16103	Namespace "{0}" is incorrect for XKMS 2.0.	The namespace in the XKMS request is incorrect for version 2.0 of XKMS.
16104	The XKMS service "{0}" does not match the request URI "{1}".	The XKMS service request does not match one that has been configured.
16105	Security policy "{0}" not found.	The system cannot locate the configure XML Signature or Verification policy.
16106	XKMS {0} element not found.	The system cannot locate the specified element in the XKMS request.
16107	Unsigned XKMS element {0} found.	The system detected that certain elements of the XKMS request that are meant to be signed were not.
16108	No certificate found in XKMS request.	The system detected that the incoming XKMS request did not contain any certificates.
16109	The certificate does not allow XKMS key usage "{0}".	The X509 Certificate cannot be used for the requested operation, because the certificate's key usage flags prohibits it.
1610A	Invalid XKMS key usage: "{0}".	The requested certificate key usage for the XKMS request is not a valid key usage.
1610B	XKMS TimeInstant not supported.	The system does not support the TimeInstant element.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
1610C	XKMS signature verification is disabled.	The system failed the XKMS required because signature verification is disabled.
1610D	XKMS response limit exceeded.	The system failed the request because the limit set for the response has been exceeded.
1610E	XKMS request failed	The system failed the XKMS request.
1610F	XKMS failed to validate certificate	The system failed to validate the X509 Certificate associated with the XKMS request.
16111	XKMS RespondWith "{0}" is not supported.	The system does not support the RespondWith XKMS element.
16112	Invalid XKMS response "{0}".	The XKMS response is invalid.
16113	The XKMS request id "{0}" in the response does not match the original request id "{1}".	The id in the XKMS response does not match the id from the XKMS request.
16114	XKMS request failed with result "{0}".	The system failed the XKMS request with the specified result.
16115	The XKMS response failed to confirm the request signature.	The request signature value element in the XKMS response does not match the signature value of the XKMS request.
1800F	Failed to parse SNMP statistics	The system failed to parse SNMP statistics.
18010	Failed to parse interfaces statistics	The system failed to parse the statistics for the network interfaces.
18011	Failed to parse route statistics	The system failed to parse the statistics for the routing tables.
18012	Failed to parse ARP statistics	The system failed to parse the statistics for the arp table.
18013	Failed to parse TCP connections.	The system failed to parse the statistics for the TCP connections.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
1A700	Database queue is full, job will not be queued	The system cannot queue another request to be archived, the database queue is at maximum capacity.
1D202	Error loading menu factory	The system failed to load one of the WebAdmin menus.
1E005	Loading default error templates failed	The system failed to load the default error templates.
1E100	The request was invalid or malformed	The WS Trust request made to the system is invalid.
22016	Failed to parse CRL	The system failed to parse the CRLs in the XKMS response.
2404C	Processing error : {0}	While sending a processed message back to the Tibco client to conclude a successful transaction, an error occurred. The body of the message being processed is indicated by parameter {0}.
24045	Restart failed - Unable to restart suspended policy {0}	The system failed to restart the indicated Tibco policy as part of the mechanism to monitor ledger files. The system keeps track of the disk space used by all Tibco ledger files. If the size of the used space exceeds the maximum allowed size, the system suspends the inbound listeners of all proxies with certified outbound transports. Once the ledger size is resized so that it is less than the maximum allowed value, the suspended listeners are restarted.
25036	Failed to queue reporting information	The system failed to store the reporting statistics in the database because the system is low in memory resources.

ERROR CODE	ERROR MESSAGE		ERROR DESCRIPTION
25037	Failed to send reporting information		The system failed to store the reporting statistics in the database because of a failure with the database.
27006	Error creating fingerprint		The system was in the process of generating a digital signature on a file but encountered an error as indicated in the error message.
3006E	OpenPGP Signature failed		There was an error when applying an OpenPGP digital signature to the data. See error message for more details.
300CD	Error occurred while attempting to load	keyring: {0}	The OpenPGP keyrings could not be loaded. See error message for more details.
300DC	Error updating the key last used date.		When performing an OpenPGP operation, the system updates the "date used" property of the OpenPGP key that was used for the OpenPGP operation. An error has occurred while updating this property for the given key.
300DD	Could not load OpenPGP keyrings		After a GDM transaction or a system Import / Export operation, they system attempts to load the new keys (the ones just imported) into memory. This error indicates that the system was unable to load the keys.
3C005	Error closing connection in pool {0}		For resource management and performance purposes, the system maintains one or more collections of database connections called 'connection pools'. When a connection to a database is needed, the system looks up the appropriate pool for any available connections that it can reuse. After reuse, the system releases the connections back to the

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		pool. In this case, the system attempted to close a connection in the pool (whose name is indicated by the parameter index {0}) but was unable to close it owing to an error condition, which is indicated in the accompanying message.
3D305	Client with IP address "{0}" was denied by IP ACL Policy "{1}"	The system denied the incoming client request because the IP ACL policy was configured to deny clients from the particular IP address.
3D501	Cannot open connection from {0} ({1})	The system attempted to open an SMTP connection with the remote host (whose hostname is indicated by the parameter index {0} and IP by the {1}) but the attempt failed owing to an error as indicated in the accompanying message.
35324	Virus scan failed. Retrying	The system failed to create a temporary file to virus scan the incoming document.
35325	Failed to create temporary file, could not reserve space.	The system failed to create a temporary file because no more space is available on disk for the file.
0E916	Overloading not supported for operation {0}	An attempt was made to import a WSDL with 2 duplicate operation names - known as operation overloading - which is not supported.
0E928	Failed to get children for node {0}	Unable to retrieve the children in the project hierarchy for the WSDL project from the repository.
0E90E	WSDL HTTP binding is not supported for port {0}	The WSDL HTTP binding is the only supported WSDL binding in this version of the product, and a port in the WSDL file specified another binding type.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0E91F	Invalid HTTP message	The URL of the message did not contain a known operation name.
0E921	Invalid WSDL Message	The inbound message did not map to any message types or operations in the appropriate WSDL project.
0E920	Process Error	This is a high level error message that is thrown when the message is successfully unmarshalled but it cannot be processed.
0E92E	WSDL policy creation failed - duplicate schema elements {0}	When importing the WSDL schema that was referenced in a WSDL import, there were duplicate schema elements declared which is not valid.
0E92B	Failed to load WSDL information	Unable to load the WSDL file due to an unexpected error.
0E912	Invalid SOAP binding, transport style, or style for port {0}	The binding data for the named port are invalid and therefore the WSDL import fails.
0E922	Invalid URL syntax	One of the elements in the WSDL file has an invalid URL syntax.
0E900	Invalid WSDL format	The format of the WSDL file is not valid in the schema check / structural validation check.
0E913	Missing element reference for document style operation {0}	A required element reference for the operation was not found.
0E914	Missing part name or type for RPC-style operation {0}	RPC operations must define a message part or schema type for the inbound and/or outbound messages. This WSDL does not do that properly; therefore, the import failed.
0E901	WSDL policy {0} not found	A WSDL policy that was referenced could not be

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		found in the repository.
0E92A	Failed to remove node {0}	Unable to remove the referenced node from the repository.
0E923	Failed to remove server policy {0}	Unable to remove the referenced server policy from the repository. A server policy is a communication manager policy.
0E917	Unknown WSDL extension {0} is required	This happens if an unknown WSDL file name extension is referenced for the import.
0E929	Failed to save node {0}	Unable to save a newly created project node during the WSDL import operation.
0E924	Failed to save policy {0}	Unable to save the high level WSDL project after the import operation has completed.
0E910	Remote server location modified. Disabling port {0}	This happens if a remote listener policy is modified and a WSDL policy's port depends on it. In this case the port is disabled.
0E915	Style conflicts with binding style for the operation {0}	The style (document or RPC) for the message conflicts with the style declaration of the WSDL port type which is not valid.
0E92D	WSDL {0} not found	This would happen if the WSDL file was not in the location that the appliance was instructed to import it from.
28009	Could not use the exported WSDLs for WSI message validation	The WS-I message analyzer could not read the specified WSDL files.
28005	Exception while getting message	The WS-I message analyzer failed to retrieve the unmarshalled message from the communication

