IBM Security Access Manager for Mobile
Version 8.0.0.1

Error Message Reference

GC27-6210-01

IBM Security Access Manager for Mobile
Version 8.0.0.1

Error Message Reference

IBM

GC27-6210-01

Note

Before using this information and the product it supports, read the information in “Notices” on page 345.

Edition notice

Note: This edition applies to version 8.0.0.1 of IBM Security Access Manager for Mobile (product number 5725-L52) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

About this publication

The *IBM Security Access Manager for Mobile Error Message Reference* lists the error and warning messages provided by IBM Security Access Manager for Mobile.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Mobile library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

IBM Security Access Manager for Mobile library

The following documents are available online in the IBM Security Access Manager for Mobile library:

- *IBM Security Access Manager for Mobile Configuration Guide*, SC27-6205-00
- *IBM Security Access Manager for Mobile Administration Guide*, SC27-6207-00
- *IBM Security Access Manager Appliance Administration Guide*, SC27-6206-00
- *IBM Security Access Manager for Mobile Auditing Guide*, SC27-6208-00
- *IBM Security Access Manager for Mobile Troubleshooting Guide*, GC27-6209-00
- *IBM Security Access Manager for Mobile Error Message Reference*, GC27-6210-00

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security IBM Security Access Manager for Mobile library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
The IBM Publications Center site (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. You can use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the IBM Accessibility website at http://www.ibm.com/able/.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Access Manager for Mobile Troubleshooting Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Message overview

Messages indicate events that occur during the operation of the system.

Depending on their purpose, messages might be displayed on the screen. By default, all informational, warning, and error messages are written to the message logs. The logs can be reviewed later to determine what events occurred, to see what corrective actions were taken, and to audit all the actions performed. For more information about message logs, see the *IBM Security Access Manager for Mobile Troubleshooting Guide*.

Message types

IBM® Security Access Manager for Mobile uses messages of specific types.

The following types of messages are used:

Informational messages
Indicate conditions that are worthy of noting but that do not require you to take any precautions or perform an action.

Warning messages
Indicate that a condition has been detected that you should be aware of, but does not necessarily require that you take any action.

Error messages
Indicates that a condition has occurred that requires you to take action.

Message format

Messages logged by IBM Security Access Manager for Mobile adhere to the Tivoli® Message Standard. Each message consists of a message identifier (ID) and accompanying message text.

Message ID format

A message ID consists of 10 alphanumeric characters that uniquely identify the message.

A message ID in Security Access Manager for Mobile is composed of:

- three-character product identifier
- two-character or three-character component or subsystem identifier
- three-digit or four-digit serial or message number
- one-character type code indicating the severity of the message

The figure that follows shows a graphical representation of a possible message ID and identifies its different parts. (Some messages might use 2 characters for the component ID and 4 digits for the serial number.)

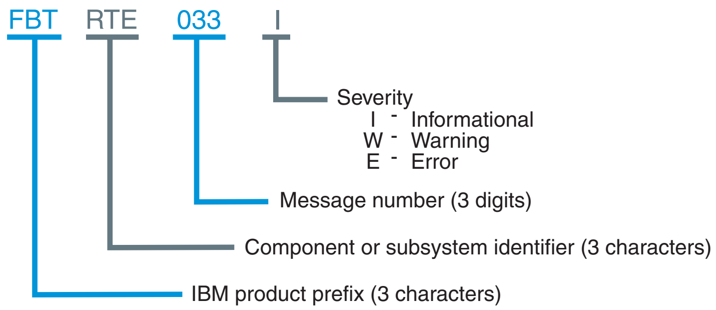
FBT
RTE
033
I
Severity
I - Informational
W - Warning
E - Error
Message number (3 digits)
Component or subsystem identifier (3 characters)
IBM product prefix (3 characters)

Figure 1. Message ID format

Component identifiers

The component identifier indicates which component or subsystem produced the message.

ADM	Administration commands
AUD	Audit
CC	Common Auditing and Reporting Service disk cache
CDS	InfoCard messages
CE	Common Auditing and Reporting Service emitter
CFG	Configuration properties
CLI	Command-line interface
CO	Common Audit Service Configuration Console
CON	Security Access Manager console
CTG	Authorization service
DPW	Secure reverse proxy
FMS	Management service
FBT	Protocol service
IDS	Identity service
IN	Common Auditing and Reporting Service installation
ISJ	Alias service JDBC component
ISL	Alias service LDAP component
IVT	Installation verification test
KES	Key service keystore management
KJK	Key service keystore management
LIB	Liberty single sign-on protocol
LOG	Logging
MB	Common Audit Service Configuration MBean
MGT	Management

MET	Metadata handling
MOD	Module
OID	OpenID messages
PWD	Password handling
RPT	Report messages
RTE	Runtime environment component configuration
SML	SAML single sign-on protocol
SOC	SOAP client
SPS	Single sign-on protocol service
STM	Secure token service
STS	Secure token service modules
STZ	RACF® PassTicket tokens
SU	Common Audit Staging Utility
TAC	Tivoli Access Manager configuration as point-of-contact server
TRC	Trust client
USC	User self care
WS	Common Auditing and Reporting Service Mobile service
WSF	WS-Federation single sign-on protocol
WSP	Provisioning service
WSS	Mobile services security management
XS	Common Audit Service XML data store
XU	Common Audit Service XML store utilities

Severity

Associated with each message is a severity level that indicates whether corrective action must be taken.

Table 1. Severity level

Severity	Description

I (Informational)	Provides information or feedback about normal events that occur. In general, no action needs to be performed in response to an informational message.
	`FBTRTE033I The domain default was successfully created.`
	`FBTSTM066I The Trust Service has been disabled.`

W (Warning)	Indicates that a potentially undesirable condition has occurred, but processing can continue. Intervention or corrective action might be necessary in response to a warning message.
	`FBTLOG002W An integer was expected.`
	`FBTTRC004W The returned RequestSecurityTokenResponse did not have a wsu:Id`

Table 1. Severity level (continued)

Severity	Description
E (Error)	Indicates that a problem has occurred that requires intervention or correction before processing can continue. An error message might be accompanied by one or more warning or informational messages that provide additional details about the problem. FBTCON013E The federation with ID *insert* could not be retrieved from the single sign-on protocol service. Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service. FBTSML260E The binding value *value* for attribute *attr* is not valid for profile *profile*.

Message text

The text of the message, in the system locale, also is recorded in the log file. If the message text is not available in the desired language, the English language text is used.

Chapter 2. Secure Reverse Proxy Messages

These messages are provided by the secure reverse proxy component.

CTGSI0301E Initialization of the distributed session cache server failed.

Explanation: The distributed session cache server was unable to initialize and cannot function until the cause of the failure is corrected.

Administrator response: Inspect the application server log files for details, take any necessary corrective action, and restart the distributed session cache server.

CTGSI0302W The client is not registered with the distributed session cache server.

Explanation: The client is not registered with the distributed session cache server. Clients must register before performing any operations.

Administrator response: No action is necessary.

CTGSI0303E The client is not authorized to perform the requested operation.

Explanation: The client attempted to perform an operation that it is not authorized to perform.

Administrator response: If the client is expected to be authorized to perform the requested operation then correct the security policy that applies to the distributed session cache server.

CTGSI0304W The concurrent session limit for the user has been reached.

Explanation: The attempt to create a new session for the user failed because creating another session would exceed the concurrent session limit for the user.

Administrator response: No action is necessary.

CTGSI0305W The client attempted to create a session with a session ID that is already in use.

Explanation: The session ID specified for the new session already exists in the shared session cache. The client must choose a new ID for the session.

Administrator response: No action is necessary.

CTGSI0306E The client attempted to use a replica set that does not exist in the distributed session cache server configuration.

Explanation: The client attempted to use a replica set that has not been specified in the distributed session cache server configuration. All replica set names must be specified in the distributed session cache server configuration.

Administrator response: Verify the client's configuration specifies all replica set names correctly and the distributed session cache server's configuration includes all any necessary replica sets.

CTGSI0307E The client attempted to perform an operation on a replica set that it has not joined.

Explanation: When clients connect to the distributed session cache server they must specify the names of all replica sets they will use. This error indicates a client has not done so.

Administrator response: Verify the client is correctly configured.

CTGSI0308E The client attempted to create or modify a session such that its concurrent session key would not be valid.

Explanation: Sessions stored by the distributed session cache server can include session data items indicating the concurrent session key. Either all of these session data items must be present and valid, or none of them. This error indicates that some, but not all, of the session data items were present.

Administrator response: This error indicates a problem with the configuration of the client or a programming error. Examine the sections of the client configuration relating to concurrent session limits and session displacement. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0309W The client's version of the session is out of date.

Explanation: The client issued a session modification request based on an out of date version of the session. The client must retrieve the current version of the session and retry the request.

Administrator response: No action is necessary.

CTGSI0310W The client specified a capability mask that does not match the active capability mask.

Explanation: The client specified a capability mask that does not match the active capability mask. The client will not be able to register until the distributed session cache server is restarted and initialized with a matching capability mask.

Administrator response: Ensure all clients accessing the distributed session cache server are compatible with the version of the distributed session cache server. It may be necessary to restart the distributed session cache server and all active clients to correct this condition. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0311E The distributed session cache server was unable to generate a new key.

Explanation: The distributed session cache server was unable to generate a new key.

Administrator response: Examine the distributed session cache server logs for further details. It may be necessary to restart the distributed session cache server completely to correct this condition.

CTGSI0312W The session was not found.

Explanation: The distributed session cache server was unable to find a session with the session ID specified by the client.

Administrator response: No action is necessary.

CTGSI0313E A parameter value was not valid.

Explanation: The client specified a parameter value that was not valid to the distributed session cache server.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0314E The specified client instance ID has already been registered by another client.

Explanation: Each client that makes use of the distributed session cache server must register a unique instance ID. This message indicates a client attempted to use an instance ID that another client had already registered.

Administrator response: Restart the client. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0315E The distributed session cache server encountered an error and was unable to complete the operation.

Explanation: While processing the client's request, the distributed session cache server encountered an error that prevented it from completing the operation.

Administrator response: Inspect the distributed session cache server logs to identify the nature and cause of the error. Take any necessary corrective measures. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0316E The client attempted to register using an active client name from a different IP address than was used to register the active instance.

Explanation: The client attempted to register using an active client name from a different IP address than was used to register the active instance.

Administrator response: Inspect the client's configuration to ensure each client uses a unique replica name. The distributed session cache server logs indicate the IP addresses of the clients using the same client name. If the IP address of the client has recently changed, wait until the distributed session cache server expires the previous registration before restarting the client. The amount of time to wait is controlled by the distributed session cache server's client idle timeout configuration parameter.

CTGSI0317W The client attempted an idle timeout operation but the capabilities required to support idle timeouts have not been enabled.

Explanation: The first client to start-up requested a set of capabilities from the distributed session cache server that did not include the session interest list capability. This capability is required to support idle timeout of sessions.

Administrator response: Examine any client configuration options relating to distributed session cache server capabilities. To change the active set of capabilities, all clients must be shut-down, and the distributed session cache server restarted. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0319E The client issued a change session request with no session data changes.

Explanation: The client issued a change session request with no session data changes.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0320E The interface version requested by the client is not supported by this server.

Explanation: The interface version requested by the client is not supported by this server.

Administrator response: Ensure the versions of client software and server software are compatible.

CTGSI0321W The distributed session cache server detected a conflict resulting from replication of the changes.

Explanation: The distributed session cache server detected a conflict resulting from replication of the changes.

Administrator response: No action is necessary.

CTGSI0322E An invalid request parameter was passed to the session administration interface.

Explanation: An invalid request parameter was passed to the session administration interface.

Administrator response: Retry the operation specifying valid parameters. Consult the IBM Security Access Manager Shared Session Administration Guide for information about valid request parameters.

CTGSI0323E An unrecognized administration operation was passed to the distributed session cache server's administration interface.

Explanation: The distributed session cache server's administration interface can only handle known request types from its clients. An unrecognized request type was sent from a client.

Administrator response: Ensure the requested administration operation is currently enabled and that the version of the client software in use is supported by this version of the distributed session cache server.

CTGSI0324E The request from the client requires a capability of the distributed session cache server that is not enabled by the distributed session cache server.

Explanation: The request from the client requires a capability of the distributed session cache server that is not enabled by the distributed session cache server.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0325E The client attempted to use a session realm that does not exist in the distributed session cache server configuration.

Explanation: The client attempted to use a session realm that does not exist in the distributed session cache server configuration. All session realm names must be specified in the distributed session cache server configuration.

Administrator response: Retry the operation specifying a defined session realm.

CTGSI0327W The distributed session cache server was not able to replicate the changes across the cluster.

Explanation: The distributed session cache server was not able to replicate the changes resulting from the request across the cluster.

Administrator response: Check the distributed session cache server logs for more information concerning this error. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSI0328E Authentication failed. You have used an invalid user name or password.

Explanation: An invalid user name or password was supplied.

Administrator response: Check your authentication information and try again.

CTGSI0329E Authentication failed. The account associated with the user has expired.

Explanation: The users account has expired.

Administrator response: Contact your system administrator to have the account reactivated.

CTGSI0330E Authentication failed. The credential associated with the user has expired.

Explanation: The user's credential has expired. This error might indicate that the user's password has expired.

Administrator response: Contact your system administrator to renew the users credential.

CTGSI0331W The session limit for this session realm has been reached.

Explanation: The attempt to create a new session for the user failed because creating another session would exceed the session limit for the session realm.

Administrator response: No action is necessary.

CTGSM0301E The new instance, *%s*, of the client, *%s*, could not be stored.

Explanation: The session management server was unable to store the details of the client.

Administrator response: Examine the log for further detailed messages regarding the error, take any necessary corrective action, and restart the client. It may also be necessary to restart the session management server.

CTGSM0303E The list of keys stored in the session list store, *%s*, for the replica set, *%s*, could not be retrieved.

Explanation: The session management server was unable to retrieve the list of keys stored in the given session list.

Administrator response: Examine the log for earlier messages regarding this error and take any necessary corrective action. If the problem persists, restart the session management server.

CTGSM0304E The session, *%s*, in the replica set, *%s*, does not have a concurrent session key.

Explanation: Every session must include the data item used as the key for maintaining concurrent session counts. A session was either created without the data item, or the data item was removed as part of a session update.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0305E The session, *%s*, in replica set, *%s*, could not be stored.

Explanation: A session could not be stored in the session cache.

Administrator response: Examine the log for other messages regarding the error and take any necessary corrective action. The error might indicate resource exhaustion.

CTGSM0306W The session management server has rejected a session modification request from the client, *%s*, for the session, *%s*, in the replica set, *%s*, based on an outdated version of the session. The client has version number *%s*, while *%s* is the current version number.

Explanation: A client has issued a session update request based on an outdated version of the session. The request has been rejected.

Administrator response: This condition can sometimes occur during normal operation of the session management server. The client can correct the condition by first requesting the current version of the session, and then re-issuing the update request based on that version. This error could also indicate a problem with the client.

CTGSM0310W The client, *%s*, is not registered.

Explanation: The client attempted the perform an operation without first registering with the session management server.

Administrator response: No action is necessary.

CTGSM0311W Returning result: *%s* (code: 0x*%s*).

Explanation: The specified result is being returned to the client. This message is usually only logged when an error result is returned.

Administrator response: If the result indicates an error has occurred, examine the log for further details and take any necessary corrective action.

CTGSM0312E A new instance of the client, *%s*, has attempted to start-up. The existing instance ID is *%s*, with the client ID of *%s*. The second instance ID is *%s*, with IP address *%s*.

Explanation: A replica attempted to register with the session management server using a replica name that was already active, and its client ID was different to that used to register the active instance. The replica's registration was denied by the session management server.

Administrator response: This message indicates two replicas are configured with the same replica name, and both are attempting to register with the session management server. If this message coincides with a planned client ID change for a replica machine, the replica cannot be restarted until its previous instance is expired. Otherwise, examine the configuration on the machines with the client ID's given to determine whether they have been configured to use the same replica name. If so, change the replica name on one machine. It may be necessary to explicitly configure the replica name on both machines to avoid a conflict.

CTGSM0316E Single sign-on was requested in session realm, *%s*, but there is no single sign-on mapping configured.

Explanation: A client requested a session be created using single sign-on within a session realm, but the session management server configuration does not specify a single sign-on mapping for the session realm.

Administrator response: Modify the session management server configuration so it specifies a single sign-on mapping to use within the session realm. The session management server must be restarted for this change to take effect.

CTGSM0317E An error occurred during statistics gathering setup: *%s*.

Explanation: An error occurred during statistics gathering setup. Statistics will not be recorded until the error is corrected and the session management server application is restarted.

Administrator response: Examine this and earlier log messages for more information regarding the error. Once the error has been corrected, restart the session management server.

CTGSM0318E Initialization of the event timer class, *%s*, failed: *%s*

Explanation: The session management server uses different event timer classes in different runtime environments. This message indicates the event timer class for this environment is not available. The session management server will not function without an event timer.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0319E The database, *%s*, could not be opened.

Explanation: The database may not exist or may have other problems.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0321E The event does not specify a session.

Explanation: The event may be corrupt or incorrectly created because it does not specify a session.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0322E The session management server could not copy the file *%s* to *%s*: *%s*

Explanation: The session management server could not copy a file.

Administrator response: Examine the error message for more information on the error. Restart the session management server application to retry the operation. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0323E The administration interface version, *%s*, requested by the client is not supported by the server. The server supports the following versions of the administration interface: *%s*.

Explanation: The interface version requested by the client is not supported by this server.

Administrator response: Ensure the versions of client software and server software are compatible.

CTGSM0324W J2EE security is disabled for this application server. No security checks will be performed by the session management server administration interface.

Explanation: The session management server administration interface security depends on J2EE security being enabled in the application server.

Administrator response: If security is required for the session management server administration interface then enable J2EE security and restart the application server.

CTGSM0325E Unable to retrieve message text for message code {0}.

Explanation: The message text for the specified message code could not be retrieved.

Administrator response: Verify the files that make up the session management server application are present in the WebSphere application server installed applications directory. The session management server will not function correctly until this problem is corrected. It may be necessary to reinstall the session management server application to correct this problem.

CTGSM0326E The file, *%s*, could not be deleted.

Explanation: A file could not be deleted.

Administrator response: Check that the file system is writable, and that the file system permissions allow the file to be deleted.

CTGSM0327E An error occurred during initialization of the class, *%s***, specified by property,** *%s***:** *%s*

Explanation: An error occurred during initialization of an event handler class.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. The session management server application must be restarted.

CTGSM0328E An error occurred while replicating session management server data: *%s*

Explanation: An error occurred while replicating session management server data. This error may indicate communication problems between cluster members.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. It may be necessary to restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0329E The session management server was not able to replicate an operation on the key, *%s***, in the map,** *%s***.**

Explanation: The session management server was not able to replicate an operation on an entry in a storage map to other nodes in the cluster. The client issuing the request that resulted in the operation will be notified of the failure.

Administrator response: Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation or server availability problems. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0330E The session management server instance was not able to establish communication with other instances in the cluster: *%s***.**

Explanation: The session management server instance was not able to establish communication with other instances in the cluster.

Administrator response: Restart the server on which this instance of the session management server runs. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0332E The session management server was not able to obtain a cluster-wide lock on the item, *%s***:** *%s*

Explanation: The session management server was not able to obtain a cluster-wide lock on a data item in order to update it.

Administrator response: Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation or server availability problems. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0333E The session management server was not able to release a lock on the item, *%s***:** *%s*

Explanation: The session management server was not able to release a cluster-wide lock on a data item after updating it.

Administrator response: Check that all WebSphere cluster members are running correctly, and that the network connections between each node are functioning. Multiple instances of this error may indicate resource starvation or server availability problems. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0334E Transfer of existing session management server data to a new instance, *%s***, failed:** *%s***.**

Explanation: Transfer of existing session management server data to a new instance failed. The new instance will not process requests until it is restarted.