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		layer.
28006	Message WSI validate failed due to an IO exception	The WS-I message analyzer failed because of a problem while reading the WSDL file.
28002	Message failed WSI validation	The message did not meet the criteria necessary to comply with the WS-I recommendations.
28007	More than one found port in WSI message validate source WSDL	The WS-I message analyzer detected a structural violation in the WSDL file.
28008	No port in WSI message validate source WSDL	The WS-I message analyzer detected a structural violation in the WSDL file.
28004	Exception while loading WSDL in WSI message verification {0}	The WS-I message analyzer failed because of a problem reading the WSDL file.
28003	Message WSI validation failed due to WSI exception	This is a top level error message that occurs when the message analyzer throws an exception.
28010	Exception while attempting to load schemas for WSI message verification {0}	There was a problem loading the schemas associated with the WSDL that has been sent to the WS-I message analyzer.
28021	Exception constructing WSDL	There was a problem constructing an object map representation of the WSDL.
28020	Cannot construct a WSDL document from given files	There was a problem constructing an object map representation of the WSDL.
28011	Exception while attempting to load schemas for WSI WSDL verification {0}	There was a problem loading the WSDL schemas

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		associated with the WSDL.
3F000	No login modules configured for {0}	The system was attempting an authentication during login when it was discovered that none of the login modules were configured. The parameter "{0}" indicates the application for which the login modules were being sought. In most cases, the application will be "forum" or "ftp". Examples of login modules include SiteMinder, Tivoli and ClearTrust. Check your license file to see which login modules are available and ensure that the necessary ones are properly configured.
3F002	Authentication failed with {0}	The system was attempting an authentication during login when an unexpected error occurred. The parameter "{0}" indicates the name of the login module that was being used to perform the authentication.
40107	Failed to authorize user {0} using SiteMinder policy {1} from {2} to {3} using {4}	The SiteMinder module tried to determine from the SiteMinder server whether the user was authorized to access a protected resource. In response, the SiteMinder server failed to authorize the user. The parameters in the error messages are defined as follows: {0} indicates the user name of the client; {1} indicates the SiteMinder policy name; {2} indicates the IP address of the client that is being authorized; {3} indicates the name of the protected resource on the SiteMinder server for which the user is being

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		authorized; {4} indicates an HTTP action: GET, POST, PUT.
40108	Failed to get cookie for user {0} using SiteMinder policy {1}	The system failed to obtain a SiteMinder Single Sign On token cookie. Message parameter {0} indicates the user name of the client for which the sign-on was being attempted and {1} indicates the name of the SiteMinder policy.
40109	Failed to logout user {0} using SiteMinder policy {1}	The system failed to logout the user (i.e. invalidate the user's session) from the SiteMinder server. The message parameter {0} indicates the username and {1} indicates the name of the SiteMinder policy.
4000A	Error storing agent configuration files	An I/O error occurred while saving the SiteMinder configuration file SmHost.conf.
40015	Authorization for user {0} failed because {1}	The SiteMinder module tried to determine from the SiteMinder server whether the user was authorized to access a protected resource. The SiteMinder server failed to authorize the user. The parameters in the error messages are defined as follows: {0} indicates the username and {1} indicates the reason for the failure.
40009	Failed to initialize SiteMinder agent for policy {0}	The system attempted to un-initialize the indicated SiteMinder policy but failed to do so. The system usually tries to un-initialize policies during system import / export and shutdown.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
40010	Failed to set DN {0} to user {1}	The system failed to set the DN alias for the user so that DN could later be retrieved to identify the user.
4000C	Failed to authenticate user {0} using SiteMinder policy {1}	The system requested the SiteMinder server to authenticate the user. As part of the authentication process, the system first determines whether the specified SiteMinder resource is a protected resource on the SiteMinder server. Once it's determined that the resource is indeed protected, the system requests the SiteMinder server to authenticate the user. The error message indicates that there was a problem during either the "is protected" test phase or the authentication phase.
41502	Failed to authenticate user using SAML policy {1}	The system failed to authenticate a user via the user's SAML credentials.
41414	Failed to upgrade {0}	The server failed to upgrade the indicated Kerberos policy as part of the system upgrade.
48000	Error during ClearTrust access	The system encountered an error when attempting to authorize a ClearTrust user. This is a generic error message to indicate runtime authorization errors. The cause of the error should be indicated in the log message.
48003	Error during ClearTrust connection initialization	This is a generic error message that represents any one of the several error conditions that can occur during the initialization of

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		the ClearTrust API. The cause of the error should be indicated in the log message.
48017	Initialization of ClearTrust policy "{0}" failed with error: {1}	The system attempted to initialize all ClearTrust policies but failed to initialize the policy indicated by parameter {0}. The reason for the failure is indicated by parameter {1}.
48100	Error during SelectAccess operation: {0}	This is a generic error message that signals errors during SelectAccess initialization as well as during user authorization with the SelectAccess server.
48118	SelectAccess init failed probably due to bad Enforcer Configuration file	The SelectAccess module failed to initialize a connection to the SelectAccess server, probably due to a bad configuration file.
48208	WS-Trust auth for user "{0}" using policy"{1}" failed because the WS-Trust response had no saml assertion	The system failed to authenticate the user using WSTrust because the response is missing the SAML assertion.
48209	WS-Trust auth for user {0} using policy {1} failed because the WS-Trust response had more than one status code	The system failed to establish WS-Trust authentication for the indicated user using the specified remote policy because the response from the server contained more than one status code. The system was expecting only one status code from the server to indicate whether the authentication was successful.
4820A	WS-Trust auth for user "{0}" using policy "{1}" failed because the SAML assertion could not be serialized	The system failed to authenticate the user using WSTrust because the SAML assertion could not be extracted from the response as valid XML.
4820E	Credentials for user "{0}" are not valid	The system failed to match the credentials provided to

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		the credentials stored locally for the user.
26008	Failed to verify the signature in the license file	The system failed to verify the signature on the license file. Please verify the integrity of the license file.
26005	Failed to retrieve system ID	The system ID did not match the ID in the license file.
26016	Failed to back up license	Before the system loads a new license file, it attempts to back up the existing license file, in doing so the system encountered an error.
2600D	Failed to save license to file	The imported license file could not be saved to disk.
26002	Failed to load license	The imported license file could not be loaded into the system. The system will attempt to restore the backup license.
26014	Failed to restore backup license	The imported license file could not be loaded into the system. The system tried to restore the backup license file but failed to do so.
00002	Reading log level failed - The value {0} pass to - logLevel is not one of the possible values	During system startup the value of the logging level specified in the configuration was not one of the possible values. The possible logging level values in descending order are: SEVERE, WARNING, INFO and DEBUG.
00018	License check failed	During system startup, the system performs several checks on the license file. For example, the system checks whether the license file exists at all, whether the signature on the license file is valid, whether the license has expired, and whether

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		the version of the system is correct. When one of the checks fails, the indicated warning message is logged.
00004	Error shutting down {0}	This is a generic message to indicate that during system shutdown the module specified by the parameter {0} could not be stopped.
00005	Starting server failed - Unknown error starting server	This is a generic error message for logging errors that might occur during system startup.
00006	Error stopping XmlServer	This is a generic error message for logging errors that might occur during system shutdown.
00017	Starting server failed	The system has several possible internal states called run levels which dictate the type of operations that can be executed by the system in a given state. During startup, the system switches between these states as necessary and if for some reason it is unable to switch a state, it logs the indicated message as a means to signal a potential problem.
00711	Reload failed - {0}	The system was in the process of importing a configuration (either through the import/export process or the GDM process) when it encountered an error.
0200D	Error - Archiving value is being truncated to 255 characters	The Archiving module enforces a 255 character limit on database writes, fields bigger than this limit are truncated.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0200F	Exception during archiving	This is a generic message to indicate that an error occurred while writing to the database.
50002	Exception during archiving	This is a generic error message for logging database related errors. Error details will be in the message.
04011	Sending heartbeat failed - Could not send heartbeat to the appliance running as Master	The client machine in the failover channel could not send a heartbeat to the master appliance probably owing to an I/O error.
None	Unknown request	The unknown request type was sent across by the one of the failover appliances.
04032	Failed to send update	The appliance could not successfully send a failover frame across to the other failover system owing to an I/O error.
04002	Failover transition failed - Unable to transition out of {0} mode	The failover process transitions between states as it transmits and receives data frames containing the system configuration. The error messages is a generic message to indicate that the failover process failed to transition out of the indicated state.
04006	Failover transition failed - A previous transition is still in progress	The failover process transitions between states as it transmits and receives data frames containing the system configuration. This error indicates the failover process attempted a transition while a previous transition was still in progress.
3A009	No default regular expression pattern policies found	The Regular Expressions module could not locate a default regular expression template file.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
3A00D	Cannot name filter policy {0}	The Regular Expressions module attempted to assign an invalid name to a Regular Expression policy.
3A00A	Mode {0} is not a supported pattern policy mode	The search mode being used to create a Regular Expression policy is invalid.
3A00C	Pattern {0} is not an acceptable Java regular expression	The indicated regular expression pattern being used to create a Regular Expression policy is invalid.
3A00B	Error while loading default pattern policy	The system encountered an error when loading the default pattern matching policies.
3A00E	Cannot perform regex replacement from policy {0} in extremely large XML document	Sentry's regular expression replacement feature currently works for document sizes up to10MB. The error indicates that the document size exceeds this limit.
3A00F	Cannot perform regex matching on a document larger than {0}	Sentry's regular expression matching feature currently works for document sizes up to 2GB. The error indicates that the document size exceeds this limit.
3A010	Cannot perform regex replacement from policy {0} in zip attachment	Sentry's regex replacement feature cannot be used on ZIP attachments.
05008	Import failed	This is a generic error messages to indicate that the GDM process failed to import a system configuration.
05013	Unable to save the last exported date	On concluding a successful GDM transfer, the system attempted to save the last exported data but failed to do so. This error, however, does not hinder the completion of the GDM transaction.
05061	GDM transaction to agent {0} at {1} failed	The GDM transfer failed owing to an SSL error.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
05004	GDM transaction to agent {0} at {1} failed	The GDM transfer failed owing to an I/O error.
05108	GDM import failed: invalid file format or wrong password	Could not decrypt FSG file during partial GDM import most probably because password was incorrect.
05109	GDM import failed	This is a generic message to indicate that the system failed to import an FSG file. Reason will be in the message.
0600D	IDP Rule: {0}, IDP Group {1}, Associated Policy: {2}, Triggered {3} time(s) on {4,choice,0#Request|1#Response|2#Error|3#None},Policy: {5}, Client IP{6}: {7}, User{8}: {9}. {10}	This log message records the number of times an IDP rule was triggered. Among other things, it identifies whether the rule triggered on request, response, error, or otherwise. The messages parameters are defined as follows: {0} = IDP rule name, {1} = IDP group, {2} = Associated Policy, {3} = number of times the rule was triggered, {4} = one of: (Request, Response, Error, None), {5} = WSDL or XML Policy name, {6} = IP restriction, {7} = Client IP, {8} = User restriction, {9} = User, {10} = Error message.
0820C	Failed to handle SSL connection from {0} to {1}	The system failed to establish and SSL connection between the remote server ({0}) and itself ({1}).
08501	Remote policy {0} not responding	Before performing any transformations or encodings on outbound documents, the system tries to verify that the connection to the remote server is valid. In this case, the remote server was found to be unavailable.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
08052	Error stopping listener {0}	The indicated listener policy could not be disabled. The system attempts to disable all listeners when it is shutting down and when it is importing a configuration (via global import or GDM transaction).
08029	Could not enable network policy: {0}	The indicated network policy could not be enabled. The system attempts to enable all listeners during system startup and when importing a configuration (via import / export or GDM transaction).
08027	Policy not found {0}	The system tried to start all listeners but could not find the indicated listener policy.
08035	Save policy {0} failed	The system tried to start all listeners and then tried to save them; the indicated listener policy could not be saved.
08028	Invalid parameter found in: {0}	The system tried at start all listeners but could not start the indicated listener; possibly because it was not properly configured as a result it could not be brought back online. Please review the policy and fix any issues.
08036	Loading policy {0} despite errors	The system was attempting to load the indicated policy after a GDM transfer or a global import and found problems with the policy. The policy, however, was loaded despite the errors. Please review the policy and fix any issues.
0800B	Error while reverting to old version of {0}	When modifying policies, the system tries to ensure that the existing policy will be left unchanged if any errors occur during the update. In this case, the

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		system ran into an error when it tried to revert to an older version of the indicated policy.
08050	Configuration import failed in the communication manager	Failure occurred when the system tried to load all network policies after a GDM transaction or an import process.
08014	ACL check failed - User {0} denied access by ACL {1}	As part of the user authentication process, it was determined that the user does not have access to the requested resource. The ACL associated with the requested resource is disallowing the user from accessing the resource.
08111	Error setting {0} IP address - {1}	An attempt was made to change the IP address of an interface {(0}) to a value that conflicts with the IP address of an existing interface.
08406	Failed to send normal response to client for policy {0}	The system was concluding a successful proxy transaction by sending a processed payload back to the client when it encountered an error.
08403	Processing aborted on policy {0}	A generic message to indicate that processing failed for a request associated with the indicated policy.
08410	Send error to client aborted because the network policy listener has shut down	The network policy listener associated with the client shut down unexpectedly as a result the error message could not be sent to the client.
08404	Error encountered while creating error response	A generic error message to indicate that something went wrong while attempting to send an error response back to the client.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
08411	Send error to client aborted because the network policy listener has shut down	The network policy listener associated with the client shut down unexpectedly as a result the error message could not be sent to the client.
08405	Failed to send error response to client	A generic error message to indicate that something went wrong while attempting to send an error response back to the client.
1E007	Unexpected error while saving error template	The system attempted to save an error template when an unexpected error occurred.
1E003	Cannot find default templates file	The system was unable to locate the file which holds the default templates.
1E004	Bad number: {0}	While load the error templates the system encountered an invalid HTTP error code in one of the templates.
1E011	Upgrade failed - an updated version of System Error Template {0} is available but will not be installed because a User Error Template already exists with that name	When upgrading the error templates to newer ones, the system ran into a name conflict between an existing System Error Template and a User Error Template.
1E010	Upgrade failed - an updated version of System Error Template {0} is available but will not be installed because the template has been modified	When upgrading the error templates to newer ones, the system discovered that the indicated System Error Template has been modified by the user and thus will not be overwritten as part of the upgrade.
1E005	Loading default error templates failed - {0}	This is a generic error message to indicate that one or more System Error Templates failed to load properly.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
1E006	Creating backup default template	This warning message indicates that the system is attempting to create a simple default template in case the system defaults fail to load.
1E000	Error reload failed - {0}	An error occurred when the system tried to reload the templates after importing a configuration either via the GDM process or the global import process.
None	Error issuing {0} command	This is a generic warning message to indicate problems encountered when issuing FTP commands.
None	Error establishing secure server data channel	An error occurred when negotiating a secure connection with the FTP server for the FTP data connection.
None	Error establishing secure client control channel	An error occurred when negotiating a secure connection for the client control connection.
0A11B	Data transfer failed - unexpected exception	This is a generic error message to indicate that the FTP transfer failed.
None	Error establishing secure client data channel	An occurred when negotiating a secure connection for the client data connection.
None	Error establishing secure socket	This is a generic error message to indicate that something went wrong when trying to establish a secure connection with the FTP server.
0A136	Failure recovery WARNING: failed to delete remote file {0}, which may be corrupt	If, when transfer a file to a remote server, an error occurs, the FTP module will delete the file from remote server. This is a generic error message to show that the delete operation failed.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0914B	Servicing request failed - Unexpected error:	This is a generic error message to indicate unexpected error conditions that might occur while servicing requests.
09145	Document processing failed - Unexpected error	This is a generic error message to indicate unexpected error conditions that might occur while processing inbound documents.
0A309	FTP data socket reset failed	A failure occurred when the system tried to close the FTP data connection.
0A309	FTP data server socket reset failed	A failure occurred when the system tried to close the FTP server connection.
0A30B	FTP data server socket setup on {0} failed	A failure occurred when the system tried to open an FTP server connection. {0} represents the local IP address to which the system tried to bind to.
0A30D	Failed to set timeout on FTP data socket	A failure occurred when the system tried to set the timeout value for the FTP data connection.
0A30C	Failed to get FTP data socket	A failure occurred when the system tried to initialize the FTP data connection socket. A socket is an endpoint for communication between two the system and an FTP server.
0A30E	Failed to close server socket for FTP data	The system failed to close the connection with the FTP server.
None	Could not start FTP adapter on {0}:{1}	The system failed to initialize its FTP server on the specified address {0} and port {1}.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0A501	Disable listener failed	The system failed to disable the FTP listener.
0A008	FTP Policy connections out of range - resetting to {0}	The number of FTP connections being set is greater than the maximum allowed.
0A005	Remove FTP User policy failed - {0}	The indicated FTP user policy could not be removed.
0A003	Dependency update failed unexpectedly for FTP Policy {0}	For every policy (FTP, HTTP, etc) the system keeps track of the how many times that policy is being referred to (or used) by other policies. In this case, an unexpected failure occurred when the system tried to update the dependencies for the indicated FTP policy.
0A001	Dependency update failed: FTP Policy {0} references OpenPGP Policy {1}, which does not exist	For every policy (FTP, HTTP, etc) the system keeps track of the how many times that policy is being referred to (or used) by other policies. In this case, a failure occurred when the system tried to update the dependencies for the indicated FTP policy because a dependent OpenPGP policy {1} could not be found.
09302	Add network policy context failed	Enabling a virtual directory for an XML or WSDL policy failed.
09001	HTTP proxy init failed: network policy {0} does not exist	The system failed to initialize the HTTP proxy because the indicated policy could not be found.
0914E	Decode of basic auth credentials failed	The system failed to decode the HTTP basic authentication credentials.
None	Authentication failed - Credentials for {0} and {1} were presented	System failed to authenticate the user because more than one credentials were presented.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
09146	Unexpected problem with stealth mode - {0}	An unexpected error occurred when the system tried to close an HTTP connection while the system was configured to interact with the client in stealth mode i.e., the client is not supposed to receive any response.
09144	Quarantine document failed	The incoming request was be scheduled for quarantining (i.e. archiving to the database) when an unexpected error occurred.
09120	Regular expression compilation failed: syntax incorrect for expression {0}	The regular expression syntax is invalid.
09602	I/O error while decoding a request or response. I/O error while decoding a request or response. We were expecting {1} more bytes to reach the Content-Length of {2} bytes	The system was decoding the HTTP request or response when the body of the messages was found to contain fewer bytes than specified in the HTTP Content-Length header.
0940B	Upgrade: new version of Request Filter Template "{0}" not loaded because existing Template has been modified	The system was updating Request Filter templates with new defaults when it found the indicated filter template had been modified by the user. As a result, the system did not update it with the new version.
1100A	Loading failed - Could not retrieve	The system failed to read the Request Filters from the system store.
09402	Recovering corrupted request filters	The system was unable to retrieve the request filters from storage. The message indicates that an attempt was made to recover them from storage.
09403	Request filters were null	The system could not find any Request Filters for a virtual directory node.
09130	Setup of statistics counter failed	The system was unable to initialize the HTTP statistics