Administrator response: Restart the server on which the new instance runs. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0335E An error occurred while receiving session management server data from another instance: *%s*

Explanation: An error occurred while receiving session management server data. This error may indicate communication problems between cluster members.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. It may be necessary to restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0336E The replication operation message was badly formed.

Explanation: A replication operation message, used to transfer data between session management server instances, was badly formed.

Administrator response: This message indicates a serious problem relating to session management server data replication. Restart the session management server application. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0337E Initialization of the event worker class, *%s*, **failed:** *%s*

Explanation: The session management server uses different event worker classes in different runtime environments. This message indicates the event worker class for this environment is not available.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0450E An SQL error has occurred: *%s* **(SQL error code:** *%s*, **SQL state:** *%s***).**

Explanation: The session management server has encountered an SQL error during a database operation.

Administrator response: This message may indicate resource starvation problems, such as disk space or memory exhaustion. Examine the system's resource usage to see if this is the case. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0451E The JDBC driver could not be initialized: *%s*

Explanation: The JDBC driver required to access the session management server database tables could not be initialized.

Administrator response: Check the properties of the JDBC data source configured for use by the session management server and restart the session management server.

CTGSM0452E The database table, *%s*, **was not found.**

Explanation: One of the session management server database tables is missing.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0453E The column, *%s*, **in the database table,** *%s*, **was not found.**

Explanation: A column in one of the session management server database tables is missing.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0454E The column, *%s*, **in the database table,** *%s*, **has the wrong type. The expected type is** *%s*, **but the type in the database is** *%s***.**

Explanation: A column in one of the session management server database tables has the wrong type.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0457E The column, *%s*, **in the database table,** *%s*, **is not a primary key.**

Explanation: A column in one of the session management server database tables is not a primary key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0458E The column, *%s*, **in the database table,** *%s*, **is not configured to use a foreign key.**

Explanation: A column in one of the session management server database tables is not configured to use a foreign key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0459E The foreign key column, *%s*, in the database table, *%s*, imports its key from the table, *%s*, but it should import from the table, *%s*.

Explanation: A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0460E The foreign key column, *%s*, in the database table, *%s*, imports its key from the column, *%s*, but it should import from the column, *%s*.

Explanation: A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0461E The foreign key column, *%s*, in the database table, *%s*, uses the update rule, *%s*, but it should use the update rule, *%s*.

Explanation: A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0462E The foreign key column, *%s*, in the database table, *%s*, uses the delete rule, *%s*, but it should use the delete rule, *%s*.

Explanation: A column in one of the session management server database tables has a misconfigured foreign key.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0463E No index was found for the column, *%s*, in the database table, *%s*.

Explanation: The database does not contain an index for the specified column.

Administrator response: Correct the database configuration and restart the session management server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0464E The JDBC driver could not be initialized.

Explanation: The JDBC driver required to access the session management server database tables could not be initialized.

Administrator response: Check the properties of the JDBC data source configured for use by the session management server. The session management server may need to be restarted.

CTGSM0602E The session management server was not able to load the class *%s*: *%s*.

Explanation: The session management server configuration specifies that it must load the given class for SSO mapping, session data inspection, or data replication. The class could not be loaded, for the given reason.

Administrator response: Verify all class names specified in the session management server configuration are spelled correctly, and all necessary files are present in the application's class path.

CTGSM0603E The session management server was not able to create an instance of the class *%s*: *%s*.

Explanation: The session management server encountered an error while trying to instantiate the class.

Administrator response: Check the class name is correct, and the Java security policy allows the session management server to instantiate the class, then restart the application. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0604E The session management server configuration specifies an illegal value for the *%s* property: *%s*.

Explanation: The property value must be a positive integer, but the configuration file specifies either a non-integer or a negative value.

Administrator response: Modify the configuration file so a positive integer is specified for the named property, and restart the session management server.

CTGSM0617E An unknown single sign-on mapping, *%s*, was specified for the session realm, *%s*.

Explanation: The single sign-on mapping name specified in the configuration for a session realm does not match any of the configured single sign-on mappings.

Administrator response: Verify the single sign-on mapping name is correctly specified and restart the session management server.

CTGSM0618E The session management server was unable to identify the version of WebSphere application server.

Explanation: The session management server application needs to identify the application server version in order to perform statistics gathering. This message indicates that it was not able to do so.

Administrator response: Ensure you are running the session management server application on a supported version of WebSphere application server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0619E A Java class name is required to be specified in the session management server configuration by property *%s*.

Explanation: Each extension specified in the session management server configuration must include the name of a Java class implementing the extension functionality. The specified property does not specify a class name.

Administrator response: Examine the session management server configuration. Verify all extension names and property names are specified correctly, and each extension configuration includes the correct Java class name. Restart the session management server application.

CTGSM0620E The Java class, *%s*, specified by property, *%s*, is not a valid session management server *%s* class.

Explanation: The Java class configured for the specified property name does not an implementation of the expected interface.

Administrator response: Ensure all Java class names specified in the session management server configuration are correct. Restart the session management server application.

CTGSM0622W The session management server was unable to read the Tivoli Common Directory configuration file: *%s*

Explanation: The session management server was unable to read the Tivoli Common Directory configuration file. The Tivoli Common Directory can be used in the logging destination configuration. Any log handlers configured to use the Tivoli Common Directory variable will write to an incorrect location until the problem is corrected.

Administrator response: Verify the Tivoli Common Directory configuration file exists and is readable. Restart the session management server once the problem has been corrected

CTGSM0626E An error occurred while reading the configuration file *%s*: *%s*

Explanation: An error occurred while attempting to read the configuration file.

Administrator response: Examine the error message to determine the cause of the problem. Once the problem has been corrected, restart the session management server.

CTGSM0627E An error occurred while writing the configuration file *%s*: *%s*

Explanation: An error occurred while attempting to write the configuration file.

Administrator response: Examine the error message to determine the cause of the problem. Once the problem has been corrected, restart the session management server.

CTGSM0633W The session management server was unable to access the Windows registry: *%s*

Explanation: The session management server attempts to access the Windows registry in order to locate the Tivoli Common Directory configuration file and the product installation directory. In this case the session management server was unable to access the Windows registry.

Administrator response: Examine the error message to determine the cause of the problem. Verify the WebSphere application server configuration includes a shared library definition for the session management server registry access library. Check the session management server deployment descriptor includes a reference to this shared library. If Java 2 security policy is enforced, ensure the session management server policy file includes the permissions required to load the registry access shared library. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0634E The session management server installation directory could not be determined: *%s*

Explanation: The session management server was unable to determine the directory in which it is stored under the WebSphere application server install applications directory.

Administrator response: Examine the error message to determine the cause of the problem. If Java 2 security policy is enforced, ensure the session management server policy file includes the permissions required to read files in the WebSphere application server configuration directory. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0637W An error was encountered while reading output from the process, *%s***:** *%s*

Explanation: An error was encountered while reading output from a process run during session management server configuration.

Administrator response: No action is necessary. If the configuration process failed, not all of the output from the process will be available.

CTGSM0638E The command, *%s***, run during session management server configuration has exceeded the time limit of** *%s* **seconds and has been terminated.**

Explanation: A process run during session management server configuration has exceeded the time limit. The process has been terminated, and session management server configuration will fail as a result. The captured output from the process will be included in a later log message.

Administrator response: Examine the output from the process, which is included in a later log message, to determine the reason the process did not complete within the time limit. Restart the session management server to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0639E An error was encountered while attempting to execute the command, *%s***, during session management server configuration:** *%s*

Explanation: An error was encountered while attempting to execute a process during session management server configuration.

Administrator response: Examine the error message to determine the cause of the problem. Restart the session management server application to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0640E The directory, *%s***, could not be created.**

Explanation: A directory could not be created.

Administrator response: Check that the file system is writable and has sufficient free space, and that the file system permissions allow the directory to be created.

CTGSM0641E An error was encountered while configuring the Tivoli Common Directory: *%s*

Explanation: An error was encountered while configuring the Tivoli Common Directory.

Administrator response: Examine the error message to determine the cause of the error. Restart the session management server application to retry the configuration process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0642E Activation of the session management server configuration MBean failed: *%s*

Explanation: Activation of the session management server configuration MBean failed.

Administrator response: Examine the error message to determine the cause of the error. It may be necessary to restart the WebSphere application server deployment manager to correct the problem.

CTGSM0644E The session management server configuration application could not create a new WebSphere application server SSL configuration: *%s*

Explanation: The session management server could not create a new WebSphere application server SSL configuration.

Administrator response: Examine the error message to determine the cause of the error. Run the session management server configuration program again to retry the operation. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0645E The session management server configuration application could not remove the WebSphere application server SSL configuration, *%s*: *%s*

Explanation: The session management server configuration application could not remove the WebSphere application server SSL configuration.

Administrator response: Examine the error message to determine the cause of the error. Attempt to remove the SSL configuration manually through the WebSphere application server administration console. Run the session management server configuration program again to retry the operation. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0648E Failed to access the WebSphere application server configuration service.

Explanation: The session management server could not access the WebSphere application server configuration service in order to complete its configuration.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0649E Failed to locate the WebSphere application server security configuration.

Explanation: The session management server could not locate the WebSphere application server security configuration in order to complete its configuration.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0651W An error occurred while parsing the WebSphere application server configuration: *%s*

Explanation: An error occurred while parsing the WebSphere application server configuration. The logging for the Session management server may not function correctly until the problem is resolved.

Administrator response: The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0652E An error occurred while retrieving the list of applications installed on the WebSphere application server: *%s*

Explanation: An error occurred while retrieving the list of applications installed on the WebSphere application server. The session management server configuration application will not function correctly until the problem is resolved.

Administrator response: The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0653E An error occurred while parsing the configuration of the application, *%s*: *%s*

Explanation: An error occurred while parsing the configuration of the named application. The session management server configuration application will not function correctly until the problem is resolved.

Administrator response: The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message.

CTGSM0654E An error occurred while attempting to restart the application, *%s*: *%s*

Explanation: An error occurred while attempting to restart the named application.

Administrator response: The message shown describes the error condition that occurred. Take the appropriate corrective action based on the details contained within the message. The session management server configuration process will not proceed until the session management server application is restarted. If the session management server application is restarted manually, the configuration process will proceed, but the results will not be reported to the configuration program.

CTGSM0659E The deployment descriptor for the session management server application could not be located.

Explanation: The deployment descriptor for the session management server application could not be located.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0663E The session management server was not able to create an instance of the class *%s***.**

Explanation: The session management server encountered an error while trying to instantiate the class.

Administrator response: Examine the log for earlier messages indicating why the class could not be instantiated. Check the class name is correct, and the Java security policy allows the session management server to instantiate the class, then restart the application. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0666E The specified configuration session is not active.

Explanation: The specified configuration session is not active. This may mean that the target session management server instance has been restarted, or that the configuration session has been displaced by a newer session.

Administrator response: Retry the configuration action.

CTGSM0667E The session management server was not able to lock the distributed configuration: *%s*

Explanation: Before updating its configuration, the session management server first locks the configuration to protect against concurrent updates. This failure may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response: Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0668E The session management server was not able to unlock the distributed configuration: *%s*

Explanation: Before updating its configuration, the session management server first locks the configuration to protect against concurrent updates. This failure may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response: Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0669E The session management server was not able to retrieve the configuration state from other instances in the cluster: *%s*

Explanation: This may indicate there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response: Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error.

CTGSM0670E The session management server was not able to distribute the updated configuration across the cluster: *%s*

Explanation: The session management server was not able to distribute the updated configuration to other instances in the cluster. This may indicate that there are communication problems between the WebSphere application servers hosting the session management server. Unless this problem is corrected, future configuration operations may operate on an outdated version of the configuration.

Administrator response: Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error. It may be necessary to restart the application server instance that logged this message.

CTGSM0671E The session management server was not able to distribute configuration result information across the cluster: *%s*

Explanation: The session management server was not able to distribute the updated configuration to other instances in the cluster. This may indicate that there are communication problems between the WebSphere application servers hosting the session management server.

Administrator response: Examine the detailed error message and previous entries in the WebSphere application server logs for more information about the error. It may be necessary to restart the application server instance that logged this message.

CTGSM0672E The new configuration is based on a previous version of the configuration. The current configuration is version *%d* and the new configuration is version *%d*.

Explanation: An update to the session management server configuration has a version number older than or equal to that of the current configuration.

Administrator response: Retry the configuration operation.

CTGSM0673E A component with the name *%s* already exists in the *%s* component set.

Explanation: An attempt was made to add a component to a set using a name already present in that component set.

Administrator response: Retry the operation using a different name for the component.

CTGSM0674E The component *%s* from component set *%s* failed to initialize: *%s*

Explanation: An SMS component failed to initialize. The component will not be available until the problem is fixed. This may make the session management server unavailable until the problem is fixed.

Administrator response: Examine the error message for details of the failure. It may be necessary to reconfigure or restart the session management server.

CTGSM0675E The component *%s* was not found in the component set *%s*.

Explanation: The specified component does not exist in the configuration.

Administrator response: Check the component name and retry the configuration operation.

CTGSM0676E An unknown configuration component set identifier, *%d*, was specified.

Explanation: The configuration component set specified does not match any of the known component sets.

Administrator response: Check the component set identifier and retry the configuration operation.

CTGSM0677E The session realm, *%s*, cannot be removed because it still contains replica sets.

Explanation: Session realms cannot be removed while they still contain replica sets.

Administrator response: Remove the replica sets that are still in the session realm before removing the session realm.

CTGSM0678E An unknown session realm name, *%s*, is specified in the configuration for the replica set, *%s*.

Explanation: The configuration for the replica set specifies a session realm name that does not match any configured session realm.

Administrator response: Check the session realm name for the replica set. Either create a session realm matching the name specified in the replica set configuration or change the replica set configuration to match an existing session realm. The replica set will not be available until the problem is corrected.

CTGSM0679E An attempt to process an SMS event failed: *%s*.

Explanation: The session management server encountered an error while trying to process an event.

Administrator response: Examine the log for other messages relating to this error, and take any necessary corrective action. If the problem persists, restart the session management server.

CTGSM0750E The SecureRandom algorithm, *%s*, could not be loaded: *%s*

Explanation: The SecureRandom algorithm specified in the session management server configuration could not be loaded.

Administrator response: Verify the SecureRandom algorithm specified in the session management server configuration is correct, and restart the application.

CTGSM0751E The SecureRandom provider, *%s*, was not found: *%s*

Explanation: The SecureRandom provider specified in the session management server configuration could not be found.

Administrator response: Verify the SecureRandom provider specified in the session management server configuration is correct, and restart the application.

CTGSM0752E The session management server was unable to determine the current key details.

Explanation: The session management server was unable to determine the current key details. The key information may have become corrupted.

Administrator response: Request a change of key using the administration interface. If the problem persists, restart the session management server.

CTGSM0753E The session management server was unable to find the key with ID: *%s***.**

Explanation: The session management server was unable to find the key. The key information may have become corrupted.

Administrator response: Request a change of key using the administration interface. If the problem persists, restart the session management server.

CTGSM0754E An error occurred while updating the key distribution information. The parameter, *%s***, could not be associated with the value:** *%s***.**

Explanation: While updating the key distribution information, the session management server encountered an error.

Administrator response: Examine the log for other messages relating to this error, and take any necessary corrective action. Request a key change using the administration interface. If the problem persists, restart the session management server.

CTGSM0755W An error occurred while updating the key distribution information. The expired key, *%s***, could not be removed.**

Explanation: While updating the key distribution information, the session management server encountered an error. This condition does not effect the operation of the session management server, but it may indicate future errors.

Administrator response: Examine the log for other messages relating to this error, and take any necessary corrective action. Unless the other messages indicate a serious problem, it is not necessary to request a new key or restart the session management server.

CTGSM0901E The session management server was not able to initialize the IBM Security Access Manager Runtime for Java: *%s*

Explanation: The session management server must initialize the IBM Security Access Manager Runtime for Java. This message indicates the initialization failed

Administrator response: Examine this and earlier log messages for information regarding the error and take any necessary corrective action. Verify the IBM Security Access Manager Runtime for Java configuration URL is specified correctly. The session management server application must be restarted.

CTGSM0902W An error occurred while accessing a IBM Security Access Manager credential: *%s*

Explanation: An error occurred while accessing a IBM Security Access Manager credential.

Administrator response: Examine the error message for specific details of the error. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0903W The session, *%s***, does not contain a IBM Security Access Manager credential.**

Explanation: The identified session does not contain a IBM Security Access Manager credential. All authenticated sessions stored in the session management server must contain a credential.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0904E A configuration value required to configure the IBM Security Access Manager Runtime for Java is missing: *%s***.**

Explanation: One of the configuration values required to configure the IBM Security Access Manager Runtime for Java is missing.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM0905E Configuration of the IBM Security Access Manager Runtime for Java failed: *%s*

Explanation: Configuration of the IBM Security Access Manager Runtime for Java has failed.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. Verify that the IBM Security Access Manager policy server and the user registry server are available. The session management server application must be restarted.

CTGSM0906E Unconfiguration of the IBM Security Access Manager Runtime for Java failed: *%s*

Explanation: Unconfiguration of the IBM Security Access Manager Runtime for Java has failed.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. Verify that the IBM Security Access Manager policy server and the user registry server are available. The session management server application must be restarted.

CTGSM0907E An error was encountered while creating the key and trust store files used to authenticate clients of the session management server: *%s*

Explanation: An error was encountered while creating the key and trust store files used to authenticate clients of the session management server.

Administrator response: Examine the error message for information regarding the error and take any necessary corrective action. Verify that the necessary Java security providers are available. The session management server application must be restarted.

CTGSM0908E IBM Security Access Manager integration has not been enabled for the session management server.

Explanation: A Security Access Manager configuration operation was requested, but Security Access Manager integration has not been enabled.

Administrator response: Enable Security Access Manager integration before attempting further Security Access Manager configuration.

CTGSM0909E The IBM Security Access Manager Runtime for Java is not currently available.

Explanation: The IBM Security Access Manager Runtime for Java is not currently available.

Administrator response: Examine earlier log messages to determine the cause of the problem. This may indicate a problem with the IBM Security Access Manager policy server. The session management server may need to be restarted.

CTGSM0910W The session, *%s***, does not contain a user UUID.**

Explanation: The identified session does not contain a user UUID. This information is required for the recording of last login information. The information should be supplied either as session data, or as a part of a IBM Security Access Manager credential.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1050E Multiple values for the *%s* **attribute of the** *%s* **session management server administration interface request were specified but no more than one value may be specified.**

Explanation: The client sent multiple values for the indicated request attribute but the attribute may only have a single value.

Administrator response: Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1051E The *%s* **attribute of the** *%s* **session management server administration interface request must be an integer value - the** *%s* **value cannot be parsed as an integer.**

Explanation: The specified request attribute must be an integer but the value provided by the client cannot be parsed as an integer value.

Administrator response: Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1052E The *%s* **attribute of the** *%s* **session management server administration interface request has a lower bound of** *%s* **- the value** *%s* **is too low.**

Explanation: The client specified a value for the specified request attribute that is less than the identified attribute's minimum valid value.

Administrator response: Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1053E The *%s* **attribute of the** *%s* **session management server administration interface request has an upper bound of** *%s* **- the value** *%s* **is too high.**

Explanation: The client specified a value for the specified request attribute that is greater than the identified attribute's maximum valid value.

Administrator response: Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1054E The required *%s* attribute of the *%s* session management server administration interface request was not provided by the client.

Explanation: A required request attribute was not sent by the session management server administration interface client.

Administrator response: Ensure the version of the client software in use is supported by this version of the session management server.

CTGSM1055E The value (*%s*) of the *%s* attribute of the *%s* session management server administration interface request could not be processed. Error: *%s*.

Explanation: The indicated value of the indicated attribute is not valid when specified as part of the indicated session management server administration interface request.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1059E The session realm *%s* specified in a *%s* request of the session management server's administration interface is not recognized by the session management server.

Explanation: The request from the client specified an undefined session realm name.

Administrator response: Retry the operation specifying a defined session realm name.

CTGSM1060E The *%s* request failed with error: *%s*

Explanation: The request from the client could not be executed.

Administrator response: Examine the log for further detailed messages regarding the error and take any necessary corrective action.