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		counters.
09204	Unexpected: could not start security handler on {0}	An unexpected error occurred when the system tried to launch an HTTP listener or Administration server (e.g. Admin UI, GDM server, etc): a security handler module for enforcing security constraints could not be started.
09205	Unexpected: could not start HTTP handler {0}	An unexpected error occurred when the system tried to launch an HTTP listener or Administration server (e.g. Admin UI, GDM server, etc): an HTTP handler module for processing HTTP requests could not be started.
09200	Stopping listener failed - Could not stop listener on port {0}	The system could not stop the HTTP listener attached to the indicated port.
09203	Could not start HTTP adapter on {0}	The system could not start an HTTP Administration server (e.g. Admin UI, GDM, etc) on the indicated port.
31000	Error enabling subscription	The system was unable to start the connection to the JMS server.
31001	Error while stopping connections	The system was unable to stop the connection to the JMS server.
0311D	No virtual directory exists for incoming message	The system processes messages based on the configuration of virtual directories. In this case, the incoming message could not be matched to a virtual directory.
32004	Expected JMSXDeliveryCount header was not present	There was an error while processing MQ messages: the JMS module failed to read a property value from the message header.
32000	Error enabling subscription	The MQ module failed to

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		start a listener on which to receive messages.
2401C	Daemon read failed	The Tibco Rendezvous daemon failed to initialize. The daemon is responsible for the delivery and acquisition of messages.
24042	Ledger files have exceeded the max size, all Tibco Policies that use ledgers will stop listening	The system keeps track of the disk space used by all Tibco ledger files. If the size of the used space exceeds the maximum allowed size, the system suspends the inbound listeners of all proxies with certified outbound transports. Once the ledger size is resized so that it is less than the maximum allowed value, the suspended listeners are restarted.
24046	Ledger files still exceed the max size	The system keeps track of the disk space used by all Tibco ledger files. If the size of the used space exceeds the maximum allowed size, the system suspends the inbound listeners of all proxies with certified outbound transports. Once the ledger size is resized so that it is less than the maximum allowed value, the suspended listeners are restarted. In this particular case, the system determined that the size of the ledger files still exceeded the maximum size allowed but no action needed to be taken on the Tibco policies because their respective listeners were already in suspended mode.
2401B	Ledger monitoring thread was stopped	This is an internal error signaling that the system process which monitors the

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		files sizes of the Tibco Rendezvous daemon's ledger files has unexpectedly terminated.
24043	Tibco policy {0} has had its listener suspended, it is still able to send queued messages	The system keeps track of the disk space used by all Tibco ledger files. If the size of the used space exceeds the maximum allowed size, the system suspends the inbound listeners of all proxies with certified outbound transports. Once the ledger size is resized so that it is less than the maximum allowed value, the suspended listeners will be restarted. The indicated Tibco policy was suspended because the combined size of the Tibco ledger files exceeds the maximum allowed.
24044	Restarting suspended Tibco policy {0}	If the size of the used space exceeds the maximum allowed size, the system suspends the inbound listeners of all proxies with certified outbound transports. Once the ledger size is resized so that it is less than the maximum allowed value, the suspended listeners are restarted. The system successfully restarted the indicated Tibco policy which had previously been suspended by an internal mechanism which keeps track of the disk space used by all Tibco ledger files.
2402E	Error enabling subscription	The system failed to initialize the Tibco Rendezvous proxy, which is responsible for receiving Tibco messages.
24000	No virtual directory associated with policy {0}	The indicated Tibco policy was not associated with a virtual directory. As a

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		result, the policy will be unable to receive messages.
24002	Tibco listener interrupted	This is an internal error signaling that the Tibco default queue, which handles incoming messages, has unexpectedly terminated.
38203	Unable to start EMS proxy	The system failed to initialize the Tibco EMS proxy, which is responsible for receiving EMS messages.
0B008	Failed to get log - Log file not found	A generic warning message to signal that the system was unable to retrieve a log file.
0B009	Failed to transform log	The logging module failed to render a particular log file into human-readable format.
0B00A	Failed reading the log	An I/O error occurred when reading a log file from disk.
0B013	Failed to configure XML parser	The logging module was unable to initialize properly.
0B012	Failed to get log - Error with the XML parser	The logging module failed to read the log file.
None	Could not read message content	The system was unable to read the Mime style email message.
50001	Error running the SQL statement: {0}	The system failed to execute the indicated SQL query.
40300	Database logging handler {0} {1} failed. Handler is being disabled	An error occurred when writing logging data to the database. The operation being performed is indicated by parameter {1}.
0B432	Failed to initialize syslog handler {0}	The Syslog module for the indicated Syslog policy could not be initialized.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0B100	Syslog handler {0} {1} failed. Handler is being disabled	An error occurred when writing logging data to the Syslog associated with the Syslog policy {0}. The operation being performed when the error occurred is indicated by parameter {1}.
0B602	Warning encountered while parsing log file	This is a generic error message to indicate log file parsing errors.
0C10B	Downloading software upgrade failed - File {0} not found on the server	The system encountered an error when attempting to download the upgrade file from the server, possibly because the file was not found.
0C10C	Downloading software upgrade failed - {0} is an unknown host	The system failed to download the software upgrade file because the IP address of a host could not be determined.
0C10D	Downloading software failed - The server refused the connection.	They system failed to download the software upgrade file because an error occurred while attempting to connect to the remote address and port. Typically, the connection fails because no process is listening on the remote address/port.
0C100	Downloading failed - Could not retrieve upgrade software from the server	This is a generic error message to indicate that the system failed to download the software upgrade file.
0C103	Software verification failed - The software downloaded from the server could not be verified	As part of the product upgrade process, the system verifies the integrity of the downloaded upgrade file so as to ensure that it is uncorrupted. Typically, the verification fails because signature on the upgrade file was invalid.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0C11C	A version for the upgrade package could not be found	As part of the product upgrade process, the system verifies the product version number of the downloaded upgrade file to ensure that the correct upgrade path is being followed. In this case, the upgrade file did not contain a valid product version number.
0C11B	Upgrades from {0}.x to {1}.x are not supported. This appliance can only be upgraded to {2}.x or {3}.x	As part of the product upgrade process, the system verifies the product version number of the downloaded upgrade file to ensure that the correct upgrade path is being followed. In this case, the system found that the correct upgrade path is not being taken. As a result, the upgraded process could not be completed.
0C115	Cannot find file {0} or it does not contain data	This is a generic error message used by the product upgrade process to indicate that the specified upgrade file is either missing or is empty.
0C111	Error verifying fingerprint	As part of the product upgrade process, the system verifies the integrity of the downloaded upgrade file so as to ensure that it is uncorrupted. This is a generic error message used by the system to capture unexpected errors that might occur during the verification process.
0C116	Upgrade failed - The version of the upgrade package cannot be determined	As part of the product upgrade process, the system verifies the product version number of the downloaded upgrade file to ensure that the correct upgrade path is being followed. In this case, the upgrade filed did not