CTGSM1061E The *%s* request caused an exception: *%s*Exception stack trace:*%s*

Explanation: The request from the client caused the indicated exception.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1062E No HTTP request for administration service authorization.

Explanation: The HTTP request object could not be accessed while authorizing an administration service operation.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1063E The user *%s* is not permitted to delegate access to the administration service.

Explanation: The identified user is not permitted to delegate access to the administration service.

Administrator response: If the identified user is expected to be able to delegate access to the administration service ensure they have the sms-delegator role.

CTGSM1064E Unable to authorize access for the *%s* operation requiring the *%s* role for user *%s* delegated by user *%s*.

Explanation: Authorization of a user for this operation has failed. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

Administrator response: Examine the log containing this message for more information describing the error that occurred and take the appropriate corrective action.

CTGSM1065E Authorization of user *%s* for role *%s* failed. *%s* exception: *%s*

Explanation: The specified exception occurred while attempting to authorize the user for the role.

Administrator response: The message shown describes the error condition that occurred. Take the appropriate corrective action.

CTGSM1066E The administration request type, *%s*, cannot be handled by class, *%s*, as specified by handler, *%s*, as it is already configured to be handled by the class, *%s*.

Explanation: The session management server administration requests may only be configured to be handled by one handler. This message indicates that a single request type is configured to be handled by more than one handler.

Administrator response: Ensure the session management server administration request handlers are configured correctly and restart the application.

CTGSM1067E Failed to locate the DSessAdmin request dispatcher.

Explanation: The request from the client could not be executed.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1363E Validation of the last login information database table failed.

Explanation: The last login information database table has not been correctly created.

Administrator response: Refer to earlier log messages regarding the creation of the last login information database table. Check that the table exists in the database. It may be necessary to modify the table manually to allow the table validation to succeed.

CTGSM1369E An error occurred while installing a component into the WebSphere application server runtime. The file, *%s*, **could not be copied to the target location,** *%s*.

Explanation: An error occurred while installing a component into the WebSphere application server runtime.

Administrator response: Check that the permissions on the target directory permit the file to be copied and that there is sufficient disk space. The file may also be copied into place manually. Restart the session management server application.

CTGSM1500W The host name of this machine could not be determined.

Explanation: The host name of the machine on which the session management server is running could not be determined.

Administrator response: Check that the system host name and network devices have been configured correctly. Restart the session management server application.

CTGSM1501E User information is required to report an audit event but no session information is available.

Explanation: User information is required to report an audit event but no session information is available.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1505W The session creation time, *%s*, **is in the future. Check time synchronization between SMS and client** *%s*.

Explanation: The session creation timestamp associated with the session being terminated is later than the current time. This indicates clock skew between the SMS and the client that created the session.

Administrator response: Synchronize the clocks of the SMS system and its clients and restart the SMS.

CTGSM1506E The auditing emitter configuration has been set to debug mode. Events will not be sent to a CARS emitter, they will be written to the log file.

Explanation: The auditing emitter configuration has been set to debug mode. Events will not be sent to a CARS emitter, they will be written to the log file.

Administrator response: No action is necessary.

CTGSM1507E The CARS Security Event Factory reported an error while constructing an event: *%s*

Explanation: The common audit reporting service (CARS) Security Event Factory reported an error while constructing an event for the reported reason.

Administrator response: Examine the reason for the failure and take any necessary corrective action.

CTGSM1509E The CARS emitter reported an error while sending an event: *%s*

Explanation: The common audit reporting service (CARS) emitter reported an error while sending an event for the reported reason.

Administrator response: Examine the reason for the failure and take any necessary corrective action.

CTGSM1514E The common audit and reporting service (CARS) encountered a severe error when initializing: Error: *%s*, **cause:** *%s***Error stack trace:***%s***Cause stack trace:***%s*

Explanation: The common audit and reporting service (CARS) encountered a severe error when initializing.

Administrator response: Examine the reason for the failure and take any necessary corrective action.

CTGSM1515E The common auditing service encountered a severe error when shutting down: Error: *%s*, **cause:** *%s***Error stack trace:***%s***Cause stack trace:***%s*

Explanation: The common auditing service encountered a severe error when shutting down.

Administrator response: No action is necessary.

CTGSM1654E The command line option, *%s*, **is not recognized.**

Explanation: The identified command line option of the smsbackup command is not recognized by the smsbackup command.

Administrator response: Re-run the smsbackup command with correct command line options.

CTGSM1655E The *%s* **command line option requires an argument.**

Explanation: The identified smsbackup command line option requires an argument.

Administrator response: Consult the documentation for the smsbackup command and re-run it specifying a valid argument for the option.

CTGSM1656E The argument to the -list option must be a readable file. The value provided, *%s*, **is not a readable file.**

Explanation: The value provided for the -list option of the smsbackup command does not identify a readable file.

Administrator response: Re-run the smsbackup command specifying a valid value for the -list option.

CTGSM1657E The file, *%s*, **could not be opened:** *%s*

Explanation: The identified file could not be opened for the specified reason.

Administrator response: Ensure that the name of the file is correct, that it exists and is that it is readable.

CTGSM1658W Line *%s* **of the list file** *%s*, *%s*, **cannot be interpreted.**

Explanation: Not all of the contents of the file specified by the -list option could be interpreted correctly.

Administrator response: Ensure the list file name is specified correctly and that the contents of the file are not corrupt.

CTGSM1659E The file, *%s*, **could not be backed up:** *%s*

Explanation: The file was indicated to be backed up by the list file and does exist but could not be backed for the reason indicated by the exception shown.

Administrator response: Ensure that all files required to be backed up are accessible to the smsbackup program.

CTGSM1660E The command, *%s*, **could not be executed:** *%s*

Explanation: The command was indicated to be executed by the list file but execution failed for the reason indicated by the exception shown.

Administrator response: Ensure that all programs required to be executed are accessible to the smsbackup program.

CTGSM1662E The directory, *%s*, **could not be created:** *%s*

Explanation: The directory specified as the output path does not exist and could not be created.

Administrator response: Re-run the smsbackup command specifying a different value for -path option or ensuring that you have permission to create the specified directory.

CTGSM1663E An error occurred writing to the file, *%s*: *%s*

Explanation: The file specified could not be written to for the reason indicated.

Administrator response: Ensure that the file system containing the file has sufficient space and that the directory containing the file may be written to.

CTGSM1800E The property, *%s*, **which is required to configure the Java client API is missing.**

Explanation: One of the configuration values required to configure the Java client API is missing.

Administrator response: Add the property to the supplied properties object.

CTGSM1801E A configuration value required to configure the Java client API is missing: *%s***.**

Explanation: The specified configuration item has not been supplied to the DSessClientConfig class.

Administrator response: Ensure that the specified configuration item is passed into the DSessClientConfig class.

CTGSM1802E The session management interface of any configured session management server could not be accessed.

Explanation: An unsuccessful attempt has been made to communicate with the session management interface of each configured session management server.

Administrator response: Ensure the session management interface of at least one configured session management server is available and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1803E An internal error occurred within the Java client API: *%s***.**

Explanation: An internal error occurred within the Java client API.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1804E The MAC algorithm, *%s***, could not be loaded:** *%s*

Explanation: The MAC algorithm which is used for Session ID generation and validation could not be loaded.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1805E The provided session ID, *%s***, is invalid.**

Explanation: The session ID that was provided to the Java client API failed the cyrpographic check which is used to validate ID's.

Administrator response: The client of the API should disregard the locally cached session and should return an error back to the client.

CTGSM1806E The provided session ID, *%s***, was incorrectly formatted.**

Explanation: The session ID that was provided to the Java client API was of an incorrect format.

Administrator response: The client of the API should disregard the locally cached session and should return an error back to the client.

CTGSM1807E A request was made to send a session which contained no data to the SMS.

Explanation: The session which was to be sent to the SMS contains no session data.

Administrator response: The client of the API should not be sending any empty sessions to the SMS. A review of the client code should be conducted.

CTGSM1950E An exception occurred while performing a WebSphere eXtreme Scale data replication operation: *%s*

Explanation: An exception occurred while performing a WebSphere eXtreme Scale data replication operation.

Administrator response: Examine the details of the WebSphere eXtreme Scale error to determine the cause and take appropriate action. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1951E The session management server was unable to initialize the WebSphere eXtreme Scale data replication service.

Explanation: The session management server was unable to initialize the WebSphere eXtreme Scale data replication service.

Administrator response: Examine previous log messages for more details of the underlying cause of the failure. Once the underlying problem has been corrected, restart the application server.

CTGSM1952E Initialization of the WebSphere eXtreme Scale data replication service failed: *%s*

Explanation: Initialization of the WebSphere eXtreme Scale data replication service failed. The session management server will not function until this problem is corrected.

Administrator response: Examine the details of the WebSphere eXtreme Scale error to determine the cause. Once the underlying problem has been corrected, restart the application server. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

CTGSM1954E An exception occurred during a remote WebSphere eXtreme Scale operation on server *%s***:** *%s*

Explanation: An exception occurred during a WebSphere eXtreme Scale operation on a remote server.

Administrator response: Examine the details of this message and the logs on the named server for more information on the cause of the problem and take any appropriate action.

DPWAD0309E The WebSEAL administration service has not been initalized.

Explanation: The WebSEAL administration service plug-in failed to initialize properly.

Administrator response: Check for other initialization errors and/or configuration problems that may have previously occurred.

DPWAD0312E Object list failed: *%s*

Explanation: The object list command failed to complete correctly.

Administrator response: This is a generic error which will contain further details when output.

DPWAD0328E The junction import command received invalid data

Explanation: An error occurred when trying to extract one or more of the junction attributes sent in the admin command.

Administrator response: Check that the data being passed into the junction import command is valid.

DPWAD0329E The junction import command received an invalid version

Explanation: The version in the junction definition is not supported by this version of WebSEAL

Administrator response: Check the version of the junction in the XML definition

DPWAD0330E The junction import could not create the junction file

Explanation: WebSEAL can not create the junction file.

Administrator response: Check the filesystem to make sure there is space available, or that the WebSEAL server has permissions to create/write the file.

DPWAD0331E The junction import could not write the junction file

Explanation: An error occurred writing the junction definition.

Administrator response: Check the filesystem to make sure there is space available, or that the WebSEAL server has permissions to create/write the file.

DPWAD0332E The junction export could not read the junction directory

Explanation: An error occurred while trying to read the contents of the junction database directory.

Administrator response: Check to make sure that WebSEAL is able to read the contents of the directory which is configured to contain the junction definitions.

DPWAD0333E Unable to add junction attributes into command handler

Explanation: An error occurred returning the junction data to the client

Administrator response: This is an internal error which occurs when WebSEAL is marshalling the junction data to the export command. Check for other errors occurring previously.

DPWAD0334E An invalid junction point was specified.

Explanation: WebSEAL was unable to build the junction filename.

Administrator response: An internal error occurred in WebSEAL when trying to build the encoded filename. Check for previous errors.

DPWAD0335E Error reading junction point *%s*.

Explanation: The file name representing the junction could not constructed.

Administrator response: An internal error occurred in WebSEAL when trying to build the encoded filename. Check for previous errors.

DPWAD0336E Error reading junction file *%s*.

Explanation: There was an error opening or parsing the junction definition file.

Administrator response: Verify the .xml file exists, is readable, and has valid data.

DPWAD0342E Error reading input user session id.

Explanation: There was an error parsing the user session id.

Administrator response: Verify that the input is being passed correctly.

DPWAD0343E Error reading input user id.

Explanation: There was an error parsing the user ID.

Administrator response: Verify that user ID is being input correctly.

DPWAD0345E No matching User Session found.

Explanation: Bad input, or User session was already terminated.

Administrator response: Verify validity of input, or assume session was already terminated.

DPWAD0362E The dynurl configuration file *%s* **cannot be opened for reading.**

Explanation: An attempt to open the dynurl configuration file for reading failed

Administrator response: Ensure that the file exists on the WebSEAL server and is readable

DPWAD0363E The jmt configuration file *%s* **cannot be opened for reading.**

Explanation: An attempt to open the jmt configuration file for reading failed

Administrator response: Ensure that the file exists on the WebSEAL server and is readable

DPWAD0364E You must specify a junction point to read or write an fsso configuration file.

Explanation: A junction point is necessary to determine which fsso configuration file to read or write

Administrator response: Add the junction point to the junction attribute of the indata attribute list

DPWAD0365E The junction: *%s* **is not a valid junction on this WebSEAL server.**

Explanation: An invalid junction point was provided.

Administrator response: Ensure that the junction attribute in indata is a valid junction

DPWAD0366E The junction: *%s* **is not an fsso junction on this WebSEAL server.**

Explanation: The junction specified is not an FSSO junction.

Administrator response: Ensure that the junction specified is an FSSO junction.

DPWAD0367E The fsso configuration file: *%s* **could not be opened for reading.**

Explanation: The junction specified could not be opened.

Administrator response: Ensure that the fsso configuration file for the junction specified exists and is readable.

DPWAD0368E Could not create dynurl configuration file: *%s*

Explanation: WebSEAL was unable to create the dynurl conf file.

Administrator response: Ensure that ivmgr has filesystem permissions to create a file in the directory where the dynurl configuration file will be stored

DPWAD0369E Reloading the in memory dynurl table failed

Explanation: An error occurred while trying to read the dynurl configuration file.

Administrator response: Ensure that the new file specified is in the proper format

DPWAD0370E Could not create jmt configuration file: *%s*

Explanation: An error occured while trying to open the jmt configuration file.

Administrator response: Ensure that ivmgr has filesystem permissions to create a file in the directory where the jmt configuration file will be stored

DPWAD0371E Reloading the in memory jmt table failed

Explanation: An error occurred while trying to read in the new jmt configuration file.

Administrator response: Ensure that the new file specified is in the proper format.

DPWAD0372W The junction specified does not exist. The configuration file: *%s* **was created.**

Explanation: An fsso junction may not be created without the configuration file being inplace. This allows the file to be created before the junction

Administrator response: The junction may now be created using this new configuration file

DPWAD0373E Could not create fsso configuration file: *%s*

Explanation: An error occurred while trying to read in the new fsso configuration file.

Administrator response: Ensure that ivmgr has filesystem permissions to create a file in the directory where the fsso configuration file will be stored

DPWAD0374E The backup operation failed for *%s*

Explanation: An error occurred while attempting to create a backup copy of the original configuration file.

Administrator response: Ensure that ivmgr has filesystem permissions to create a file in the directory where the configuration file resides.

DPWAD0375E Reloading junction: *%s* **failed**

Explanation: An error occurred while trying to load the fsso configuration file.

Administrator response: Ensure that the new file specified is in the proper format.

DPWAD0376E The restore operation failed for *%s*

Explanation: An error occurred while trying to restore a backed up version of a configuration file.

Administrator response: Ensure that ivmgr has filesystem permissions to create a file in the directory where the configuration file resides.

DPWAD0386E Failed to open the supplied junction archive file.

Explanation: An error occurred when trying to access a junction archive file.

Administrator response: Ensure that the specified file name is correct and that the WebSEAL server can access the file.

DPWAD0387E The supplied junction archive file contains an invalid junction definition.

Explanation: An error occurred while trying to access a junction archive file.

Administrator response: Ensure that the supplied file is correctly formatted.

DPWAD0391W Failed to execute the program (*%s***). (Errno =** *%d***).**

Explanation: An error occurred when attempting to run the specified program.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD0394W The requested file segment contained binary characters.

Explanation: A request to display a binary file was submitted. A binary file can be displayed only if the '-encode' option is supplied.

Administrator response: Ensure that the correct file has been requested and if so that the '-encode' option is supplied to the command.

DPWAD0404E Failed to locate the authorization server password, required for the server sync command.

Explanation: The server sync command is not available because the authorization server password could not be determined.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0405E Failed to synchronize the WebSEAL server.

Explanation: The server sync command did not complete successfully.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0406E The server name supplied was not valid.

Explanation: The server name supplied to the server sync command was not valid.

Administrator response: Ensure that a valid server name is supplied with the server sync command. The server name must not be the same as the name of the server that runs the command.

DPWAD0411E The TCP/IP host information could not be determined from the server hostname: *%s***. Ensure that the server hostname is correct and that the domain name server is functioning correctly.**

Explanation: The TCP/IP address for the specified host could not be determined.

Administrator response: Ensure that the IP address for the specified host name can be resolved. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD0412E The configuration entry found within the *%s* **stanza was not valid:** *%s* **=** *%s***.**

Explanation: The specified configuration entry contained a value that must be corrected.

Administrator response: Correct the configuration entry which is not valid.

DPWAD0413E An attempt to create a temporary file failed.

Explanation: An attempt was made to create a temporary file and the file could not be created.

Administrator response: Check the log file for additional errors. Also check the file system to ensure that there is adequate disk space available.

DPWAD0415E An ICAP Server for the '*%s*' resource was not found.

Explanation: An unknown ICAP resource was specified.

Administrator response: Check the ICAP configuration within both the WebSEAL configuration file and the policy database.

DPWAD0416E An ICAP Server for the specified resource was not found.

Explanation: An unknown ICAP resource was specified.

Administrator response: Check the log file for additional errors.

DPWAD0417E A bad response was received from the ICAP server.

Explanation: The response which was received from the ICAP server was incorrectly formatted.

Administrator response: Check the configuration of the ICAP server.

DPWAD0418E Failed to connect to the ICAP server: *%s*.

Explanation: An attempt to contact an ICAP server failed. The ICAP server is required to be able to correctly service the Web request.

Administrator response: Ensure that the configuration for the ICAP server is correct and that the ICAP server is available. Check the log file for additional errors.

DPWAD0419E Failed to connect to a required ICAP server.

Explanation: An attempt to contact an ICAP server failed. The ICAP server is required to be able to correctly service the Web request.

Administrator response: Ensure that the configuration for the ICAP server is correct and that the ICAP server is available. Check the log file for additional errors.

DPWAD0420E The maximum number of concurrent requests which can be processed for this session has been reached.

Explanation: The user session has reached the maximum number of simultaneous requests which can be processed by WebSEAL.

Administrator response: Either increase the configured maximum number of requests which can be processed by a session, or wait for existing requests for the user session to complete.

DPWAD0421W The session, owned by *%s*, has reached it's soft limit of *%d* concurrent requests.

Explanation: The user session has reached the warning point for the number of simultaneous requests which can be processed by WebSEAL.

Administrator response: Prepare to increase the hard limit of concurrent requests for a user session, or wait for existing requests for the user session to complete.

DPWAD0431E Failed to locate the authorization server password, required for the cluster functionality.

Explanation: The cluster support is not available because the authorization server password could not be determined.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0432E Failed to execute the server task '*%s*' on *%s*: *%s*

Explanation: An attempt to execute a server task command failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0433E Failed to execute a server task command

Explanation: An attempt to execute a server task command failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0434E Failed to create the administration context for *%s***:** *%s*

Explanation: An attempt to create an administration context failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0435E Failed to create an administration context

Explanation: An attempt to create an administration context failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0436E An unexpected result was received from the server task command: *%s* **(***%s***)**

Explanation: An unexpected result was received from the server task command.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0438E Failed to synchronize with the cluster master

Explanation: An attempt to synchronize the local configuration with the cluster master server failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0439E Failed to restart the cluster

Explanation: An attempt to restart the cluster failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0440E Failed to restart the cluster: 0x*%lx*

Explanation: An attempt to restart the cluster failed.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0441E Failed to restart the cluster as a cluster restart is already in progress

Explanation: An attempt to restart the cluster failed as a prior request to restart the cluster is still in progress.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0442E The server, *%s***, failed to restart within a reasonable period of time.**

Explanation: The specified server did not restart within the allocated period of time. This restart was performed as a part of the cluster synchronisation.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0445E *%s*

Explanation: An unspecified error has occurred.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD0446E Both the '-ripple' and '-status' options cannot be specified at the same time.

Explanation: The cluster restart command cannot have both the '-ripple' and '-status' options specified in the same command.

Administrator response: Re-issue the command with either of the options, but not both.

DPWAD0447E The server is not fully initialized.