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		contain a product version number. As a result, the upgrade process could not be completed.
0C107	Software upgrade failed - {0}	The upgrade process failed owing to an error while applying the upgrade file to the system.
0C109	Upgrade failed - Error reading/writing to the process	The upgrade process failed owing to an error while applying the upgrade file to the system.
0C108	Upgrade failed - process interrupted	The upgrade process was interrupted by another process before the upgrade was completed.
0C110	Fingerprint verification failed - The length of the fingerprint {0} is incorrect	As part of the product upgrade process, the system verifies that the fingerprint (digital signature plus digest sum) of the upgrade file is valid. In this case, it was determined that the fingerprint was invalid. As a result, the upgrade process could not be completed.
06011	Monitoring Exception	This is a generic message to indicate one of any number of errors that the system might encounter while monitoring SOAP traffic.
21202	Could not load library	The system could not load libraries necessary for it to configure the network settings.
21009	Cannot set {0} to 100Mbs Full Duplex	An error occurred when the system tried to set the physical characteristics of the indicated interface ({0}) to 100Mbs speed and full duplex data transmission mode.
2100A	Cannot set {0} to Auto-negotiate	An error occurred when the system tried to set the physical characteristics of

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		the indicated interface ({0}) to auto-negotiation communication mode.
21308	Failed to add net route with destination {0} and netmask {1} to {2}	The system failed to add a route to a network ({0}) via the indicated interface ({2}).
2130B	Failed to delete net route with destination {0} and netmask {1} from {2}	The system failed to delete a network route associated with the indicated interface ({2}).
21307	Failed to add host route with destination {0} to {1}	The system failed to add a route to the host ({0}) via the interface ({1}).
2130A	Failed to delete host route with destination {0} from {1}	The system failed to delete the indicated host route ({0}) from the indicated interface ({1}).
21306	Failed to set {0} as the default gateway	The system failed to set the indicated host as the default gateway.
21309	Failed to delete default gateway {0}	The system failed to delete the indicated host as the default gateway.
3520B	could not connect to WSDM	The system failed to start the WSDM Observer owing to connectivity problems with the WSDM manager. Typically, this happens when the WSDM manager is not listening for connections on the address/port as specified on the system Admin UI screen for Unicenter WSDM configuration.
35205	WSDM Observer has had an error while starting	When the system initializes the CA WSDM module, it tests connectivity to the WSDM manager SOAP endpoint as specified on the system's Admin UI screen for Unicenter WSDM configuration. The management IP, management port, and

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		WSDM management directory parameters are used to construct an endpoint query to fetch the WSDL file using the '?WSDL' mechanism. If this query fails for some reason (I/O error while opening connection, timeout, etc), the system logs this error message.
3520A	WSDM has had an unhandled error	This is a generic error message logged by the CA WSDM module to signal only those errors which the system will ignore completely. Typically, such errors occur during the CA WSDM module's monitoring of requests and responses, and are caused by document processing errors such as unsupported encoding.
35304	Exception on Default AV daemon start	The system failed to start the Default AV daemon service.
35305	Exception on Default AV daemon stop	The system failed to stop the Default AV daemon service.
3531D	Problem while updating from URL: {0}	The system failed to update the Default AV files retrieved over HTTP (as configured in the Admin UI). {0} describes the reason for the failure.
3530E	Provided main.cvd is not a Default AV virus database	During update of the Default AV files, the system detected that the new main.cvd is invalid.
3530F	Provided daily.cvd is not a Default AV virus database	During update of the Default AV files, the system detected that the new daily.cvd is invalid.
35308	Exception on Default AV update	This is a generic error message logged by the Default AV module to signal error conditions that might

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		occur during the Default AV update process.
35003	{0} could not be started	The indicated Partner Module failed to initialize.
35005	{0} failed SOAP request handling	The indicated Partner Module failed to handle an incoming SOAP request.
35006	{0} failed SOAP response handling	The indicated Partner Module failed to handle a SOAP response.
35007	{0} failed SOAP fault handling	The indicated Partner Module failed to handle a SOAP fault.
35012	{0} failed notification of accessible WSDL	The system attempted to notify to the indicated Partner Module that the module has access to a WSDL file on the product which the module can use for auto-configuration. The Partner Module failed to process this notification.
3500E	{0} failed XML request handling	The indicated Partner Module failed to handle a request associated with an XML project.
3500F	{0} failed XML response handling	The indicate Partner Module failed to handle a response associated with an XML project.
35010	{0} failed XML fault handling	The indicated Partner Module failed to handle a fault associated with an XML project.
35013	{0} failed WSDL retrieval	The system failed to assemble a list of WSDL URLs associated with the indicated Partner Module.
3500C	{0} failed IDP monitoring	The indicated Partner Module failed to monitor a triggered IDP rule.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
35008	{0} failed response monitoring	The indicated Partner Module failed to monitor the outbound response message.
35009	{0} failed error monitoring	The indicated Partner Module failed to monitor the outbound error message.
35014	Problem "{0}" during virus scan	The Partner virus scan module failed to scan the document (and/or attachment) as indicated by parameter {0}.
35011	Problem during virus scan	This is a generic message used to indicate any of the possible errors that might occur during virus scanning.
0E448	Task ACL search failed	ACL check on a WSDL operation failed.
0E44A	Failed to upgrade {0} to domain {1}	The indicated policy belonging to the indicated domain could not be saved to the system storage.
0E44B	Failed to upgrade pattern match on {0}	The indicated WSDL policy's regular expressions could not be updated.
None	The selected document does not contain an XML Schema	The XML schema was malformed or the document was not an XML schema.
0E703	Invalid schema format	This is a generic message to indicate that the XML Schema was malformed.
0E704	Invalid schema format: {0}	This is a generic message to indicate that the XML Schema was malformed.
0E003	Task list {0} task {1} is not configured	While executing the validate document task, the system found that the task was not configured, possibly because the schemas were not loaded.
0E216	Exception while processing document.	This is a generic error message to indicate that there was an error while