Explanation: An attempt to access the server failed due to the fact that it is not fully initialized. This can occur during server start-up or shutdown.

Administrator response: Allow extra time for the server to finish initialization and then retry the operation. If the problem persists check the log file for additional errors.

DPWAD0448E The new user identity (*%s*) does not match the current authenticated user identity (*%s*).

Explanation: The identity which is provided in a subsequent authentication operation must match the identity which was used during the original authentication operation.

Administrator response: The user must present the same user ID provided in the previous authentication operation.

DPWAD0449E The new user identity does not match the current authenticated user identity.

Explanation: The identity which is provided in a subsequent authentication operation must match the identity which was used during the original authentication operation.

Administrator response: The user must present the same user ID provided in the previous authentication operation.

DPWAD0452E eCSSO authentication is enabled but no Master Authorization Server is defined.

Explanation: The e-community-sso-auth has been set without setting a master authorization server.

Administrator response: Update the configuration file and set a master authorization server in the master-authn-server value under the [e-community-sso] stanza.

DPWAD0453E Duplicate eCSSO domain '*%s*' defined under the [e-community-domains] stanza.

Explanation: Each domain under the [e-community-domains] stanza must be unique.

Administrator response: Remove the duplicate entry and retry.

DPWAD0454E Unable to configure the eCSSO authentication module for domain/host '*%s*': status 0x*%lx*.

Explanation: The eCSSO (consume or create) authentication module configured for the domain/host specified returned an error while being initialised.

Administrator response: Either a bad shared library was specified for the authentication module or the configuration is incorrect, for example the key files specified are missing or inaccessible.

DPWAD0455E The value '*%s*' is not a valid option for ip-support-level. Use one of 'displaced-only', 'generic-only', or 'displaced-and-generic'.

Explanation: An invalid setting was set for the webseald configuration file option ip-support-level.

Administrator response: Change the setting for ip-support-level to a valid one.

DPWAD0456E The value displaced-only is not a valid option for ip-support-level when ipv6-support is enabled.

Explanation: displaced-only can not be set when ipv6-support = yes.

Administrator response: Change the setting for ip-support-level to generic-only or displaced-and-generic.

DPWAD0457E The authentication challenge type specified is not valid: *%s*

Explanation: The challenge type string located in the WebSEAL configuration file was not valid.

Administrator response: Change the setting for auth-challenge-type to be a valid challenge type.

DPWAD0458E The corresponding authentication method for the challenge type, *%s*, is not enabled.

Explanation: The corresponding authentication method for the specified challenge type is not enabled.

Administrator response: Either remove the failing challenge type from the auth-challenge-type configuration entry, or enable the corresponding authentication method.

DPWAD0459E The authentication challenge type contains multiple entries for *%s*.

Explanation: The challenge type string located in the WebSEAL configuration file contains multiple rule sets for a single mechanism.

Administrator response: Remove the duplicate entries in the auth-challenge-type configuration entry.

DPWAD0460E The following authentication challenge type contains a syntax error or invalid pattern.*%s*

Explanation: The challenge type string located in the WebSEAL configuration file contains a syntax error.

Administrator response: Correct the syntax error for the auth-challenge-type configuration entry.

DPWAD0600E An error occurred attempting to determine the current installed version of WebSEAL. WebSEAL cannot start.

Explanation: This error occurs if the current installed version of WebSEAL cannot be determined. This indicates a severe problem.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD0601E The version string '*%s*' is invalid.

Explanation: This error occurs if an invalid version number is found.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD0602E An error occurred attempting to determine the originally installed version of WebSEAL to verify that the configuration file is up-to-date. WebSEAL cannot start.

Explanation: This error occurs if the originally installed version of WebSEAL cannot be determined. This indicates a severe problem.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD0603E An error occurred attempting to backup the configuration file.

Explanation: This error occurs when WebSEAL is trying to make a backup copy of the original configuration file before upgrade.

Administrator response: Examine the log file for additional errors. More information about the problem that occurred will be present.

DPWAD0604E An error occurred attempting to restore the configuration file.

Explanation: This error occurs when WebSEAL is trying to restore a backed up copy of the configuration file.

Administrator response: Examine the log file for additional errors. More information about the problem that occurred will be present.

DPWAD0605W The configuration file entry [*%s*]*%s* was not found.

Explanation: This error occurs when WebSEAL is trying to determine the version of the WebSEAL server that created the configuration file.

Administrator response: No action is necessary - the WebSEAL server will try another method to determine the original version of WebSEAL installed, and update the configuration file as necessary.

DPWAD0606E An error occurred attempting to migrate the configuration file entry [*%s*]*%s*.

Explanation: This error occurs when WebSEAL is trying to perform migration of a configuration file entry.

Administrator response: You may need to manually update the entry to allow migration to proceed. Examine the configuration file and documentation for more information on the particular entry.

DPWAD0607E An error occurred attempting to migrate the configuration file entry [*%s*].

Explanation: This error occurs when WebSEAL is trying to perform migration of a configuration file stanza.

Administrator response: You may need to manually update the entry to allow migration to proceed. Examine the configuration file and documentation for more information on the particular entry.

DPWAD0611E A serious error occurred performing configuration file migration. You may need to perform manual migration of some configuration options.

Explanation: This message indicates that a serious problem occurred while attempting to update the configuration file.

Administrator response: Refer to other log messages to attempt to determine the problem. You may be able to perform manual migration of configuration file entries. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman. If you wish to attempt to manual migration, comment the problematic entries out of the WebSEAL configuration file and restart the WebSEAL server. Once the WebSEAL server has started successfully, manually modify the configuration file to restore the functionality you have disabled, refering to the WebSEAL Administration Guide where necessary.

DPWAD0752E A replica set must be specified for the virtual host junction '*%s*'.

Explanation: When the SMS is used for session storage, all virtual host junctions must have a replica set specified with the -z junction option.

Administrator response: Create the junction using the -z <replica-set> option. The <replica-set> must be one of the replica sets listed in the WebSEAL configuration file.

DPWAD0753E A replica set must be specified for the junction.

Explanation: When the SMS is used for session storage, all virtual host junctions must have a replica set specified with the -z junction option.

Administrator response: Create the junction using the -z <replica-set> option. The <replica-set> must be one of the replica sets listed in the WebSEAL configuration file.

DPWAD0754E The Virtual Host junction '*%s*' must have an eCSSO domain key in the configuation file for it's virtual host name '*%s*'.

Explanation: When the Virtual Host junction was created or restored from the junction database it's virtual host name was discovered not to have a eCSSO domain key. These are configured using [e-community-domains] and [e-community-domain-keys:<domain>]

Administrator response: Add a eCSSO key for the domain the Virtual Host junction is in using the [e-community-domains] and [e-community-domain-keys:<domain>] stanzas and restart WebSEAL so it recognises the changes. Then retry creating the Virtual Host junction.

DPWAD0755E The Virtual Host junction must have an eCSSO domain key in the configuration file for it's virtual host name.

Explanation: When the Virtual Host junction was created or restored from the junction database it's virtual host name was discovered not to have a eCSSO domain key. These are configured using [e-community-domains] and [e-community-domain-keys:<domain>]

Administrator response: Add a eCSSO key for the domain the Virtual Host junction is in using the [e-community-domains] and [e-community-domain-keys:<domain>] stanzas and restart WebSEAL so it recognises the changes. Then retry creating the Virtual Host junction.

DPWAD0756W The junction reload command did not complete for regular junctions as a previous reload is still in effect. Try again later.

Explanation: A reload command issued earlier is still waiting for some requests using the older junction definitions to complete. New reload commands will not have an effect until these requests complete. Virtual Host junctions are independent and you should look for a separate message if they are busy too.

Administrator response: The command has had no effect on junctions, retry the command at a later time.

DPWAD0757W The junction reload command did not complete for Virtual Host junctions as a previous reload is still in effect. Try again later.

Explanation: A reload command issued earlier is still waiting for some requests using the older Virtual Host junction definitions to complete. New reload commands will not have an effect until these requests complete. Regular junctions are independent and you should look for a separate message if they are busy too.

Administrator response: The command has had no effect on Virtual Host junctions, retry the command at a later time.

DPWAD0782E Could not take junction offline

Explanation: This message is followed by an explanation of why the junction could not be taken offline.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0783E Could not take Virtual Host junction offline

Explanation: This message is followed by an explanation of why the Virtual Host junction could not be taken offline.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0784E Could not throttle junction

Explanation: This message is followed by an explanation of why the junction could not be throttled.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0785E Could not throttle Virtual Host junction

Explanation: This message is followed by an explanation of why the Virtual Host junction could not be throttled.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0786E Could not bring junction online

Explanation: This message is followed by an explanation of why the junction could not be brought online.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0787E Could not bring Virtual Host junction online

Explanation: This message is followed by an explanation of why the Virtual Host junction could not be brought online.

Administrator response: Correct the problem described in the message displayed after this message.

DPWAD0788E You can only change the operation state of TCP, SSL, TCP Proxy, and SSL Proxy junctions.

Explanation: Not all junction types support operational state changes.

Administrator response: Ensure you are applying the command to the correct junction.

DPWAD0789E You can only change the operation state of TCP, SSL, TCP Proxy, and SSL Proxy Virtual Host junctions.

Explanation: Not all Virtual Host junction types support operational state changes.

Administrator response: Ensure you are applying the command to the correct Virtual Host junction.

DPWAD0790E Invalid server ID

Explanation: The argument passed to -i was not a valid server UUID.

Administrator response: Obtain the correct UUID by using the 'show' command.

DPWAD0791E Invalid server ID

Explanation: The argument passed to -i was not a valid server UUID.

Administrator response: Obtain the correct UUID by using the 'virtualhost show' command.

DPWAD0792E Server *%s* **not found at junction** *%s*

Explanation: An attempt was made to change the operational state of a junction server based on a UUID which did not match any of the servers of the junction.

Administrator response: Use the 'show' command to find the correct UUID.

DPWAD0793E Server *%s* **not found at Virtual Host junction** *%s*

Explanation: An attempt was made to change the operational state of a Virtual Host junction server based on a UUID which did not match any of the servers of the Virtual Host junction.

Administrator response: Use the 'virtualhost show' command to find the correct UUID.

DPWAD1050E The filename must not contain any path information.

Explanation: A base path for the database files has been statically configured and as such the supplied file name should not contain any path information.

Administrator response: Specify the name of the database without any path information.

DPWAD1053E An error occurred while writing the WebSEAL flow data to disk.

Explanation: An error occured while WebSEAL was committing the collected flow data to disk. One or more records may be missing for the last time period.

Administrator response: No action is required.

DPWAD1054E The *%s* **system routine failed:** *%d***.**

Explanation: An error occured when WebSEAL attempted to execute a system routine.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD1055E A system routine failed.

Explanation: An error occured when WebSEAL attempted to execute a system routine.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD1056E A process terminated unexpectedly: *%d***.**

Explanation: A process which was currently being monitored terminated unexpectedly. This process will be automatically restarted.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWAD1059E The validation of the secret token for the request failed.

Explanation: To help prevent cross-site request forgery attacks the requests for certain management pages need to contain a token which can be compared against data contained within the user session. The validation of this token failed because either the token was missing from the request, or the token did not match the value contained in the user session.

Administrator response: Ensure that the resource request contains the correct secret token for the user session.

DPWAD1060E Unsolicited authentication requests are not permitted.

Explanation: The server has been configured to deny unsolicited authentication requests. The authentication information must first be requested by WebSEAL in response to an unauthenticated request for a protected resource.

Administrator response: First request a resource which requires authentication and then supply the authentication information to the server.

DPWAD1200E The incoming connection from *%s* **has been blocked.**

Explanation: The incoming connection has been temporarily blocked by the Web Application Firewall functionality.

Administrator response: Check the log file for additional errors. For the error code from the message and additional troubleshooting steps, see the IBM Security Access Manager for Web Troubleshooting Guide.

DPWAD1201E An invalid csv field was provided: *%s*

Explanation: An invalid field was provided.

Administrator response: Examine the configuration and correct the offending field.

DPWAD1202E An invalid configuration value was provided: *%s*

Explanation: An invalid configuration value was provided.

Administrator response: Examine the configuration and correct the offending value.

DPWAD1203E An invalid number of fields were provided within the csv file: *%s*

Explanation: An invalid number of fields were discovered in a csv file.

Administrator response: Examine the configuration and correct the offending csv file.

DPWAD1204E An unknown issue was discovered, *%d***, and as such no action was taken.**

Explanation: An issue was discovered for which there was no configured action.

Administrator response: Examine the configuration and ensure that an action exists for the specified issue.

DPWAD1206E An incompatible ISS protocol analysis module library was found.

Explanation: An incompatible ISS protocol analysis module was specified within the WebSEAL configuration.

Administrator response: Install a compatible ISS protocol analysis module distribution, or disable this functionality within WebSEAL.

DPWAD1207E An internal error was encountered within the ISS protocol analysis module.

Explanation: An error was returned from the ISS protocol analysis module.

Administrator response: Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1208E An unrecoverable error was encountered within the ISS protocol analysis module : *%s***.**

Explanation: An error was returned from the ISS protocol analysis module.

Administrator response: Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1209E An insufficient amount of memory was supplied to an internal WAF routine.

Explanation: An insufficient amount of memory was supplied to one of the internal WAF routines.

Administrator response: Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1210E The client connection has been blocked due to a security attack which was detected by the protocol analysis module.

Explanation: The protocol analysis module detected a potential attack in a prior request from the client and as such has blocked all connections from this client for a period of time.

Administrator response: Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWAD1211E An error occurred while saving the WAF statistics data to the disk.

Explanation: An error occured while WebSEAL was saving the collected WAF statistics to the disk. One or more records might be missing for the last time period.

Administrator response: No action is required.

DPWCA0150E Invalid UNIX user name (*%s***)**

Explanation: See message.

Administrator response: Use a valid user name

DPWCA0151E Invalid UNIX group name (*%s***)**

Explanation: See message

Administrator response: Put user in a valid group.

DPWCA0152E Could not change process GID (*%s***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0153E Could not change process UID (*%s***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0154E Could not become background process (*%d***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0155W Could not start background process

Explanation: See message.

Administrator response: Contact support.

DPWCA0156E Could not use RPC protocol sequence (*%s***,***%s***,0x***%8.8lx***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0157E Could not fetch RPC bindings (0x*%8.8lx***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0158E Could not release RPC bindings (0x*%8.8lx***)**

Explanation: See message.

Administrator response: Contact Support.

DPWCA0159E Caught signal (*%d***)**

Explanation: See message.

Administrator response: Contact Support.

DPWCA0160E Could not create new thread (*%d***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0161E Could not cancel thread (*%d***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0162E Could not join thread (*%d***)**

Explanation: See message.

Administrator response: Contact Support.

DPWCA0163E Could not set RPC authorization function (0x*%8.8lx***)**

Explanation: See message.

Administrator response: Contact support.

DPWCA0164E Could not setup authentication info (0x*%8.8lx*)

Explanation: Unable to perform login.

Administrator response: Check login parameters.

DPWCA0165E Could not set server login context (0x*%8.8lx*)

Explanation: Unable to set the network credentials to those specified by login context.

Administrator response: Check that network credentials are correct.

DPWCA0166E Could not perform network login (*%s*,*%s*,0x*%8.8lx*)

Explanation: See message.

Administrator response: Verify that user/password is correct.

DPWCA0167E Could not fetch key from keytab file (*%s*,*%s*,0x*%8.8lx*)

Explanation: See message.

Administrator response: Check that the keyfile is set up correctly, and the user information is valid.

DPWCA0168E Could not refresh login context (0x*%8.8lx*)

Explanation: WebSEAL was unable to refresh the login based on existing login information.

Administrator response: Check validity of login information

DPWCA0169E Could not determine login context expiration (0x*%8.8lx*)

Explanation: See message.

Administrator response: Check validity of login information.

DPWCA0170E Could not set RPC interface (0x*%8.8lx*)

Explanation: See message.

Administrator response: Check interfaces.

DPWCA0171E Could not register RPC endpoints (*%s*,0x*%8.8lx*)

Explanation: See message.

Administrator response: Check endpoints.

DPWCA0172E Could not unregister RPC interface (0x*%8.8lx*)

Explanation: See message.

Administrator response: Check validity and status of interfaces.

DPWCA0173E Could not export bindings to name service (*%s*,*%s*,0x*%8.8lx*)

Explanation: See message.

Administrator response: Check status of name service.

DPWCA0174E Could not unregister RPC endpoints (0x*%8.8lx*)

Explanation: See message.

Administrator response: Check validity and status of endpoints.

DPWCA0175E Could not unexport bindings from name service (*%s*,0x*%8.8lx*)

Explanation: See message.

Administrator response: Check validity of interfaces and name service.

DPWCA0176E Malloc failure (0x*%8.8lx*)

Explanation: See message.

Administrator response: Check status of memory on the system.

DPWCA0177E This CDAS does not support this authentication style: (*%d*)

Explanation: See message.

Administrator response: Check validity of authentication style

DPWCA0178E General CDAS (Cross Domain Authentication Service) failure (*%s*, 0x*%8.8lx*)

Explanation: See message.

Administrator response: See message.

DPWCA0179E Pthread error occurred: *%d*

Explanation: See message.

Administrator response: Check system resources.

DPWCA0180E An invalid rule was supplied: *%s*

Explanation: An invalid rule was retrieved from the rules file.

Administrator response: Correct the rule within the specified rules file.

DPWCA0181E No rules were found in the rules file

Explanation: No valid rules were found in the rules file.

Administrator response: Add a valid rule to the rules file, or specify a different rules file.

DPWCA0182W The cache entries have exceeded the maximum cache size.

Explanation: The cache has reached its configured limit.

Administrator response: Increase the permitted size of the cache.

DPWCA0300E API internal error: (*%s***,** *%d***)**

Explanation: See message.

Administrator response: See message.

DPWCA0301W A timeout occurred while waiting for authentication information from *%s***.**

Explanation: A requested authentication operation required further authentication information. This information was not received in a timely fashion.

Administrator response: No action is required.

DPWCA0458E malloc() failure

Explanation: The application was unable to allocate the required memory.

Administrator response: Ensure that there is enough system memory.

DPWCA0751E There is no user authentication information available.

Explanation: The user did not provide their information for authentication

Administrator response: Check user information for authentication

DPWCA0753E Unable to encode certificate data

Explanation: See message.

Administrator response: Verify that xauthn_cert is valid

DPWCA0754E Failure reading string key or value of replacementString from WebSEAL configuration file.

Explanation: See message.

Administrator response: Ensure the value exists for the replacementString in the WebSEAL configuration file.

DPWCA0755E Unable to perform DN mapping.

Explanation: An internal error has occurred. A function was called with invalid parameters.

Administrator response: Contact support.

DPWCA0756E Error building replacement string.

Explanation: An error occurred while preparing an LDAP search filter.

Administrator response: Check for other errors in the configuration file which may provide more information. If no other errors are found, call support.

DPWCA0757E Failure extracting key-value pairs from CERT-DN.

Explanation: An error occurred while parsing the DN from a certificate.

Administrator response: Check that the certificate DN is valid.

DPWCA0759E Invalid parameter passed to get_name_value

Explanation: An internal error has occurred.

Administrator response: Call support.

DPWCA0760E Invalid replacement string entry found

Explanation: The entries in the replacement string stanza must contain '=' characters.

Administrator response: Check that all entries in the replacement string stanza contain an equals sign.

DPWCA0761E Out of memory in get_name_value function

Explanation: Memory allocation failed.

Administrator response: Check per process memory allocation limits.

DPWCA0762E Calloc function could not allocate memory

Explanation: Memory allocation failed.

Administrator response: Check per process memory allocation limits.

DPWCA0763E The last character in the DN was the = following the name

Explanation: The format of the certificate DN was not valid.

Administrator response: Make sure the certificate DN is valid.

DPWCA0764E Unexpected end of string encountered parsing certificate DN

Explanation: See message.

Administrator response: Check the format of the last string in certifcate DN

DPWCA0765E The search string is NULL

Explanation: An internal error has occurred.

Administrator response: Call support.

DPWCA0766E The return dn is NULL

Explanation: An internal error has occurred.

Administrator response: Call support.

DPWCA0768E Error loading XKMS CDAS configuration file.

Explanation: There was an error in the XKMS CDAS configuration file.

Administrator response: Look for other log messages indicating which entries were not found.

DPWCA0769E Error searching suffix '*%s***', return status = 0x***%x***

Explanation: An LDAP search failed.

Administrator response: Verify the LDAP server is running and that the suffix exists.

DPWCA0770E Bad Parameters passed to build_search_filter function.

Explanation: An internal error has occurred.

Administrator response: Call support

DPWCA0771E Error retrieving value from certificate DN.

Explanation: Make sure that the DN contains all of the strings specified in the replacement strings list.

Administrator response: An error occurred while trying to replace a value from the certificate DN.

DPWCA0774E Unable to attach thread to existing JVM.

Explanation: An error occurred when trying to attach a thread to a JVM.

Administrator response: Make sure the JVM being used is a supported JVM.

DPWCA0775E Unable to create JVM or attach to an existing JVM.

Explanation: An error occurred when trying to discover whether or not a JVM already existed in the current process.

Administrator response: Make sure the JVM being used is a supported JVM.

DPWCA0778E Unable to attach thread in shutdown. Aborting cleanup.

Explanation: An error occurred while trying to attach to the JVM to perform clean up activities.

Administrator response: None necessary.

DPWCA0779E Cannot load class: *%s*

Explanation: An error occurred while trying to load a java class.

Administrator response: Make sure the classpath in webseald.conf is correct and that the class can be found in a jar file in the classpath.

DPWCA0780E Cannot create new object: *%s*

Explanation: An error occurred while creating a new object.

Administrator response: Make sure the classpath in webseald.conf is correct and that the class can be found in a jar file in the classpath.

DPWCA0781E Cannot load class method: *%s***.init**

Explanation: An error occurred while trying to load the init method for the class.

Administrator response: Make sure that the class is valid and implements the 'init' method.

DPWCA0782E Exception ocurred in *%s***.init(***%s***)**

Explanation: An exception occurred while invoking the init method of a class.

Administrator response: Check the log file for other details about the exception and make sure the properties file contains no errors.

DPWCA0783E Cannot load class method: *%s***.validate**

Explanation: An error occurred while trying to load the validate method for the class.

Administrator response: Make sure that the class is valid and implements the 'validate' method.

DPWCA0785E Exception ocurred in validate, certificate DN = *%s*

Explanation: An exception occurred while invoking the validate method of a class with the specified certificate DN.

Administrator response: Check the log file for other details about the exception.

DPWCA0787E DN of first entry is NULL.

Explanation: An LDAP search returned an entry without a DN.

Administrator response: Call support.

DPWCA0788E Parsing the names and values for replacement string failed.

Explanation: An error occurred retrieving values needed to certificate DN mapping.

Administrator response: Check the log file for additional errors. Verify the replacement strings in webseald.conf are correct.

DPWCA0900E Unable to open ITIM CDAS configuration file.

Explanation: An error occurred while opening the ITIM CDAS configuration file.

Administrator response: Check the file path in the WebSEAL configuration file and verify that the ITIM CDAS configuration file exists.

DPWCA0901E Incorrect number of arguments used for ITIM CDAS initialization.

Explanation: Bad number of arguments used in ITIM CDAS configuration.

Administrator response: Verify that the correct number of arguments are specified in the WebSEAL configuration file for initializaion of the ITIM CDAS.

DPWCA0902E No ITIM CDAS configuration file or action in the WebSEAL configuration file.

Explanation: Bad parameter for ITIM CDAS configuration file name or action type.

Administrator response: Verify that the ITIM CDAS configuration file name path are correct in the WebSEAL configuration file and that the CDAS action type is either 'check' or 'sync'.

DPWCA0904E Could not create the sending message to ITIM.

Explanation: See message.

Administrator response: Contact support.

DPWCA0905W Function call, *func***, failed error:** *error code error text***.**

Explanation: The specified GSKit function failed while setting up for SSL connections to junctions or from browsers. Or perhaps the initial handshake failed due to invalid certificates or the browser simply closed the connection abruptly.

Administrator response: Examine the error text for details. Typical problems might be that the PKCS#11 library is incorrectly specified, or the PKCS#11 token or token password is incorrect, or the PKCS#11 token is not set up.

DPWCA0906E Could not create socket (*%d***)**

Explanation: This message is overloaded in its meaning. It can mean there was a failure in creating a socket for connecting, setting socket options on it, or creating sockets for HTTP and HTTPS connections.

Administrator response: Check WebSEAL has not exceeded system resource limits. Examine the errno in the system error header file for details.

DPWCA0907E Could not connect socket (*%d***)**

Explanation: This message means that there was a failture to connect to a specific socket.

Administrator response: Examine the errno in the system error header file for details.

DPWCA0908E Could not get the ITIM server host address

Explanation: See the message.

Administrator response: Check whether ITIM server is already running. If ITIM is running, check the ITIM CDAS configuration file to verify the ITIM server URL is specified correctly.

DPWCA0909E Windows library call failed. Could not call the function WSAStartup.

Explanation: The WSAStartup function must be the first Windows Sockets function called by an application or DLL. It allows an application or DLL to specify the version of Windows Sockets required and to retrieve details of the specific Windows Sockets implementation. The application or DLL can only issue further Windows Sockets functions after a successfully calling WSAStartup.

Administrator response: Check WS2_32.DLL in the system environment.

DPWCA0910E Unable to allocate memory

Explanation: Memory allocation failed.

Administrator response: Check per process memory allocation limits.

DPWCA0911E Could not find host name or IP address of ITIM server in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Check the ITIM Password URL part in the ITIM CDAS configuration file.

DPWCA0912E Could not find KeyDataBase in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Verify that the KeyDataBase entry exists in the ITIM CDAS configuration file.

DPWCA0913E Could not find KeyDataBase Password in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Verify that the KeyDataBase Password entry exists in the ITIM CDAS configuration file.

DPWCA0914E Could not find Source DN in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Verify that the Source DN entry exists in the ITIM CDAS configuration file.

DPWCA0915E Could not find ITIM Principal Name in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Verify that the ITIM Principal Name entry exists in the ITIM CDAS configuration file.

DPWCA0916E Could not find ITIM Principal Password in the ITIM CDAS configuration file.

Explanation: See the message.

Administrator response: Verify that the ITIM Principal Password entry exists in the ITIM CDAS configuration file.

DPWCA0917E Could not find ITIM message header.

Explanation: ITIM server replied with an invalid HTTP message header.

Administrator response: Check ITIM server for error message details. Verify the version of the reverse password server component.

DPWCA0922E The password could not be changed in ITIM. The password has beeen changed in TAM.

Explanation: Message indicates that module failed to change the password in ITIM. Password in TAM has been changed.

Administrator response: No action is required.

DPWCF0450E The IBM Security Access Manager Runtime installation directory could not be found. Install IBM Security Access Manager Runtime.

Explanation: The installation directory for AMRTE could not be found in the registry. This is probably because AMRTE is not installed.

Administrator response: Make sure that AMRTE is installed.

DPWCF0451E The IBM Security Access Manager WebSEAL installation directory could not be found. Install IBM Security Access Manager WebSEAL.

Explanation: The installation directory for AMWeb could not be found in the registry. This is probably because AMWeb is not installed.

Administrator response: Make sure that IBM Security Access Manager WebSEAL is installed.

DPWCF0452E The configuration file '*%s*' could not be opened.

Explanation: The configuration file may not exist, or file system permissions may prevent it from being opened.

Administrator response: Make sure that the configuration file exists and can be read and written.

DPWCF0453E The file '*%s*' could not be opened. Error code: *%d*

Explanation: The file could not be opened. The system function returned the indicated error code

Administrator response: Make sure that the file exists in the system, and that it is readable and writable. If necessary, look up the system error code to determine the problem.

DPWCF0454E The file '*%s*' could not be closed. Error code *%d*.

Explanation: A file could not be closed because of the indicated system error.

Administrator response: Make sure that the file system on which the file is located is not full. Also make sure that the directory for the file exists and is writable. If necessary, look up the system error code to identify the problem.

DPWCF0455E The directory '*%s*' could not be opened. Error code: *%d*

Explanation: The directory could not be opened because of the indicated system error code.

Administrator response: Make sure that the directory exists and file system permissions allow it to be read.

DPWCF0456E The directory '*%s*' could not be closed. Error code: *%d*

Explanation: Closing a directory failed because of the indicated system error code.

Administrator response: Make sure that the directory exists and is writable.

DPWCF0457E The instance name '*%s*' is already in use.

Explanation: The instance name is already in use.

Administrator response: Use a different instance name.

DPWCF0458E The length of the instance name '*%s*' is more than *%d* characters.

Explanation: The provided instance name is more than 20 characters.

Administrator response: Use an instance name that has less than 20 characters.

DPWCF0459E The instance name '*%s*' contains invalid characters. Instance names must consist of alphanumeric characters plus the symbols: '-' '_' '.'

Explanation: The provided instance name contains illegal characters.

Administrator response: Use an instance name that contains only valid characters.

DPWCF0460E The IP address '*%s*' does not exist in the system.

Explanation: The provided IP address does not exist in the system.

Administrator response: Make sure that the provided IP address exists in the system.

DPWCF0461E The key file '*%s*' does not exist in the system.

Explanation: The provided key file does not exist in the system.

Administrator response: Make sure the provided key file exists in the system.

DPWCF0462E The key file password is incorrect.

Explanation: The key file password may have been entered incorrectly.

Administrator response: Make sure that the key file password is entered correctly.

DPWCF0463E The LDAP server could not be contacted through SSL on port *%d*.

Explanation: The SSL LDAP port may have been entered incorrectly, or the LDAP server may not be running.

Administrator response: Make sure the LDAP server is running. Correct the SSL LDAP port if necessary.

DPWCF0464E The key file for SSL communcation with the LDAP server is invalid.

Explanation: The wrong key file may have been entered.

Administrator response: Make sure that the provided key file is a valid key file for SSL communication with the LDAP server

DPWCF0465E SSL environment could not be opened. Error: *%s*.

Explanation: An internal SSL error occurred.

Administrator response: The action to correct this problem depends on details in the error message.

DPWCF0466E Port '*%s*' is already in use.

Explanation: The provided port is already in use.

Administrator response: Use a different port, or remove the service that is using the port.

DPWCF0467E Fields marked with an asterisk (*) are required.

Explanation: Not all required inputs were provided.

Administrator response: Fill in values for all of the required fields.

DPWCF0468E The Policy Server could not be contacted. Make sure the Policy Server is running and try again.

Explanation: The Policy Server must be running in order to configure WebSEAL.

Administrator response: Make sure the Policy Server is functioning properly. Restart the Policy Server if necessary.

DPWCF0469E The file '*%s*' could not be copied to '*%s*'

Explanation: An error occurred when trying to copy a file.

Administrator response: Make sure the orginal file exists and the directory for the new file exists. Make sure the file system has sufficient space to copy the file. Make sure the destination directory is writable.

DPWCF0470E The directory '*%s*' could not be copied to the directory '*%s*'.

Explanation: The original directory or the path of the new directory may not be existed.

Administrator response: Make sure the orginal directory exists and the path of the new directory also exists.

DPWCF0471E The directory '*%s*' could not be created.

Explanation: The path to the directory that want to be created may be not existed in the system.

Administrator response: Make sure the path to the directory that want to be created exists in the system.

DPWCF0472E The random password could not be generated.

Explanation: Memory allocation operation failed.

Administrator response: Check memory limits on your machine, and increase availabel memory if possible

DPWCF0473E The WebSEAL instance '*%s*' failed to configure.

Explanation: WebSEAL instance cannot be configured due to the error that displayed before this message

Administrator response: Unconfigure this WebSEAL instance and run configuration program again.

DPWCF0474E The WebSEAL instance '*%s*' failed to unconfigure.

Explanation: WebSEAL instance cannot be unconfigured due to the error that displayed before this message

Administrator response: Run unconfiguration program again.

DPWCF0475E The specified document root directory '*%s*' does not exist.

Explanation: The provided document root directory does not exist.

Administrator response: Make sure the document root directory exists in the system.

DPWCF0476E The specified option '*%s*' is invalid.

Explanation: The specified option is invalid. Only the flags in the usage message are valid.

Administrator response: The specified option is invalid. Use one of the options from the usage and try again.

DPWCF0477E The specified option '*%s*' needs a parameter.

Explanation: The specified option must have a parameter.

Administrator response: Need to specify a parameter for the specified action.

DPWCF0478E The action option needs to be specified.

Explanation: The "action" option needs to be specified to configure or unconfigure WebSEAL instance from command line.

Administrator response: Need to specify the "action" option in the command line inputs.

DPWCF0479E The specified certificate label '*%s*' is invalid.

Explanation: The provided certificate label is incorrect.

Administrator response: Make sure the certificate label is entered correctly.

DPWCF0480E The response file '*%s*' could not be opened.

Explanation: The provided response file does not exist.

Administrator response: Make sure the response file exists.

DPWCF0481E The instance name '*%s*' does not exist to unconfigure.

Explanation: No instance with the provided name was found on the system.

Administrator response: Make sure the instance name was typed correctly.

DPWCF0482E Could not determine the hostname of the machine. Error code: *%d*

Explanation: An error occurred when attempting to determine the host name of the local system.

Administrator response: Make sure the network configuration on the machine is correct.

DPWCF0483E The entry '*%s*' in the response file does not have a value

Explanation: A needed entry in the response file did not have a value.

Administrator response: Make sure that the value of the entry exists in the response file.

DPWCF0484E Error: the configuration program must be run as root.

Explanation: The configuration program needs to be run as the root user in order to be able to function properly.

Administrator response: Run the configuration program as the root user.

DPWCF0485E The ownership of '*%s*' cannot be changed to user ivmgr, group ivmgr. Error code: *%d*.

Explanation: An attempt to change the ownership of a file or directory failed. The system error number can be used to determine the cause of the failure.

Administrator response: Make sure the file or directory exists.

DPWCF0486E Could not create symbolic link from '*%s*' to '*%s*'. Error code: *%d*.

Explanation: An attempt to create a symbolic link failed.

Administrator response: Make sure the destination directory for the symlink exists, and no file or directory exists in that location already. Look up the system error code for further information if necessary.

DPWCF0487E The hash table for configuration options cannot be initialized.

Explanation: The hash table can not be initialized because the allocation of the options failed.

Administrator response: Check memory limits on your machine, and increase available memory if possible

DPWCF0488E The file '*%s*' could not be moved to '*%s*'

Explanation: An error occurred when trying to move a file.

Administrator response: Make sure the orginal file exists and the directory for the new file exists. Make sure the file system has sufficient space to move the file. Make sure the destination directory is writable.

DPWCF0489E ERROR: For WebSEAL to function correctly the maximum number of threads per process should be at least 96. This value can be increased by modifying the MAXTHREADPROC or MAX_THREAD_PROC kernel parameter through the sam utility.

Explanation: The MAXTHREADPROC or MAX_THREAD_PROC must be greater than 96 for WebSEAL to function correctly.

Administrator response: Use the sam utility to increase the MAXTHREADPROC or MAX_THREAD_PROC and run the configuration program again.

DPWCF0490E The configuration status could not be set.

Explanation: This problem should not occur. If it does happen, the machine should be restarted and run the configuration program again.

Administrator response: Restart the machine and run the configuration program again.

DPWCF0491E The file '*%s*' could not be deleted. Error code: *%d*.

Explanation: An attempt to delete a file failed.

Administrator response: Make sure that the file and the directory containing the file are both writable.

DPWCF0492E The socket could not be created. Error code: *%d*

Explanation: An error occured when attempting to initialize a socket.

Administrator response: Look up the system error code for additional information. Check system resource limits on the number of file descriptors, and increase the limits if necessary.

DPWCF0493E The -interactive option is not supported on this platform.

Explanation: The amwebcfg utility does not support the -interactive flag on Windows.

Administrator response: Should not use interactive option for the amwebcfg utility on windows

DPWCF0494E The executable file 'ldapsearch' could not be found.

Explanation: The installlation directory for the LDAP client could not be found.

Administrator response: Make sure the LDAP client is installed correctly.

DPWCF0495E The configuration value of an entry [*%s***] '***%s***' could not be retrieved from the configuration file '***%s***'.**

Explanation: An attempt to retrieve an entry from a configuration file failed.

Administrator response: Check logs for additional errors. The configuration file may not exist or might not be readable. The entry might not exist in the configuration file.

DPWCF0496E The user '*%s***' does not have permission to unconfigure the server.**

Explanation: Only IBM Security Access Manager Administrators are allowed to configure or unconfigure WebSEAL.

Administrator response: Run the configuration program again, supplying the ID and password of an Administrative user.

DPWCF0497E The response file '*%s***' does not exist.**

Explanation: The provided response file does not exist or is not readable.

Administrator response: Make sure the response file exists and is readable.

DPWCF0498E The user '*%s***' could not be removed from the group '***%s***'. Error message: '***%s***'**

Explanation: The function ivadmin_group_removemember failed to remove the user from the group because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0499E The objectspace '*%s***' could not be created. Error message: '***%s***'**

Explanation: The function ivadmin_objectspace_create failed to create the objectspace because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0500E The ACL '*%s***' could not be created with an error: '***%s***'**

Explanation: The function ivadmin_acl_create failed to create the ACL because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0501E The description of ACL '*%s***' could not be set to '***%s***'. Error message: '***%s***'**

Explanation: The function ivadmin_acl_setdescription failed because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0502E The permissions for group '*%s***' in the ACL '***%s***' could not be set. Error message: '***%s***'**

Explanation: The function ivadmin_acl_setgroup failed to set the group permissions because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0503E The permissions for user '*%s***' in the ACL '***%s***' could not be set. Error message: '***%s***'**

Explanation: The function ivadmin_acl_setuser failed to set the user permissions because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0504E The permissions for anyother in the ACL '*%s*' could not be set. Error message: '*%s*'

Explanation: The function ivadmin_acl_setanyother failed to set the permissions for anyother because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0505E The permissions for unauthenticated in the ACL '*%s*' could not be set to '*%s*'. Error message: '*%s*'

Explanation: The function ivadmin_acl_setunauth failed to set the permissions for unauthenticated because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0506E The ACL '*%s*' could not be attached to the protected object '*%s*'. Error message: '*%s*'

Explanation: The function ivadmin_protobj_attachacl failed to attach the acl to a protected object because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0507E The protected object '*%s*' could not be created. Error message: '*%s*'

Explanation: The function ivadmin_protobj_create failed to create a protected object because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0508E The protected object '*%s*' could not be deleted. Error message: '*%s*'

Explanation: The function ivadmin_protobj_create failed to delete the protected object because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0509E The group '*%s*' could not be retrieved. Error message: '*%s*'

Explanation: The function ivadmin_group_get fails to retrieve the group because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0510E The group '*%s*' could not be created. Error message: '*%s*'

Explanation: The function ivadmin_group_create failed to create a group because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0511E The descript for group '*%s*' could not be set to '*%s*'. Error message: '*%s*'

Explanation: The function ivadmin_group_setdescription failed because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0512E The DN of the group '*%s*' could not be retrieved. Error message: '*%s*'

Explanation: The function ivadmin_group_getdn failed because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0513E The directory '*%s*' could not be deleted.

Explanation: The directory may not exist.

Administrator response: Make sure the directory exists.

DPWCF0514E The ivadmin context could not be created. Error message '*%s*'. Use pdadmin to manually create 'su-admins' and 'su-excluded' groups as instructed in the appendix of WebSEAL upgrade document.

Explanation: The function ivadmin_context_createdefault2 failed because of the indicated error.

Administrator response: Fix the problem indicated by the error message.

DPWCF0515E Use pdadmin to manually create 'su-admins' or 'su-excluded' groups as instructed in the appendix of WebSEAL upgrade document.

Explanation: The 'su-admins' or 'su-groups' could not be created in the upgrade process. It should be created manually.

Administrator response: Fix the problem indicated by the message.

DPWCF0516E The tivoli_common_dir entry in the log.properties file has an empty value.