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		processing a document.
0E217	Error removing tasks from repository	An error occurred updating the system storage when removing a task.
0E219	Error saving tasks	An error occurred updating the system storage when saving a task.
0E001	Failed to process task list {0} at task {1}	This is a generic error message to indicate that the indicated task ({1}) failed to execute.
0E005	One or both of the arguments passed to archive are null	A generic warning message to signal that the archive task could not be executed because it did not receive the required data objects to perform its operations.
0E018	No matches found for xpath {0} during archiving task	The Archive task failed because none of the XML elements specified by the user for archiving were found in the actual document.
0E007	Security policy {0} not found	The system tried to execute a XML security task, but could not locate the indicated security policy.
0E008	Something went wrong applying task	A generic message to indicate a processing error during the execution of a task.
0E009	User not identified	A generic error message to indicate that the task that relies on user identification (such as add SAML assertion task) could not be executed to completion because a user was unknown to the system.
0E00A	No signing key found for user {0}	The system could execute a sign document task because the system was unable locate a signing key for the indicated user.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0E00C	Verify task failed	This is a generic error messages to indicate that the verify document task failed to verify the document signature.
0E000	Unknown User Identification Mechanism: {0}	The system was asked to identify the user via an unsupported identification mechanism. Supported mechanisms include, among others, Protocol, WS Security, and SAML X.509.
0E00E	No certificate	This is a generic error message to indicate that the system was unable to process either a user identity task or an add SAML assertion task because it could not find an appropriate X.509 certificate.
0E019	No matches found for xpath {0} during map xml task	The incoming XML document did not contain the indicated XML element which had been selected for the map XML to attributes task.
0E021	No matches found for xpath {0} during map attributes to XML task	The incoming XML document did not contain the indicated XML element which had been selected for the Map attributes to XML task.
0E01E	Directed to virus scan but no scanners are available	The Virus Scan task could not detect any configured Virus scan modules.
0E21F	ACL check failed - Reason unknown; user {0} ACL {1}	While processing an inbound document, the system determined that it could not perform an ACL check to determine whether the user had Execute privileges.
10400	Failed to stop CLI connection	This is a communication error with the CLI. The CLI connection failed to stop after user logout.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
10401	Failed to either accept an incoming CLI connection or be able to handle it	This is a communication error with the CLI. There was an error either when accepting a connection to the CLI or when processing a CLI instruction.
10402	Failed to stop listening for CLI connection	This is a communication error with the CLI. The CLI server could not be stopped.
10200	Failed to read header	This is a communication error with the CLI. There was an error during an interaction between the CLI and the client.
10203	Failed to read payload	This is a communication error with the CLI. There were an error during an interaction between the CLI and the client.
10205	Failed to process input	This is a communication error with the CLI. The CLI server was unable to process the input instruction sent by the client.
41200	Quarantine operation failed	This is a generic error message that a quarantine operation failed to write to the database.
25001	Reporting Manager Exception	This is a generic error message that the system failed to execute a report.
25007	Scheduled Report Run failed - Delivery format not set for Report {0}	The indicated WS Report failed to execute because no delivery format was specified on the Web Services Reporting Criteria policy. Scheduled reports are delivered in the following formats: chart, comma separated values (csv) and XML.
25012	Email not sent. No email address specified for report {0}	No email will be sent out for the indicated WS Report because no recipient email

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		address was specified on the Web Services Reporting Criteria policy.
25011	No data in range for report {0}	No data for the specified range was found with which to create the WS Report. An email will be sent out to the recipient(s) with the details.
25006	Scheduled Report Run failed - Report ID {0}	This is a generic warning message to indicate problems encountered when running WS Reports.
2500E	Retrieve record count failed	The WS Reporting module encountered an error when querying the database for reporting statistics records.
2502B	Failed to schedule report {0}	The indicated WS Report could not be scheduled because the scheduled date could not be determined.
11100	Backup failed - Could not back up system configuration	This is a generic warning message to indicate problems encountered when backing up the system configuration.
08209	Error securing plain socket	The system attempted to upgrade a plain network connection to an SSL-enabled connection, but failed to do so.
12300	Error getting statistics manager	The XML encryption module failed to initialize the statistics counters that are used to keep track of encryption statistics like number of elements successfully encrypted.
12303	Could not get a certificate: {0}	The encryption module was unable encrypt a document because it could not find the needed X.509 certificate indicated by parameter {0}.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
13000	Hash failed - Could not obtain message digest	The system failed to compute the message digest value of a user credential, such as a password.
13007	Login failed - {0} has invalid credentials to log into enable mode	The indicated user could not be authenticated to log into the CLI in enable mode, possibly because the password entered is incorrect.
13005	Login failed - Invalid credentials - {0} via {1,choice,0#CLI/ssh|1#CLI/serial|2#WebAdmin|3#GDM|4#WSDL API} from {2}	The system could not successfully login the indicated user ({0}) over the indicated interface (possible interface choices include: CLI/SSH, CLI/Serial, WebAdmin, GDM, or WSDL API) from the remote address ({2}).
13006	Login failed - No permissions to access this module - {0} via {1,choice,0#CLI/ssh|1#CLI/serial|2#WebAdmin|3#GDM|4#WSDL API}	The logged in user ({0}) does not have the proper permissions to access the indicated module (possible modules include: CLI/SSH, CLI/Serial, WebAdmin, GDM, or WSDL API).
1401D	Invalid CRL: CRL (issuer DN={0}): thisUpdate field ({1}) is later than current date ({2})	This is a warning that the indicated CRL ({0}) cannot be used because its validity period has not arrived yet. The thisUpdate field indicates the issue date of this CRL.
1401E	Invalid CRL: CRL (issuer DN={0}): nextUpdate field ({1}) is earlier than current date ({2})	This is a warning that the indicated CRL ({0}) cannot be used because it is not the latest CRL issued by the CA, i.e., it has expired. The nextUpdate field indicates the date by which the next CRL will be issued.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
14303	Unsupported URI scheme: {0}	This is a warning that a CRL Distribution Point in the X.509 certificate could not be accessed because the URI scheme of the distribution point is unsupported. Currently only HTTP, HTTPS and LDAP URIs are supported.
14302	Error during CDP CertStore processing	This is a generic warning to signal a problem while accessing a CRL Distribution Point.
14006	Could not establish connection to certificate store	A generic warning that something went wrong when retrieving CRLs from a file-based CRL storage.
14223	CRL could not be used because it is not FIPS compliant: {0}	A warning that a CRL was not FIPS-compliant. Typically, this means that the signature type used on the CRL was non-compliant.
14224	CRL could not be used because the certificate that signed it is not FIPS compliant: {0}	A warning that a CRL could not be used because its signer certificate was non-compliant with FIPS. Typically, this means that the key size of the certificate used to sign the CRL was smaller than that allowed by FIPS.
23005	An error occurred while attempting to retrieve the Security World ID	A warning that the system was unable to retrieve the "security world ID" loaded on the HSM. The "security world ID" uniquely identifies a security world.
30095	OpenPGP Signature Verification failed	A generic warning message to signal that an OpenPGP signature verification operation failed. Typically, this occurs when the signature on the document was invalid, when the signed document was corrupted during transfer,

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		or when network I/O fails.
30060	OpenPGP Encryption failed	A generic warning message to signal that an OpenPGP encryption operation failed. Typically, this occurs when there is a problem with the encryption key or when network I/O fails.
3003D	Public Key (Alias {0}, ID {1}) not found	The system failed to find the indicated OpenPGP public key in the system-wide OpenPGP public keyring.
3003E	Private Key (Alias {0}, ID {1} not found	The system failed to find the indicated OpenPGP private key in the system-wide OpenPGP private keyring.
30012	Error while querying keyring	A generic warning message to signal that the system was unable to retrieve an OpenPGP key from one of the system-wide OpenPGP keyrings.
300FD	Key not added. Key validity check failed.	A generic warning message to signal a failed attempt to import an OpenPGP key into the system-wide keyrings. The key was considered invalid; therefore, not loaded.
3003C	Error occurred while flushing keyring	A generic warning message to signal that the system was unable to synchronize the in-memory version of the keyrings with the file-based version. Typically, synchronization occurs after a key has either been deleted or imported.
3006D	OpenPGP decryption failed	A generic warning message to signal that an OpenPGP decryption operation failed. Typically, this occurs when there is a problem using the

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		decryption key or when network I/O fails.
300EF	Error building literal message.	A generic warning message to indicate that an encrypted or signed message could not be built.
300F0	Error building compressed message	A generic warning message to indicate that compression prior to encryption (or after signing) did not complete successfully.
300F1	Error building encrypted message	A generic warning message to indicate that message encryption failed.
300D6	Invalid public key version	The OpenPGP public key version was invalid. Currently version 2, 3, and 4 are supported.
300D1	OpenPGP key date parse error	A generic warning to indicate that the system was unable to parse the dates contained in an OpenPGP key.
300D7	Invalid master key version	The OpenPGP master public key version was invalid. Currently versions 2, 3, and 4 are supported.
300D8	Could not perform operation due to I/O error	A generic warning message to indicate that an OpenPGP operation could not be carried out because of network I/O problems.
30009	Invalid key material	A generic warning message to indicate that the OpenPGP key was unusable.
300F7	Nightly key expiration task error	The scheduled key expiration task (which runs every night to send out expiration or advance alert emails) failed.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
300FC	Unable to send OpenPGP key expiration email because system alert email was not set	The scheduled key expiration task (which runs every night to send out expiration or advance alert emails) failed to send out an email. Typically, this happens when a recipient email address has not been specified.
3004D	Error getting statistics manager	A generic warning message to indicate that the system was unable to initialize the statistics module which will be used for recording OpenPGP transaction statistics.
3004E	Error getting statistics counters: {0}	A generic warning message to indicate that the system was unable to initialize the statistics module which will be used for recording OpenPGP transaction statistics. In particular, one of the counters ({0}) used by the statistics module failed to initialize.
15602	Could not load keys and certificates	A warning message to indicate that PKCS keys could not be loaded into the system after a reboot, global import or GDM transaction.
15600	Could not reset keystore	A warning message to indicate that the system could not reset the PKCS key store during a factory reset operation.
15601	Could not load default signer group	A warning message to indicate that the system could not load the default CA group which contains the default Root CA certificates.
1560B	The supporting HSM key file not found for keystore in import	The supporting HSM key file not found for keystore in import.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
15706	Encountered error while trying to load {0} from keystore	The system failed to retrieve the private key associated with the indicated alias. Typically, this occurs if the key could not be recovered, e.g., the password was incorrect.
15707	Could not load private key from key store for {0}	The indicated key does not exist in the system keystore.
1574F	Loaded unsupported key ({0}) on this platform. Policies using this key may fail to operate properly	The size of the key loaded exceeds the maximum allowed size. The maximum allowed size depends on the system configuration, i.e., whether it is using an HSM.
1570C	Could not load {0} from key store	A generic warning message that the indicated certificate or key could not be loaded from the system key store.
15708	Could not load certificate chain from key store for {0}	The system attempted to load the indicated key pair and its associated certificate chain when it was found that either the key pair did not exist or it did not contain a certificate chain.
15709	First certificate in certificate chain for {0} is null	The system attempted to load the indicated key pair and its associated certificate chain from the system keystore when it was found that the first certificate in the chain (which is the user's certificate corresponding to their private key) was missing.
1570A	Could not load X.509 certificate from key store for {0}	The system was unable to load the indicated X.509 certificate from the system keystore. Typically, this occurs when the indicated certificate does not exist in the keystore.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
15708	Could not load certificate from key store for {0}	The system was unable to load the indicated certificate from the system keystore. Typically, this occurs when the indicated certificate does not exist in the keystore.
15E0F	Unable to send PKCS key expiration email because system alert email was not set	A generic warning message that the nightly key expiration task (which sweeps through all PKCS keys to determine their expiration status) could not send out an email because no email recipients were specified by the Admin UI Administrator.
15E10	Nightly key expiration task error	A generic warning message that the nightly key expiration task (which sweeps through all PKCS keys to determine their expiration status) was unable to process a key owing to some unknown error.
15403	Could not import key and cert chain	The system was unable to import a PKCS 12 key pair.
12219	Client auth failed	The system was unable to authenticate the client peer application based on the X.509 certificate chain presented by the client. Typically, authentication fails because the system does not trust the root X.509 certificate (or one of the intermediary X.509 certificates) presented by the client in the certificate chain.
1221F	Server auth failed	The system was unable to authenticate the server peer application based on the X.509 certificate chain presented by the server. Typically, authentication

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		fails because the system does not trust the root X.509 certificate (or one of the intermediary X.509 certificates) presented by the client in the certificate chain.
12205	null or zero-length client certificate chain	The system failed to authenticate the client (or server) peer application using the X.509 certificate chain presented by the peer application. The failure occurred because the peer application did not present a certificate chain.
12206	null or zero-length authentication type	The system failed to authenticate the client (or server) peer application using the X.509 certificate chain presented by the peer application. The failure occurred because the authentication algorithm parameters were not properly negotiated between the system and the peer application.
1901A	No statistics counter name specified	The statistics module was asked to return a statistics counter but the counter was not named.
1901B	Statistics counter not found: {0}	The system could not retrieve the indicated statistics counter.
46007	Failed to send alert, the system is low on resources	The system was unable to reserve the necessary amount of memory for the alert job owing to low levels of available memory.
46003	Email Send Failed. Email To: {0} Subject: {1} Attempt: {2}. Reason: {3}	The system was unable to send an email alert. The number of attempts made is indicated by parameter {2}, and the reason for failure is indicated by parameter {3}.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
46006	Alert not sent because SMTP Server is not set	The system was unable to send an email alert because no SMTP server was specified (on the Web Admin UI's System screen).
46000	Failed to add attachment	The system encountered an error while adding an attachment to an alert email.
00101	Could not retrieve SSL termination policy {0}; using factory default SSL termination policy	While configuring SSL on one of the Administration servers (e.g., WebAdmin or GDM) the system was unable to retrieve the indicated SSL termination policy and as a result, defaulted to the system-wide default SSL termination policy.
0D03A	Configuring network failed	There was an error while changing the network management configuration. During this configuration change, the system configures the appliance's IP, netmask, routing information, and the state (one-port, two-port, inline modes).
0D018	Invalid topology mode value {0}	An unexpected attempt was made to set the appliance's network state to an illegal value. Allowed state values include one-port, inline and two-port.
0D01E	Error changing topology, switching to previous configuration	The system failed to switch to a new network state and will attempt to restore the old state. Allowed state values include one-port, inline and two-port.
0D009	Failure adding {0,choice,0#net|1#host} route to destination {1}	The system was unable to add a route to the indicated destination. The choice of route type is between net route and host route.

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
0D029	Error setting the WAN and LAN port	The system was unable to set the WAN / LAN port settings when it tried to initialize the network configuration.
0D045	Error setting host route	The system was unable to configure the host routes when it tried to initialize the network configuration.
0D03B	Could not configure bridging interface	An attempt to configure the Ethernet bridging necessary for the Inline Single IP network topology mode failed to complete successfully.
1A000	System monitor thread interrupted	The diagnostic thread which monitors the status of all system components encountered an unexpected error.
1A007	Obtaining an instance of {0} failed	An attempt to access the indicated module failed.
1A004	Shutting down system because of a failure in {0}	An attempt to start the indicated module failed. The system will be shut down.
None	Error secure deleting file {0}; attempting standard delete	An attempt to delete the indicated file in a secure manner failed to complete successfully. The system will go ahead and delete the file in an unsecured, standard manner.
None	Error secure deleting file '0}	A generic message to indicate that an attempt to delete the indicated file in a secure manner failed to complete successfully.
1A101	Could not delete file: {0}	A generic message to indicate that an attempt to delete the indicated file in a secure manner failed to complete successfully.
1A513	DNS configuration failed	An attempt by the system

ERROR CODE	ERROR MESSAGE	ERROR DESCRIPTION
		to configure its DNS settings failed.
1A516	NTP configuration failed	An attempt by the system to configure its NTP settings failed.
1A602	Socket proxy failed to accept client connection for proxying to remote server {0}:{1}	An unsuccessful attempt was made to forward (proxy) a client connection to the indicated remote server.
1A601	Socket proxy failed to connect to remote server {0}:{1}	An unsuccessful attempt was made to forward (proxy) a client connection to the indicated remote server.
1A604	Socket proxy client to server error	An unsuccessful attempt was made to forward (proxy) client data to the remote server.
1A606	Socket proxy server to client error	An unsuccessful attempt was made to proxy remote server data back to the client.