Explanation: The tivoli_common_dir entry must contain Tivoli Common Directory in log.properties file if Tivoli Common Directory is used.

Administrator response: Add a Tivoli Common Directory to tivoli_common_dir entry in log.properties file.

DPWCF0517E The log.properties file does not exist.

Explanation: The log.properties file must exist in Tivoli Common Directory if Tivoli Common Directory is used.

Administrator response: Make sure the log.properties file exists in Tivoli Common Directory.

DPWCF0518E Failed to create Tivoli Common Directory for WebSEAL.

Explanation: An error occurred when creating Tivoli Common Directory for WebSEAL.

Administrator response: The action to correct this problem depends on details displayed in previous error messages.

DPWCF0519E Failed to relocate Tivoli Common Directory for WebSEAL.

Explanation: An error occurred when relocating the Tivoli Common Directory for WebSEAL.

Administrator response: The action to correct this problem depends on details displayed in previous error messages.

DPWCF0520E The '*%s*' option must be provided on the command line.

Explanation: The option displayed in the message must be provided in the command line in order to successfully configure WebSEAL.

Administrator response: Provide the option displayed in the message on the command line.

DPWCF0521E The '*%s*' option only uses 'y' or 'n' for its parameter.

Explanation: The option displayed in the message requires 'y' or 'n' for its value.

Administrator response: Need to provide 'y' or 'n' as the value of the option displayed in the message on the command line.

DPWCF0522E The administrator ID or password is invalid.

Explanation: A valid administrator ID and valid password are required to configure WebSEAL.

Administrator response: Make sure that the administrator ID and password provided are correct.

DPWCF0523E The request-log-format entry in the logging stanza contains an invalid directive: *%s*

Explanation: The request-log-format value is invalid.

Administrator response: Correct the invalid request-log-format configuration value.

DPWCF0524E The request-log-format entry in the logging stanza contains an invalid parameter for a directive.

Explanation: The request-log-format value is invalid.

Administrator response: Correct the invalid request-log-format configuration value.

DPWCF0525W The ping-method value of '*%s*' is not a valid ping-method, defaulting to HEAD.

Explanation: The ping-method specified is not supported. A default value of 'HEAD' has been used.

Administrator response: No action is necessary.

DPWCF0527W The configuration item (*%s*, *%s*) is missing, defaulting to a value of: '*%s*'.

Explanation: The required configuration entry is missing, a default value will be used.

Administrator response: Add the required configuration entry to the configuration file.

DPWCF0528W The configuration file entry encountered is not valid.

Explanation: A configuration entry was retrieved from the configuration file which was not of the expected type or formatting.

Administrator response: Examine the log files for additional information.

DPWCF0529E Domain cookies cannot be shared when the session management server has been configured.

Explanation: The configuration items [session] shared-cookie-name and [session] dsess-enabled are mutually exclusive. If you are attempting to acheive single sign-on in an SMS environment, Disable the shared-cookie-name configuration entry. If you are in an environment without the SMS, disable the dsess-enabled configuration entry.

Administrator response: Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0530E A login redirect page cannot be specified when JavaScript redirection is enabled.

Explanation: The configuration items [acnt-mgt] enable-js-redirect and [acnt-mgt] login-redirect-page are mutually exclusive.

Administrator response: Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0531E The configured single sign-off resource is invalid. The resource must reside on a standard junction.

Explanation: The single sign-off resource must reside on a standard junction and the URI specified must begin with a '/'.

Administrator response: Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0532E The configured list of user-agent patterns will not match all user-agent strings. The list must contain a match-all pattern.

Explanation: The configured list of user-agent patterns will not match against all possible user-agent strings. Add a new entry to the [user-agents] stanza with the pattern '*'.

Administrator response: Correct the configuration as needed and restart the WebSEAL daemon.

DPWCF0533E The [user-agents] stanza must be configured when flow data is enabled.

Explanation: The configuration stanza [user-agents] must be configured and contain at least one entry when using the flow data functionality.

Administrator response: Correct the configuration as needed and restart the WebSEAL daemon.

DPWDS0150E An attempt to create a UUID has failed with the following error: *%s* **(error code: 0x***%x***)**

Explanation: An attempt to create a UUID has failed.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0151E An attempt to retrieve the machine address code (MAC) failed: *%s* **(error code: 0x***%lx***)**

Explanation: An attempt to retrieve the MAC of the server failed.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0152E Memory could not be allocated.

Explanation: An error occurred when the process attempted to allocate memory. There is not enough free memory available to complete the request.

Administrator response: Examine the system for processes consuming excessive memory and restart them. Ensure the system has sufficient physical and virtual memory for its expected load. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0153E No more entries were found in the specified list.

Explanation: An operation requested another entry from a list when there were no remaining entries.

Administrator response: This message is logged as a clarifying addition to another error message. Refer to the recommended action for that error message. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

DPWDS0154E An invalid number was supplied.

Explanation: The system was expecting a number to be supplied, but something else was supplied instead.

Administrator response: Examine other error messages for more detail, correct any problem, and retry the operation.

DPWDS0155E The number which was supplied is too large.

Explanation: The number which was supplied to the system was too large to fit into the allocated memory.

Administrator response: Examine other error messages for more detail, correct any problem, and retry the operation.

DPWDS0156E A system routine failed.

Explanation: A system routine failed.

Administrator response: Examine the log for additional information. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0157E The *%s* **system routine failed: system error code:** *%d*

Explanation: A system routine failed for the reason indicated by the system error code.

Administrator response: Examine the log for additional information. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0158E The requested data is not available.

Explanation: An operation requested data that was not available.

Administrator response: This message is logged as the reason part of an error message. Refer to the recommended action for that error message. For further detailed information about the failure examine earlier messages in the log containing this message. Correct any problems and retry the operation.

DPWDS0159E A command line option was not of the correct format.

Explanation: A command line option was not specified correctly.

Administrator response: Re-run the configuration program ensuring the correct command line options are provided.

DPWDS0160E The supplied configuration data was not valid.

Explanation: A configuration entry was found to be invalid.

Administrator response: Examine the log for further details of the error, correct the configuration, and retry the operation.

DPWDS0161E The command line option, -*%s***, is not valid.**

Explanation: The command line option is not valid for the current program.

Administrator response: Check the usage of the program and re-run it with the correct options.

DPWDS0162E A binary has been executed with incorrect arguments.

Explanation: A binary has been executed with incorrect arguments.

Administrator response: Examine the log files for further error messages, correct any problem, and retry the operation.

DPWDS0163W The '*%s***' parameter of the command is invalid.**

Explanation: The specified parameter, supplied for an administration task, was invalid.

Administrator response: Review the format of the command text to ensure all parameters are correct.

DPWDS0164W An invalid command parameter was supplied.

Explanation: One of the command parameters, supplied for an administration task, was invalid.

Administrator response: Review the format of the command text to ensure all parameters are correct.

DPWDS0165E Could not open file *%s* **(system error code:** *%d***).**

Explanation: The identified file could not be opened for the specified reason.

Administrator response: Check to ensure that the file exists and has the correct permissions.

DPWDS0166E The configuration file could not be opened.

Explanation: The specified file could not be opened.

Administrator response: Check that the file exists and has the correct permissions.

DPWDS0167E Expected configuration data could not be located in the configuration file.

Explanation: An expected configuration item is not present in the configuration file.

Administrator response: Examine the log for further details of the error, correct the configuration, and retry the operation.

DPWDS0168E The *%s* stanza of *%s* requires specification of the *%s* configuration parameter.

Explanation: An expected configuration item is not present in the configuration file.

Administrator response: Correct the configuration and retry the operation.

DPWDS0169E Could not open configuration file '*%s*' due to error: '*%s*'.

Explanation: The identified file could not be opened for the specified reason.

Administrator response: Check to ensure that the file exists and has the correct permissions.

DPWDS0300E The distributed session cache client failed to initialized.

Explanation: The client for the distributed session cache interface could not be initialized.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0301E A general failure has occured within the distributed session cache client.

Explanation: An error has occured within the distributed session cache client.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0302E A replica set which is unknown to the distributed session cache client has been supplied (*%s*).

Explanation: An operation on a unknown distributed session cache replica set has been requested.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0303E A replica set which is unknown to the distributed session cache client has been supplied.

Explanation: An operation on a unknown distributed session cache replica set has been requested.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0304E The requested version *%d* of the session key was not found for replica *%s* in replica set *%s*.

Explanation: A request was made for a session key which is not currently stored. This error occurs when an old session ID is used.

Administrator response: Either increment the key expiration time within the configuration file, or ensure that old session ID's are not used.

DPWDS0305E The requested key was not found.

Explanation: A request was made for a session key which is not currently stored. This will usually occur when an old session ID is used.

Administrator response: Either increment the key expiration time within the configuration file, or ensure that old session ID's are not used.

DPWDS0306E No session keys are currently available.

Explanation: A request was made for the current session key, but no key has been stored in the key table .

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0307E An error occurred when attempting to communicate with the SOAP server URL *%s*: *%s* (error code: *%d*/0x*%x*).

Explanation: An attempt was made to communicate with the SOAP server and a failure occured within the underlying communications layer.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Ensure that the SOAP server is running and reachable. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0309E An error was returned from the SOAP server in cluster *%s* when calling the *%s* interface: *%s* (code: 0x*%x*).

Explanation: The distributed session cache server returned an error.

Administrator response: Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0310E An invalid key size was returned by the distributed session cache server: *%d*, whereas it should be: *%d*.

Explanation: The distributed session cache server has passed a key to the client which is not the expected key size.

Administrator response: Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0311E An incorrect key version was returned by the distributed session cache server to replica *%s* in replica set *%s*: *%d*, whereas it should be: *%d*.

Explanation: The distributed session cache server has passed a key to the client which is not the expected version.

Administrator response: Examine messages within the distributed session cache server log. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0312E The distributed session cache server could not be reached.

Explanation: An unsuccessful attempt has been made to communicate with an interface of the distributed session cache server.

Administrator response: Ensure that the distributed session cache server is running and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0313E The cryptographic routine, *%s*, failed : *%s* (error code: 0x*%x*).

Explanation: A call in to a cryptographic routine has failed.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0314E The cryptographic routine, *%s*, failed.

Explanation: A call in to a cryptographic routine has failed.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0315W An invalid session key was provided to the distributed session cache server client.

Explanation: A session key with an invalid format was provided to the distributed session cache server client.

Administrator response: Ensure that the distributed session cache server is running and can be reached by the client. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0316E The distributed session cache server did not return a response.

Explanation: The distributed session cache server did not return a response to a request made by the shared distributed session cache client.

Administrator response: Ensure that the distributed session cache server is running and can be reached by the client. Examine the distributed session cache server's logs for error messages relating to this failure. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0319E The distributed session cache server client attempted to join the replica set '*%s*' twice with the replica name '*%s*'.

Explanation: The distributed session cache server client has been configured to join a replica set twice using the same replica name. The client must use different replica names for each server instance in a replica set.

Administrator response: Modify the configuration file to specify different replica names for each server instance joining the same replica set. Restart the server.

DPWDS0320E The DN contained within the server certificate, *%s*, is not recognised by replica *%s* in replica set *%s*.

Explanation: The DN found within the server certificate was not listed as a valid DN within the configuration file.

Administrator response: Ensure that the correct server certificate is supplied, or modify the list of valid DN's within the configuration file.

DPWDS0321E The replica *%s* in replica set *%s* does not have permission to access the distributed session cache server.

Explanation: The distributed session cache server has been configured to require authentication, but the distributed session cache client either did not authenticate, or authenticated using an identity that does not have permission to access the distributed session cache server.

Administrator response: Ensure the distributed session cache client has been configured to use HTTPS to access the distributed session cache server, and that the configuration file specifies the correct client certificate. Check that the distributed session cache server security role mappings are correct. It may be necessary to restart the client.

DPWDS0322E The distributed session cache server for the replica set, *%s*, of the replica, *%s*, could not be reached.

Explanation: An unsuccessful attempt has been made to communicate with an interface of the distributed session cache server.

Administrator response: Ensure that the distributed session cache server is running and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0323E No session keys are currently available for replica *%s* in replica set *%s*.

Explanation: A request was made for the current session key, but no key has been stored in the key table .

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0450E Error parsing STS response element line *%d*, column *%d*: '*%s*'. The element text was '*%s*'.

Explanation: The STS returned an unintelligible XML response.

Administrator response: If other elements of the STS response are complete, SSO will continue. Otherwise, SSO will fail. If SSO fails, exmaine the element to determine why the STS response was invalid.

DPWDS0451E Unable to parse timestamp '*%s*'

Explanation: The timestamp returned from the STS was unintelligible.

Administrator response: Examine the element to determine why the timestamp was invalid.

DPWDS0452E Unable to parse timestamp.

Explanation: The timestamp returned from the STS was unintelligible.

Administrator response: Examine the element to determine why the timestamp was invalid.

DPWDS0453E The STS response did not contain the element '*%s*'

Explanation: The STS response was incomplete.

Administrator response: The TFIM server may not be functioning properly, or the STS module may need to be modified to return the necessary data.

DPWDS0454E The STS response did not contain a necessary element.

Explanation: The STS response was incomplete.

Administrator response: Examine other entries in the logs to determine which element was missing. The TFIM server may not be functioning properly, or the STS module may need to be modified to return the necessary data.

DPWDS0455E Token types other than 'kerberos' require that you specify an HTTP header name with the 'header-name' configuration option or an HTTP cookie name with the 'cookie-name' configuration option.

Explanation: A configuration option was missing from the configuration file

Administrator response: Add the needed entries to the configuration file.

DPWDS0456E Error *%08x* **occurred when retrieving a token for user '***%s***' to access '***%s***'. Refer to other log messages for additional detail.**

Explanation: An attempt to retrieve a token to access a resource failed. Other messages with greater detail have been logged.

Administrator response: Examine other entries in the logs to determine the root cause of the failure.

DPWDS0600E An unexpected AXIS exception was caught while processing a client request. Error message *%s* **(0x***%x***) was returned with the exception.**

Explanation: AXIS returned an exception condition while process a client request.

Administrator response: Refer to the error log to determine if an error message accompanied the exception.

DPWDS0601E A failure occurred while processing a received distributed session request.

Explanation: An error occurred when processing a distributed session request.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0602E The server could not bind to the configured address: *%s*

Explanation: An error occurred when the server attempted to bind to the configured IP address.

Administrator response: Chck the configured IP address to ensure that it is a valid local address on the server.

DPWDS0604W The distributed session cache server has started.

Explanation: The distributed session cache server has started.

Administrator response: No action required.

DPWDS0605W The distributed session cache server has been stopped.

Explanation: The distributed session cache server has been stopped by the administrator.

Administrator response: No action required.

DPWDS0606E Could not accept incoming connection on '*%s***:***%d***': system error number =** *%d*

Explanation: The Operating System returned an error when the server attempted to accept an incoming connection.

Administrator response: Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0607E Could not accept incoming connection

Explanation: The Operating System returned an error when the server attempted to accept an incoming connection.

Administrator response: Check the server has not exceeded system resource limits.

DPWDS0608E Could not poll for any incoming connections: system error number = *%d*

Explanation: The Operating System returned an error when the server attempted to poll for an incoming connection on the configured addresses and port.

Administrator response: Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0609E Could not poll for incoming connection

Explanation: The Operating System returned an error when the server attempted to poll for an incoming connection on the configured addresses and port.

Administrator response: Check the server has not exceeded system resource limits.

DPWDS0610E Could not determine the local network address of a connection: system error number = *%d*

Explanation: The Operating System returned an error when the server attempted to determine the network interface over which the incoming connection was received.

Administrator response: Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0611E Could not determine the local network address of a connection

Explanation: The Operating System returned an error when the server attempted to determine the network interface over which the incoming connection was received.

Administrator response: Check the server has not exceeded system resource limits.

DPWDS0612E The *%s* **'***%s***' is a duplicate or a subset of another configured** *%s* **entry.**

Explanation: It is not valid to specify the same address twice, or to specify an address like '::' or 0.0.0.0 with additional addresses as they cover all addresses.

Administrator response: Modify the server configuration file and remove the listen-address configuration entry which is causing the problem.

DPWDS0613E A configured address is a duplicate or a subset of another.

Explanation: It is not valid to specify the same address twice, or to specify an address like '::' or '0.0.0.0' with additional addresses as they cover all addresses.

Administrator response: Modify the server configuration file and remove the address causing the problem.

DPWDS0614E accept-admin-address values must be a subset of the listen-address addresses.

Explanation: It is not valid to specify an accept-admin-address that is not also included by the listen-address configuration.

Administrator response: Modify the server configuration file and correct the accept-admin-address configuration entry which is causing the problem.

DPWDS0615E Could not determine the remote network address of a connection: system error number = *%d*

Explanation: The Operating System returned an error when the server attempted to determine the remote network address from which the incoming connection was received.

Administrator response: Check the server has not exceeded system resource limits. For further details on the problem refer to the system error number in the operating system documentation.

DPWDS0616E Could not determine the remote network address of a connection

Explanation: The Operating System returned an error when the server attempted to determine the remote network address from which the incoming connection was received.

Administrator response: Check the server has not exceeded system resource limits.

DPWDS0617W Entering standby mode.

Explanation: The DSC server is changing mode, or starting up in standby mode. This is likely expected behavior caused by the startup of the server, or by the changing of the server mode by an administrator.

Administrator response: This is likely expected behavior and no action is required.

DPWDS0618W Entering active mode.

Explanation: The DSC server is changing mode into active mode. At startup the server begins in standby mode and if appropriate will change to active mode. Or the active Distributed Session Cache server may have failed and this server is taking over as the active. Or the administrator has changed the mode of the server.

Administrator response: If this is not a startup mode change, then check the previous primary DSC server for failure.

DPWDS0619E A database operation failed on line *%d* **with error** *%d***: '***%s***'. Native error** *%d***. SQL state: '***%s***'**

Explanation: An error was encountered while saving or reading session data to or from the database.

Administrator response: Check the SQL error message for the possible cause.

DPWDS0620E A database operation failed.

Explanation: An error was encountered while saving or reading session data to or from the database.

Administrator response: Check the log for an SQL error message which contains a possible cause.

DPWDS0621E The command 'ADMIN COMMAND 'hsb state' failed with an error *%d*: '*%s*'.

Explanation: An error was encountered while attempting to determine the HSB state of the embedded SolidDB server.

Administrator response: Check the error code and message for a possible cause.

DPWDS0622E Unable to start the embedded SolidDB server. Error *%d*.

Explanation: An error was encountered while attempting to start the embedded SolidDB server.

Administrator response: Check the error code for the possible cause, such as invalid permissions on the database and log files.

DPWDS0623E Unable to start the embedded SolidDB server.

Explanation: An error was encountered while attempting to start the embedded SolidDB server.

Administrator response: Check the error code in the log for a possible cause, such as invalid permissions on the database and log files.

DPWDS0624E Unable to register a shutdown notifier function with the SolidDB server. Error *%d*.

Explanation: An error was encountered while attempting to register a call back function with the embedded SolidDB server. This call back is required for detection of the shutdown of the embedded SolidDB server.

Administrator response: Check the error code for the possible cause.

DPWDS0625E Unable to register a shutdown notifier function with the embedded SolidDB server.

Explanation: An error was encountered while attempting to register a call back function with the embedded SolidDB server. This call back is required for detection of the shutdown of the embedded SolidDB server.

Administrator response: Check the error code in the log for the possible cause.

DPWDS0626E Unable to load and extract functions from the SolidDB shared library.

Explanation: An error was encountered while attempting to load the library containing the embedded SolidDB server.

Administrator response: Check the log for additional error messages.

DPWDS0627E The configuration value of *%d* for number-of-nodes is not valid. It must be 0, 1, 2 or 4.

Explanation: The number-of-nodes configuration value has an incorrect value.

Administrator response: Change the configuration file value to be correct and retry.

DPWDS0628E The configuration value for number-of-nodes is not valid. It must be 0, 1, 2 or 4.

Explanation: The number-of-nodes configuration value has an incorrect value.

Administrator response: Change the configuration file value to be correct and retry.