APPENDIX

Appendix A - Constraints in Logging Guide

ELEMENT	CONSTRAINTS	CHAR COUNT
Remote Syslog Policy Name	Unique & case sensitive. Will accept the '@' character	1-32
Data Source User	Unique	Unlimited
Data Source Password	Unique, case sensitive & any ASCII character	Unlimited

Appendix B - Specifications in Logging Guide

ELEMENT SUPPORTED	SPECIFICATIONS
Log Config	The default Log Lifespan (in days) is 15. The log lifespan may be configured to hold a maximum of 90 days of logs on the system. Once the maximum is reached, a new log file is started, and no older entries are retained.
Internal Logs	Logs are limited to 1GB per day. Once the limit has been reached the log is deleted and a new one is started.
Remote Syslog	Up to six servers can be specified to be forwarded syslog datagrams.
Packet Captures supported	Users may capture up to 100,000 packets per capture on the Packet Capture screen. **
Database Connections	99
Database Support	Oracle 9i, 10g, MySQL V3.23.36 or higher, DB2 7.2 (DB2 8.3*).

* Available with patch upgrade.
** Limited only by disk space.

Appendix C - Database Dictionary for Logging Tables

The following tables list common database terms, definitions and conventions used in the Logging database.

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
ADMINISTRATIVE_LOG			Device Audit Log
	ID	NUMBER(16)	Record Key (sequence)
	SOURCE	VARCHAR2(21)	Source IP address and Port
	LINENUM	VARCHAR2(16)	Line number in hex format
	ISFIPS	CHAR(1)	Indicates if the device is running in FIPS mode. Valid values are Y and N
	TIME	TIMESTAMP	Time and date
	TIMEZONE	VARCHAR2(3)	GMT Zone
	SESSIONID	VARCHAR2(16)	Session ID
	SOURCEUSER	VARCHAR2(80)	User ID of the web admin user
	SOURCEIP	VARCHAR2(16)	IP address of were the web admin logged in from
	LOGLEVEL	VARCHAR2(8)	The set logging level
	MSGCODE	VARCHAR2(8)	Log message ID code
	MSG	VARCHAR2(2000)	Description of log message ID code

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
RUNTIME_LOG			Device System Log
	ID	NUMBER(16)	Record Key (sequence)
	SOURCE	VARCHAR2(21)	Source IP address and Port
	LINENUM	VARCHAR2(16)	Line number in hex format
	ISFIPS	CHAR(1)	Indicates if the device is running in FIPS mode. Valid values are Y and N
	TIME	TIMESTAMP	Time and date
	TIMEZONE	VARCHAR2(3)	GMT Zone
	LOGLEVEL	VARCHAR2(8)	The set logging level
	MSGCODE	VARCHAR2(8)	Log message ID code
	MSG	VARCHAR2(2000)	Description of log message ID code

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
IDP_AUDIT			Intrusion Detection and Prevention (IDP) Log
	ID	NUMBER(16)	Record Key (sequence)
	EVENTTIME	TIMESTAMP	Time and date
	EVENTTIMEZONE	VARCHAR2(3)	GMT Zone
	SOURCE	VARCHAR2(21)	Source IP address of request
	SOURCEUSER	VARCHAR2(80)	User ID of the authenticated client (protocol based, supports HTTP and SSL)
	SOURCEIP	VARCHAR2(16)	Client IP address
	SOURCEPORT	NUMBER(8)	Client Port number
	STATUSCODE	NUMBER(8)	HTTP code
	IDPRULE	VARCHAR2(80)	Name of IDP rule
	NETPOLICY	VARCHAR2(80)	Name of Network Listener Policy
	CRITERION	VARCHAR2(80)	IDP Rule criterion
	PERIOD	VARCHAR2(80)	IDP Rule period
	VALUE	VARCHAR2(80)	IDP Rule value
	WSDLPORT	VARCHAR2(80)	Port from WSDL file
	WSDLSERVICE	VARCHAR2(80)	Service name from WSDL file
	WSDLOPERATION	VARCHAR2(80)	Name of Operation from WSDL file
	WSDLREQUEST	VARCHAR2(80)	Name of Operation input parameter from WSDL
	WSDLRESPONSE	VARCHAR2(80)	Name of Operation output parameter from WSDL

Appendix D - Database Dictionary for Database Tables

The following tables list common database terms, definitions and conventions used with the Data Source databases.

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
META_DATA			Stores selected element names and there values for archive task policies
	ID	NUMBER SEQUENCE	Record key (sequence)
	NAME	VARCHAR2(255)	XML element name
	VALUE	VARCHAR2(255)	XML element value
	CLASS	NUMBER	Unused field
	DATATYPE	VARCHAR2(255)	Set from the archive task policy. Valid values are: string, integer, float, boolean, date
	DESCRIPTION	VARCHAR2(255)	Set from the archive task policy comment textbox
	TIMESTAMP	DATE	Device system date

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
XML DOCUMENT			Stores the xml message as a blob
	ID	NUMBER SEQUENCE	Record key (sequence)
	XML	BLOB	XML message

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
DOCUMENT_NAME			Store the name of the archive task list
	ID	NUMBER SEQUENCE	Record key (sequence)
	NAME	VARCHAR2(255)	Name of archive task list
	TIMESTAMP	DATE	Device system date

Index

10g Oracle database support....15
10g RAC
  Oracle Real Application Cluster support....15
2005 Microsoft SQL Server database support.15
4 My SQL database support 15
5 My SQL database support 15
7.2 DB2 database support 15
9i Oracle database support....15
archive logs 9
archiving
  asynchronous mode for database 18
  connect descriptor 18
  database name 18
  database port....18
  database server IP....18
  database username 18
  databases supported 18
  max connections....18
  password for database user 18
  synchronous mode for database 18
Archiving
  terms....17
  upgrade db driver....16
Archiving screen....15
Audit logs....2
code in Internal Logs....8
conventions used 1
Daemon Facility code
  Syslog 12
Database
  upgrading drivers for....15
database dictionary for Logging tables 8
DB2 connectivity
  setting up DB2 server for JDBC proxy....17
DB2 database schema name....18
DB2 support for archiving....15
Download format for logs
  HTML 4
  plain text....4
  XML....4
download Packet Capture to local file system .14
Error Codes in system....20
Error state in Internal Logs....8
examples for Internal Logs....8
examples for Remote Syslogs 13
General User Facility code
  Syslog 12
GNU zip mode....4
HTML as download format for logs 4
ID in Internal Logs 7
Internal Log Configuration screen
  terms....4
Internal Logs
  code....8
  Error state....8
  examples 8
  ID 7
  message 8
  session number 7
  time....7
  Warning state 8
Internal Logs screen
  terms....7
Local 0 Facility code
  Syslog....12
Local 1 Facility code
  Syslog....12
Local 2 Facility code
  Syslog....12
Local 3 Facility code
  Syslog....12
Local 4 Facility code
  Syslog....12
Local 5 Facility code
  Syslog....12
Local 6 Facility code
  Syslog....12
Local 7 Facility code
  Syslog....12
log lifespan....5
Logging tables in database dictionary 8
Logs
  archiving 9
  Audit logs....2
  setting refresh time for logs....8
  System logs....2
message in Internal Logs....8
Microsoft SQL Server support for archiving....15
MySQL support for archiving 15
Oracle database schema name....18
Oracle support for archiving....15
Packet Capture
  downloading to local file system....14
  starting and stopping 13
packet captures....13
plain text as download format for logs 4
policy name
  Syslog....11
Remote Syslogs
  example....13
  terms....11
schemas supported on dbs....18
Server IP
  Syslog....12
session number in Internal Logs....7
set refresh time for logs 8

set up DB2 server for JDBC proxy 17
Settings screen
GNU zip mode 4
log lifespan 5
zip mode 4
start and stop Packet Capture 13
summary of Error Codes 20
Syslog
policy name 11
Server IP 12
Syslog Port 12
Syslog Daemon Facility code 12
Syslog General User Facility code 12
Syslog Local 0 Facility code 12
Syslog Local 1 Facility code 12
Syslog Local 2 Facility code 12
Syslog Local 3 Facility code 12
Syslog Local 4 Facility code 12
Syslog Local 5 Facility code 12
Syslog Local 6 Facility code 12
Syslog Local 7 Facility code 12
Syslog Port 12
System logs 2
terms
for Archiving screen 17
terms on Internal Log Configuration screen
SETTINGS 4
terms on Internal Logs screen 7
time in Internal Logs 7
upgrade database drivers 15
upgrading db driver 16
Warning state in Internal Logs 8
XML as download format for logs 4
zip mode 4