DPWDS0629E The configuration value of *%d* for node-number is not valid. It must be 0 for number-of-nodes = 0, else a value from 1 to number-of-nodes.

Explanation: The node-number configuration value has an incorrect value.

Administrator response: Change the configuration file value to be correct and retry.

DPWDS0630E The configuration value for node-number is not valid. It must be 0 for number-of-nodes = 0, else a value from 1 to number-of-nodes.

Explanation: The node-number configuration value has an incorrect value.

Administrator response: Change the configuration file value to be correct and retry.

DPWDS0631E The option -n '*%s*' is not valid for -N '*%s*'. For -N 0 the value for -n must be 0, else a value from 1 to the value of -N.

Explanation: The -n command line option value has an incorrect value.

Administrator response: Correct the command line option and retry.

DPWDS0632E The password option -p must be supplied and must not be an empty string.

Explanation: The -p command line option value was not provided or was an empty string.

Administrator response: Correct the command line option and retry.

DPWDS0633E The option '*%s*' must be supplied.

Explanation: A required command line option value was not provided.

Administrator response: Add the missing option to the command line and then retry.

DPWDS0634E The option -N '*%s*' is not valid. It must be one of 0, 1, 2 or 4.

Explanation: The -N command line option value has an incorrect value.

Administrator response: Correct the -N command line option and retry.

DPWDS0636E Only one of the '-C', '-U' or '-X' options must be provided.

Explanation: Either none of the -C, -U or '-X' options were provided, or more than one was provided.

Administrator response: Either ensure that only one of the -C, -U, or -X options are provided.

DPWDS0637E The Distributed Session Cache server is already configured or there is an unexpected problem with the configuration file '*%s*'

Explanation: Either the Distributed Session Cache server configuration file exists, indicating it is already configured, or there was a problem attempting to check if the file exists.

Administrator response: Unconfigure the Distributed Session Cache server before attempting to configure it again. If the specified configuration file does not exist then ensure the directory which would contain the file is valid.

DPWDS0638E Unable to contact the remote DSC server at '*%s*'.

Explanation: A test probe of the specified Distributed Session Cache server failed. This indicates that it may not be operational, the network connection is down, or the address and port used to access it are not correct.

Administrator response: Ensure that the specified Distributed Session Cache server is running.

DPWDS0639E Unable to open the file '*%s*' error *%d*: '*%s*'.

Explanation: The configuration process failed to open the template configuration file.

Administrator response: Examine the error code and message for the cause of the failure and correct it.

DPWDS0640E Unable to create the file '*%s*' error *%d*: '*%s*'.

Explanation: The configuration process failed to create a new configuration file.

Administrator response: Examine the error code and message for the cause of the create failure and correct it.

DPWDS0641E Error processing the configuration file '*%s*' line *%d*: '*%s*'.

Explanation: An error occured while processing the configuration file.

Administrator response: Examine the specified line for the cause of the error and correct it.

DPWDS0642E Unable to remove the file '*%s*' error *%d*: '*%s*'.

Explanation: The unconfiguration process failed to remove a file.

Administrator response: Examine the error code and message for the cause of the failure and correct it.

DPWDS0643E Failed to create and initialize the backing database.

Explanation: The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable to create and initialize the database.

Administrator response: Retry the operation to see if the problem persists.

DPWDS0644E Failed to put the backing database into a writable mode.

Explanation: The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable to put the database into a mode which will allow the data to be modified.

Administrator response: Retry the operation to see if the problem persists.

DPWDS0645E Failed to cleanly shutdown the backing database.

Explanation: The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool was unable cleanly shutdown the database.

Administrator response: Retry the operation to see if the problem persists.

DPWDS0646E Failed to copy the data from the primary distributed session cache backing database to the secondary.

Explanation: The DSC uses a backing SolidDB database to replicate session data for failover scenarios. The configuration tool failed to perform the initial copy of the data from the primary database to the secondary.

Administrator response: Ensure that the primary distributed session cache server is running and correctly configured as the primary node for replication.

DPWDS0647E Failed to change the ownership of the backing database or configuration files.

Explanation: The ownership of the DSC backing SolidDB database or configuration files could not be changed to the user and group ID specified in the template configuration file.

Administrator response: Retry the operation to see if the problem persists.

DPWDS0648E Failed to send updates to the master Distributed Session Cache server. State *%d* with error *%d* '*%s*'. Attempting to recover.

Explanation: When an isolated Replica Distribute Session Cache server reconnects with the Master it will send it's updates to the Master. This error message indicates that the send failed and an attempt is being made to recover automatically.

Administrator response: The server will attempt to recover. Monitor for additional message in case recovery is not successful. Ensure the network and all Distribute Session Cache servers are functioning correctly.

DPWDS0651W The Distribute Session Cache server is waiting for the initial copy of the database to be send to it.

Explanation: The embedded SolidDB server is configured as a Secondary in a Highly Available pair and is waiting for the Primary in the pair to send the initial copy of the database.

Administrator response: If the copy does not occur then ensure the associated Distributed Session Cache servers are running so they can provide the database.

DPWDS0653W The Distribute Session Cache server has applied the updated copy of database.

Explanation: The embedded SolidDB server has received a complete replacement copy of the database from the primary and is now using it.

Administrator response: No action is required.

DPWDS0654E Failed to unregister this replica from the master database.

Explanation: While unconfiguring the node the tool was not able to unregister it from the master database.

Administrator response: If the master node will also be unconfigured you can ignore this error. If the master node is not running then start it and attempt to clear this issue by configuring and unconfiguring this node. The configure may experience an error as the node may have been left registered, but this can be ignored and the unconfigure should clear the issue.

DPWDS0655E The tool was not able to create the tempory file '*%s*', error: '*%s*'.

Explanation: While unconfiguring the node the tool was not able to create a tempory file of SQL commands to unregister it from the master database.

Administrator response: If the master node will also be unconfigured you can ignore this error.

DPWDS0750E The administration interface of the distributed session cache server did not return all expected data.

Explanation: Return data from a distributed session cache server administration operation was missing.

Administrator response: Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0751E The administration interface of the distributed session cache server returned some unexpected data.

Explanation: The return data from a distributed session cache server administration operation was of an unexpected format.

Administrator response: Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information -

http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0752E The *%s* operation of the distributed session cache server administration interface did not return all expected data: *%s*.

Explanation: The indicated return data from a distributed session cache server administration operation is missing.

Administrator response: Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0753E The *%s* operation of the distributed session cache server administration interface returned some data for the *%s* attribute which was not in the expected format.

Explanation: The return data from a distributed session cache server administration operation was of an unexpected format.

Administrator response: Ensure the correct version of the distributed session cache server and client is being used. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0754E An error occurred when attempting to communicate with the administration interface of the distributed session cache server using the URL *%s*: *%s* (0x*%x*).

Explanation: An attempt was made to communicate with the administration interface of the distributed session cache server and a failure occurred within the underlying communications layer.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Ensure the administration interface of the distributed session cache server is available and reachable. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0755E The administration interface of the distributed session cache server could not be accessed.

Explanation: An unsuccessful attempt has been made to communicate with the administration interface of the distributed session cache server.

Administrator response: Ensure the administration interface of the distributed session cache server is available and can be reached by the client. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWDS0762W No replicas were found for the specified replica set.

Explanation: A request was made to display a specified replica set, but no replicas are currently registered with the replica set.

Administrator response: No action is required, this is a status message.

DPWDS0766W No sessions were found which match the specified search criteria.

Explanation: A request was made to list sessions which match specified criteria, but no matching sessions were found.

Administrator response: No action is required, this is a status message.

DPWDS0767W The '*%s*' instance is invalid.

Explanation: The specified instance, supplied for an administration task, was invalid.

Administrator response: Review the format of the command text to ensure all parameters are correct.

DPWDS0768E The administration operation is not permitted on the interface which was used to contact the distributed session cache server.

Explanation: The Distributed Session Cache server can be configured to restrict access for administration commands to a subset of the network interfaces it is configured to use. The administration request was not received on one of the permitted interfaces.

Administrator response: Change the interface of the Distributed Session Cache server being addressed, or adjust the configuration of the Distributed Session Cache server.

DPWDS0769E The administration operation from '*%s*' is not permitted on the interface '*%s*'.

Explanation: The Distributed Session Cache server can be configured to restrict access for administration commands to a subset of the network interfaces it is configured to use. The administration request was not received on one of the permitted interfaces.

Administrator response: Change the interface of the

Distributed Session Cache server being addressed, or adjust the configuration of the Distributed Session Cache server.

DPWDS0770E Function call, *func*, failed error: *error code error text***.**

Explanation: The specified GSKit function failed while setting up for SSL connections to the Distributed Session Cache server. Or perhaps the initial handshake failed due to invalid certificates or the client simply closed the connection abruptly.

Administrator response: Examine the error text to gain insight on the problem.

DPWIV0151E Could not initialize serviceability component (*%s***, 0x***%8.8lx***)**

Explanation: WebSEAL was unable to register the service component with the serviceibility subsystem or register an in memory catalog. The error code output in the message will give finer details as to why. Most likely it will be due to a lack of memory or a design flaw.

Administrator response: Check memory ulimit on UNIX platforms, and available memory on all types of platforms. Increase available memory to the WebSEAL process if applicable.

DPWIV0152E Could not register serviceability message table (*%s***, 0x***%8.8lx***)**

Explanation: WebSEAL was unable to register an in memory catalog. The error code output in the message will give finer details as to why. Most likely it will be due to a lack of memory or a program design flaw.

Administrator response: Check memory ulimit on UNIX platforms, and available memory on all types of platforms. Increase available memory to the WebSEAL process if applicable.

DPWIV0154E Could not open configuration file (*%s***,** *%d***)**

Explanation: The configuration file output in the message was not able to be opened. The error code also output in the message will give finer details. This code is likely to be one of: 8, failed to lock the file, generic locking catch-all code. 10, unable to open the file, general open catch-all code. 11, bad argument to function from program design flaw. 12, failed to lock the file, it is already locked. 13, File permissions don't allow the program to open the file. 14, Insufficent memory available to the program.

Administrator response: Based on the error code output in the message do one of the following actions. 8 or 12, the program may already be running, or the another process may have the file open and locked. 10 or 13, check the file exists and in the case of 13, check the ownership and access permissions. WebSEAL can change the user it is running as so examine the WebSEAL configuration file for unix-user. 11 contact technical support. 14, check the data ulimit for the process and the available memory. Increase it if possible.

DPWIV0155E Configuration stanza missing (*%s***)**

Explanation: A necessary configuration file stanza was not found.

Administrator response: Make sure the name of the stanza is spelled correctly in the configuration file.

DPWIV0156E Configuration item missing (*%s***,** *%s***)**

Explanation: The configuration entry, output in the error message, is missing from under the stanza, also output in the error message. The entry is not optional. Possibly a spelling mistake, or a new WebSEAL binary was installed that requires additional new entries.

Administrator response: Fix any spelling errors or add the missing entry.

DPWIV0157E Could not initialise servicibility messaging (0x*%8.8lx***)**

Explanation: See message.

Administrator response: The message contains an error code that gives more specific details on the cause. Also until the servicibility messaging is setup, English messages may be output, and on UNIX platforms these may additionally be put into syslog under the user facility. Once the first servicibility message file is initialised successfully errors may be output to standard error log files. Check for these messages for more specific details. Also check the language pack for the locale has been installed.

DPWIV0158E Could not set process rlimit.

Explanation: The UNIX process attempted to set it's ulimit values for the number of file handles and on some platforms the virtual memory size. If the operatining system has set hard ulimits smaller than the ones requested then it could fail.

Administrator response: Increase relevant operating system kernel specific limits. Typically WebSEAL needs 2048 file handles (except on Solaris, where it is 1024). On Solaris WebSEAL attempts to ensure it has a minimum virtual memory ulimit of 192MB. Another reason this might fail is that the process was not started by root.

DPWIV0161E Server is already running (PID *%d*)

Explanation: The program can not have multiple instances running. In the case of WebSEAL, only one WebSEAL process can be running per instance. The confilicting program was determined by reading it's Process ID (PID) from the a file and determining if that PID was active.

Administrator response: Ensure only one instance is running. On UNIX examine the output of the ps command to determine the offending instance. It is possible that if an old PID is in the PID file, and another process has aquired this old PID that the message is in error. In that case simply remove the PID file and start the process again.

DPWIV0162E Could not create PID file (*%s*, *%d*)

Explanation: The program could not create the file, specified in the message text. The reason can be determined in more detail from the error number, also found in the error text. On UNIX the meaning of this error code can typically be found in /usr/include/sys/errno.h. Windows may need to contact technical support as the included files are not shipped with the operating system. Typical problems might be insufficent priviledges, or lack of disk space.

Administrator response: Check the ownership and permissions on the file, or directory containing the file, allow the process to create or recreate it. Check there is sufficent disk space on the file system/partition to contain the file.

DPWIV0163E Could not become background process because output redirection failed (*%d*)

Explanation: One of the four steps to creating a background daemon process has failed. If the error number specified in the error text is -1 or -2, then it was unable to connect standard error or standard out to a log file. For WebSEAL this log file is the server-log entry in the configuration file. Typically this can be caused by insuffcent priviledges on the file or the directory containing the file for WebSEAL.

Administrator response: Examine the error code, if -1 or -2 then check the ownership and permissions of the servers log file and containing directory.

DPWIV0164W Could not start background process

Explanation: If this message is generated during an attempt to start WebSEAL then the attempt by WebSEAL to fork itself into the background has failed. Typpically some initialization failed in the child process and an additional message will be logged by the background child process. But it could also be due to insuffcent operating system resources.

Administrator response: For WebSEAL startup check for additional errors that indicate why the background process stopped.

DPWIV0166E Could not load configuration

Explanation: Unable to load WebSEAL configuration (typically webseald.conf) for for locating LDAP configuration information or unable to load ldap configuration file (typically ldap.conf). Additional messages should be logged detailing why.

Administrator response: Locate additional logged message to determine the problem. If no additional messages, examine the ownership, permissions, and existance of these files.

DPWIV0167E Invalid UNIX user name (*%s*)

Explanation: The server (typically WebSEAL) failed to get information for the user. It is likely that it is an invalid user name.

Administrator response: Update the WebSEAL configuration file (typically webseald.conf) and correct the user name for 'unix-user' to a valid one.

DPWIV0168E Invalid UNIX group name (*%s*)

Explanation: The server (typically WebSEAL) failed to get information for the group. It is likely that it is an invalid group name.

Administrator response: Update the WebSEAL configuration file (typically webseald.conf) and correct the group name for 'unix-group' to a valid one.

DPWIV0169E Could not change process GID (*%s*)

Explanation: The server (typically WebSEAL) failed to change the processes group ID to the one specified. This can happen if the server does not have the privaledges required.

Administrator response: Start the server as root or change the owner of the program to root and set the 's' bit in it's perms.

DPWIV0170E Could not change process UID (*%s*)

Explanation: The server (typically WebSEAL) failed to change the processes user ID to the one specified. This can happen if the server does not have the privaledges required.

Administrator response: Start the server as root or change the owner of the program to root and set the 's' bit in it's perms.

DPWIV0172E Unexpected end of byte stream

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0173E Could not stop background process (errno *%d*)

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0174E Could not change the working directory (errno *%d*)

Explanation: A child CGI process of WebSEAL is unable to change to the directory containing the CGI. The meaning of the errno value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response: Lookup the errno in errno.h for the cause.

DPWIV0175E Could not open a pipe (errno *%d*)

Explanation: WebSEAL failed to create a pipe for communicating to a child CGI process of WebSEAL. The meaning of the errno value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response: Lookup the errno in /usr/include/sys/errno.h for the cause.

DPWIV0176E Could not fork (errno *%d*)

Explanation: WebSEAL failed for fork so that it could execute a CGI. This could be due to insufficent operating system resources.

Administrator response: Lookup the errno in /usr/include/sys/errno.h for the cause.

DPWIV0177E Could not duplicate file descriptor (errno *%d*)

Explanation: A CGI created by WebSEAL failed to redirect it's standard out or standard in to the pipes used to communicate with the parent WebSEAL process.

Administrator response: Lookup the errno in /usr/include/sys/errno.h for the cause.

DPWIV0178E Operation forbidden by the operating system

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0179E Unknown user

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0180E Missing .conf file setting

Explanation: The expected bind-dn or bind-pwd entries in the ldap configuration file (typically ldap.conf) are missing.

Administrator response: Add the missing bind-pwd or bind-dn entry.

DPWIV0181E *%s*: Missing [*%s*] setting: *%s*

Explanation: An ldap entry is missing from the configuration file.

Administrator response: Add the missing entry.

DPWIV0186E Unable to setup a connection to the LDAP server

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0187E Invalid LDAP 'replica' entry in config file

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0189E Unable to configure LDAP replica into server.

Explanation: Message is not used. This is purely used as in internal status code.

Administrator response: No action is required

DPWIV0192W LDAP server *%s* has failed

Explanation: The LDAP server named in the message is not responding to requests.

Administrator response: Check the LDAP server is operational. Once operational WebSEAL will start using it again automatically. Check the LDAP server name is correct.

DPWIV0193W LDAP server ***%s*** **has recovered**

Explanation: The LDAP server named in the message was previously non-operational. It is now responding correctly to requests and will be used again.

Administrator response: No action required.

DPWIV0194E Could not become background process because pipe failed. (*%d*)

Explanation: The pipe() function failed. This error value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response: Make sure server has the permission to create interprocess pipes.

DPWIV0195E Could not become background process because fork failed. (*%d*)

Explanation: The fork() function failed. This function fails when insufficient memory is available, or machine process limit is reached. The error value can typically be found in /usr/include/sys/errno.h and will give finer details on the cause.

Administrator response: Make sure server machine resources are available.

DPWIV0196W Could not start background process: ***%s***

Explanation: This is due to the failure to execute a CGI program. Either the program is not executable, or system resources are not available to run the program.

Administrator response: WebSEAL could not successfully start a child process. Most likely the program does not exist or is not executable.

DPWIV0197E Error in stanza file ***%s*** **on line** ***%d*****:** ***%s***

Explanation: An error occurred while attempting to read data from a stanza file.

Administrator response: Correct the problem in the stanza file.

DPWIV0198E Error in stanza file.

Explanation: An error occurred while attempting to read data from a stanza f ile. Log files will contain more information.

Administrator response: Examine log files to identify the error in the stanza file.

DPWIV0199E An unexpected exception occurred at line ***%s*****:*****%d***

Explanation: An internal error occurred.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0200E An unexpected exception occurred

Explanation: An internal error occurred.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0201E The azn-api function '*%s*' returned 0x*%lx*

Explanation: An unexpected azn-api function failure occurred.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0202E An azn-api function unexpectedly failed

Explanation: An unexpected azn-api function failure occurred.

Administrator response: Check log files for additional details. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0203E Additional information from azn-api: ***%s*** **=** ***%s***

Explanation: An azn-api error occurred, and this message contains more detail about the error.

Administrator response: Check log files for additional details. The exact action to take depends on the context of the error.

DPWIV0204E An invalid permission string, ***%s*****, was located for the** ***%s*** **method within the** ***%s*** **stanza.**

Explanation: A configured permission string is invalid and not recognized by the IBM Security Access Manager Authorization engine.

Administrator response: Correct the specified permission string within the configuration file and ensure that the permission string is valid.

DPWIV0205E The system function '*%s*' returned 0x*%lx*.

Explanation: An unexpected system function failure occurred.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0450E Could not create new thread (*%d*)

Explanation: WebSEAL failed to create an additional thread. This may be due to running out of operating system resources or exceeding process limits.

Administrator response: Check memory and thread limits for the process, and available memory. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0452E Could not cancel thread (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to stop a thread that monitors a junctions health.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0453E Could not join thread (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to cleanup a stopped thread that monitors junction health.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0454E Could not create mutex (*%d*)

Explanation: WebSEAL failed to create a mutex used to protect internal resources. This may be due to insufficent Operating System resources or exceeding process limits such as memory.

Administrator response: Check memory limits for the process, and available memory. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0455E Could not destroy mutex (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to cleanup a mutex used to protect system resources.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0456E Could not lock mutex (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to lock a mutex used to protect system resources.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0457E Could not unlock mutex (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to lock a mutex used to protect system resources.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0458E Could not create condition variable (*%d*)

Explanation: WebSEAL failed to create a condition variable used to wait for events to occur. This may be due to insufficent Operating System resources or exceeding process limits such as memory.

Administrator response: Check memory limits for the process, and available memory. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0459E Could not destroy condition variable (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to release resources used by a condition variable.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0460E Could not wait on condition variable (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to wait on a condition variable.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0461E Could not broadcast on condition variable (*%d*)

Explanation: This message indicates a serious internal error involving the threading library.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0462E Could not signal on condition variable (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to signal a condition variable.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0463E Could not set thread cancelability (*%d*)

Explanation: WebSEAL has an unrecoverable internal error when trying to modify a threads cancel state.

Administrator response: Contact technical support, this is an unexpected internal error. The error number can be looked up in /usr/include/sys/errno.h for more details on the problem.

DPWIV0465E Error msg returned from stanza function: (*%s*).For entry: *%s*/*%s*.

Explanation: The migrate tool has had an error while manipulating a configuration file full of stanzas and entries. The bracketted error string within the error message gives more detail.

Administrator response: Correct the error specified by the bracketted error string.

DPWIV0466E Unsupported configuration item type (*%d*)

Explanation: The migrate tool has had an unrecoverable internal error. It has encountered an unknown entry type.

Administrator response: Contact technical support, this is an unexpected internal error.

DPWIV0467E Could not create new pthread key (*%d*)

Explanation: See message.

Administrator response: Contact product support.

DPWIV0468E Could not create default pthread attributes.

Explanation: WebSEAL failed to create pthread attributes.

Administrator response: Check available memory for the process.

DPWIV0469E pthread_attr_setdetachstate() failed (*%d*)

Explanation: This message indicates a serious internal error involving the threading library.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0470E Could not destroy pthread attributes.

Explanation: WebSEAL failed to delete pthread attributes.

Administrator response: Check available memory for the process.

DPWIV0471E pthread_rwlock_init() failed (*%d*)

Explanation: This message indicates a serious internal error involving the threading library.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV0750E Could not unlink file (*%s*, *%d*)

Explanation: Unable to remove the file used to store the process ID (PID) of the server (typically WebSEAL). This file is used when WebSEAL is started to detect if WebSEAL is already running. Only one process per instance of WebSEAL can be running.

Administrator response: Remove the file by hand. Check the permissions and ownership of the directory where the file is stored to ensure the server can update it. Check the error number returned for greater details of the cause. It can be looked up in /usr/include/sys/errno.h.

DPWIV0752E Could not open file (*%s*, *%d*)

Explanation: Unable to open the file specified in the error text. This error message is only used internally by WebSEAL and some test programs.

Administrator response: The error number specified in the error text gives more details. It can be looked up in /usr/include/sys/errno.h.

DPWIV0753E Error resetting file pointer (*%d*)

Explanation: An attempt to setup for reading or writing a file from the start failed. This file is being used to supply content for a local junction.

Administrator response: This is unexpected and if it persists should be reported to technical support. The error number in this message can be looked up in /usr/include/sys/errno.h for additional details on the cause.

DPWIV0754E Could not close file (*%d*)

Explanation: Closing a file used for supplying content for a local junction failed.

Administrator response: This is unexpected and if it persists should be reported to technical support. The error number in this message can be looked up in /usr/include/sys/errno.h for additional details on the cause.

DPWIV0755E Could not truncate file (*%d*)

Explanation: Truncating a file in a local junction failed.

Administrator response: This is unexpected and if it persists should be reported to technical support. The error number in this message can be looked up in /usr/include/sys/errno.h for additional details on the cause.

DPWIV0756E Could not deallocate file descriptor *%d*. (errno: *%d*)

Explanation: Unable to close unused file handles in child CGI process.

Administrator response: This is unexpected and if it persists should be reported to technical support. The error number in this message can be looked up in /usr/include/sys/errno.h for additional details on the cause.

DPWIV0759W Directory (*%s*) could not be created. (Errno = *%d*)

Explanation: Unable to create the directory specified in the error message. The directory is created to store content from a PUT HTTP request.

Administrator response: This may be due to lack of disk space or permissions on parent directories. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0760W The specified path is invalid. (*%s*)

Explanation: The path specified to the DELETE HTTP request is not valid on the local junction.

Administrator response: Correct the HTTP URL to contain a valid path on the local junction.

DPWIV0761W The file (*%s*) attributes cannot be obtained. (Errno = *%d*)

Explanation: Unable to fetch information on the file specified in the error message. This file is possibly going to be the target of a HTTP PUT request.

Administrator response: This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0762W Can't delete non-empty directory (*%s*)

Explanation: This is only used as an internal status. It occurs either during a PUT or DELETE HTTP request when the replaced or deleted directory is not empty.

Administrator response: Don't PUT or DELETE on this directory until it is empty.

DPWIV0763W Failed to delete file (*%s*) (Errno = *%d*)

Explanation: A HTTP PUT or DELETE request is either replacing or deleting a file on a local junction. This failed.

Administrator response: This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0764E Could not rename file (*%s*, *%s*, *%d*)

Explanation: Unable to rename/move the file to the destination. This is done in response to a HTTP DELETE request when the delete files are to be archived.

Administrator response: This may be due to permissions on the source or destination file or their directories. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0766W Write to file (*%s*) failed. (Errno = *%d*)

Explanation: The server failed to write to an open file.

Administrator response: This may be due to permissions on the file or because there is insufficient room in the file system. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0767E List of directory (*%s*) failed. (Errno = *%d*)

Explanation: A system error occurred while trying to read a directory's contents.

Administrator response: Examine the directory specified and attempt to determine and correct the problem that caused the system error.

DPWIV0768E Could not copy file (*%s*, *%s*, *%d*)

Explanation: Unable to copy the file to the destination. The source of this error depends on the context of the operation that failed.

Administrator response: This may be due to permissions on the source or destination file or their directories. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0769W Read from file (*%s*) failed. (Errno = *%d*)

Explanation: The server was unable to read from the file specified.

Administrator response: This may be due to permissions on the file. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV0770W Could not close file (*%s*). (Errno = *%d*)

Explanation: The server was unable to close an open file.

Administrator response: This may be due to insufficient file system space. For more details on the cause lookup the errno in /usr/include/sys/errno.h

DPWIV1050E Could not create socket: ERRNO = *%d*

Explanation: WebSEAL failed to create a socket for connections to junctions, or failed to create the listening sockets for HTTP and HTTPS connections from client browsers.

Administrator response: Check WebSEAL has not exceeded system resource limits. For more details on the cause lookup the errno in /usr/include/sys/errno.h.

DPWIV1051E Could not bind socket to port (*%d*, *%d*)

Explanation: WebSEAL failed to bind a socket to the HTTP or HTTPS port specified in it's configuration file.

Administrator response: Check WebSEAL has not exceeded system resource limits. Check the port numbers are valid in the WebSEAL configuration file. Check these ports don't clash with other servers on the same system. For more details on the cause lookup the errno in /usr/include/sys/errno.h.

DPWIV1052E Could not bind socket to port *%d*, interface *%s* (errno *%d*)

Explanation: WebSEAL failed to bind a socket to the HTTP or HTTPS port specified in it's configuration file on a specific network interface address.

Administrator response: Check WebSEAL has not exceeded system resource limits. Check the port numbers and interface addresses are valid in the WebSEAL configuration file. Check these ports don't clash with other servers on the same system. For more details on the cause lookup the errno in /usr/include/sys/errno.h.

DPWIV1053E Cannot understand requested network interface *%s*

Explanation: WebSEAL failed to validate the HTTP or HTTPS network interface address specified in its configuration file.

Administrator response: Check the interface addresses are valid in the WebSEAL configuration file.

DPWIV1054E Could not connect

Explanation: WebSEAL was unable to connect to a junctioned Web server.

Administrator response: Check that the host name and port number specified for the junction are correct. Check that the junctioned Web server is available and responding.

DPWIV1055E Could not read from socket

Explanation: WebSEAL was unable to read from a junctioned Web server, or from a browser. The browser or Web server may have closed the connection prematurely.

Administrator response: Retry the operation, the error condition may be temporary. If the error reoccurs check log files for related messages. Verify that the browser or junctioned Web server is functioning properly.

DPWIV1056E Could not write to socket

Explanation: WebSEAL was unable to write to a junctioned Web server, or to a browser. The browser or Web server may have closed the connection prematurely.

Administrator response: Retry the operation, the error condition may be temporary. If the error reoccurs check log files for related messages. Verify that the browser or junctioned Web server is functioning properly. If this occurs when WebSEAL is writing to a junctioned Web server, try sending the request to the junctioned Web server directly and examine the response from the server.

DPWIV1057E Could not close socket (errno *%d***)**

Explanation: WebSEAL encountered an error when attempting to close a socket.

Administrator response: No action required.

DPWIV1058E Could not call select() on socket

Explanation: WebSEAL encountered an error while using the select function on a socket.

Administrator response: No action required.

DPWIV1059E Timeout occurred while attempting to read from socket

Explanation: A timeout occurred when WebSEAL was attempting to read from a socket.

Administrator response: No action required.

DPWIV1060E Could not read from socket (*%d***)**

Explanation: A timeout occurred when WebSEAL was attempting to read from a socket.

Administrator response: No action required.

DPWIV1061E Could not write to socket (*%d***)**

Explanation: An unexpected error occurred while writing to a socket.

Administrator response: No action required.

DPWIV1062E Unable to resolve IP address for hostname '*%s***' (Error** *%d***:** *%s***)**

Explanation: An attempt to resolve a hostname to an IP address failed. There are many possible reasons for failure, and the system error code and error text can be used to isolate the problem.

Administrator response: The source for this error depends on the exact context of the error. Administrators should verify that the hostname specified is correct, and that DNS can resolve the hostname properly. Check the DNS configuration the server logging this error. The system error code and error text may provide more detail about the problem.

DPWIV1063E Unable to resolve IP address for hostname.

Explanation: An attempt to resolve a hostname to an IP address failed.

Administrator response: Check the logs for additional error messages. Other messages will contain more detail about the problem.

DPWIV1064E Could not set socket options (*%d***)**

Explanation: There was a failure in setting socket options.

Administrator response: Check that WebSEAL has not exceeded system resource limits. For more details on the cause, lookup the errno in /usr/include/sys/errno.h.

DPWIV1065E Could not get socket options (*%d***)**

Explanation: There was a failure trying to get socket options.

Administrator response: Check that WebSEAL has not exceeded system resource limits. For more details on the cause, look up the errno in /usr/include/sys/errno.h.

DPWIV1066E Could not obtain the socket details: ERRNO = *%d*

Explanation: WebSEAL failed to obtain the connection details for a connected socket.

Administrator response: Check WebSEAL has not exceeded system resource limits. For more details on the cause lookup the errno in /usr/include/sys/errno.h.

DPWIV1200E Could not write to SSL connection

Explanation: This is used only as an internal error code. It should not be visible.

Administrator response: No action required.

DPWIV1201E Could not read from SSL connection

Explanation: This is used only as an internal error code. It should not be visible.

Administrator response: No action required.

DPWIV1203E Could not create new SSL connection

Explanation: This is used only as an internal error code. It should not be visible.

Administrator response: No action required.

DPWIV1210W Function call, *func***, failed error:** *error code error text***.**

Explanation: The specified GSKit function failed while setting up for SSL connections to junctions or from browsers. Or perhaps the initial handshake failed due to invalid certificates or the browser simply closed the connection abruptly.

Administrator response: Examine the error text to gain insite on the problem. Typical problems might be that the PKCS#11 library is incorrectly specified, or the

PKCS#11 token or token password is incorrect, or the PKCS#11 token is not setup.

DPWIV1212W No server DN is defined for '*%s*'. The junctioned server DN verification is not performed.

Explanation: No server DN is defined in the junction database. DN verification against server certificate will be ignored.

Administrator response: Recreate the junction specifying the junctioned servers certificate DN or turn off mutual authentication on the junction.

DPWIV1213E Could not get junctioned server (*%s*) certificate

Explanation: The SSL connection to the specified junction did not have a certificate presented from the junctioned server.

Administrator response: Check the server side's certificate has been configured.

DPWIV1214E Could not get junctioned server (*%s*) certificate's DN

Explanation: See message.

Administrator response: Check the junctioned server is presenting a certificate that has a printable DN present

DPWIV1215E Error in junctioned server DN verification (*%s*)

Explanation: The DN in the certificate presented by the junctioned server contains a DN that does not match the one specified when the junction was created.

Administrator response: Check the junctioned server's DN with the one specified during the junction creation.

DPWIV1216E The junctioned server presented an invalid certificate.

Explanation: The certificate presented by the backend server failed validation.

Administrator response: Install the CA root certificate in the WebSEAL certificate key database.

DPWIV1217W SSL connection error.

Explanation: This is an internal error status not visible. Error code returned when an ssl connection failed

Administrator response: Check logs for more details.

DPWIV1218E Error in junctioned server DN verification.

Explanation: The DN specified when the junction was created did not match the DN in the certificate presented by the server.

Administrator response: Check the junctioned server's DN with the one specified during the junction creation.

DPWIV1219E An SSL toolkit failure occured while calling *%s*. Error: *%s*.

Explanation: An internal SSL error occurred.

Administrator response: The action to correct this problem depends on details in the error message.

DPWIV1220E An ICC toolkit failure occurred.

Explanation: An internal ICC error occurred.

Administrator response: This error is always accompanied with a serviceability log error message detailing the ICC routine which failed and the reason for the failure. The action to correct this problem depends on details in the serviceability log message. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV1221E An ICC toolkit failure occurred while calling *%s*. Error: *%s*.

Explanation: An internal ICC error occurred.

Administrator response: The action to correct this problem depends on details in the error message. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV1222E An ICC toolkit failure occurred while calling *%s*. No further details are known.

Explanation: An internal ICC error occurred. However, no details about the error we able to be determined beyond the name of the ICC function which failed.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWIV1350E An error occurred when loading a shared library.

Explanation: This message indicates that a problem occurred when loading a shared library. Other log messages will have additional information.

Administrator response: Examine log files for more detailed error messages.

DPWIV1351E The shared library '*%s*' could not be loaded because of system error code *%d*. System error text: *%s*.

Explanation: Opening a shared library failed. The shared library may not exist, permissions on the library may be incorrect, or it may contain other errors that prevent it from loading.

Administrator response: Examine the system error code and text to determine the nature of the problem. Make sure the shared library exists and is readable. Make sure all of the symbols in the library can be resolved.

DPWIV1352E The symbol '*%s*' in the shared library '*%s*' could not be loaded because of system error code *%d*. System error text: *%s*.

Explanation: Resolving a symbol from a shared library failed after the library was initially loaded. The symbol may not exist in the library or other symbols on which this symbol depends might not be available.

Administrator response: Examine the system error code and text to determine the nature of the problem. Make sure the shared library implements and exports the function being resolved. Make sure all of the symbols required by the shared library can be resolved.

DPWNS0150E Process can't access directory '*%s*', error: 0x*%8.8lx*

Explanation: The process is trying to change it's working directory

Administrator response: Check the UID running the process has the correct permissions

DPWNS0165E The certificate revocation check result was undetermined. The subject issuer is '*%s*'.

Explanation: An OCSP CRL check could not determine if the certificate is revoked. This is usually due to an unresponsive OCSP responder.

Administrator response: Check the OCSP responder is operating.

DPWNS0166E The junction server, '*%s*', certificate revocation check result was undetermined. The subject issuer is '*%s*'.

Explanation: An OCSP CRL check could not determine if the junctions certificate is revoked. This is usually due to an unresponsive OCSP responder.

Administrator response: Check the OCSP responder is operating.

DPWNS0301W Junction server '*%s*:*%d*' is renegotiating SSL sessions at a rate of *%ld* per minute.

Explanation: The SSL server junctioned behind WebSEAL is forcing WebSEAL to renegotiate new SSL Sessions at a rate higher than specified by [junction] jct-ssl-reneg-warning-rate.

Administrator response: Ensure the junctioned SSL server has SSL session caching enabled and functioning correctly, or check that any intervening load balancers are not causing this issue by forcing WebSEAL to alternate between two SSL servers.

DPWNS0450E The pattern '*%s*' is not a valid MIME type matching pattern.

Explanation: MIME type patterns must be either exact (type/subtype), subtype wild cards (type/*), or type and subtype wildcards (*/*).

Administrator response: Make sure the mime type specified is valid.

DPWNS0451E Invalid MIME matching pattern.

Explanation: Mime type patterns must be either exact (type/subtype), subtype wild cards (type/*), or type and subtype wildcards (*/*).

Administrator response: Make sure the mime type specified is valid.

DPWNS0452E Invalid MIME type '*%s*'.

Explanation: An attempt was made to lookup a match for a MIME type that did not contain a '/'.

Administrator response: Check the MIME type configuration of your servers to verify that they are returning valid MIME types for all documents.

DPWNS0453E Invalid MIME type.

Explanation: An attempt was made to lookup a match for a MIME type that did not contain a '/'.

Administrator response: Check the MIME type configuration of your servers to verify that they are returning valid MIME types for all documents.

DPWNS0600E Compression initialization failed with error code *%d* (*%s*).

Explanation: Initialization of compression failed. This error should never occur.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS0601E Compression failed with error code *%d* (*%s*).

Explanation: Compression of a document failed. This error should never occur.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS0602E Completion of compression failed with error code *%d* (*%s*).

Explanation: The completion of document compression failed. This error should never occur.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS0603E An error occured during document compression.

Explanation: This error is returned when a problem was encountered during document compression.

Administrator response: Examine log files for additional information.

DPWNS0750E The HTTP header key '*%d*' is invalid.

Explanation: This message indicates an internal error. An attempt was made to reference an HTTP header using an invalid key.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS0900E The client certificate EAI request failed: *%s* (0x*%lx*)

Explanation: This error is returned when the EAI request which has been generated by WebSEAL does not return a valid HTTP response.

Administrator response: Examine log files for additional information.

DPWNS0901E No EAI authentication data was provided with the EAI response.

Explanation: This error is returned when the EAI response lacks all of the configured EAI authentication headers.

Administrator response: Examine the log files for additional information. Check the EAI application to ensure that valid authentication headers are being set.

DPWNS1050E Session cache creation failed.

Explanation: This message can indicate a failure due to system resource limitations.

Administrator response: Check available system memory and process resource usage limits.

DPWNS1051E Addition or update of a session cache entry failed.

Explanation: This message indicates an internal error.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1052W A session cache entry was not found.

Explanation: This message indicates that an expected session cache entry was not found.

Administrator response: No action is necessary unless other problems are experienced.

DPWNS1053E Session owner tracking is not supported in this configuration.

Explanation: This message indicates that an attempt was made to get a list of the sessions associated with a user when session owner tracking was not enabled.

Administrator response: Refer to the WebSEAL Administration Guide for instructions on how to enable tracking of session owners.

DPWNS1054E Invalid session ID.

Explanation: This message indicates that an invalid session ID was encountered when trying to generate an internal representation of the ID. The most likely cause of this error is a malformed session cookie from a browser.

Administrator response: No action is necessary. A new session and session cookie is created as needed.

DPWNS1055E You are already logged in from another client. You can either wait for the other login to end or contact your local support personnel to cancel the existing login.

Explanation: This message indicates that the maximum number of concurrent sessions for the user has been reached and no new sessions will be permitted until one of the existing sessions has ended.

Administrator response: Refer to the WebSEAL Administration Guide discussion of concurrent login sessions for more complete information.

DPWNS1056W You are already logged in from another client. Do you want to terminate your existing login or cancel this new login request?

Explanation: This message indicates that the maximum number of concurrent sessions for the user has been reached, and that the user can choose to replace an existing session.

Administrator response: The action depends on the reason for the previous session. If the user closed their browser without properly logging out or does not need their old session, they can press the 'Terminate existing login' button. If the user does need their old session, they should press the 'Cancel this new login' button.

DPWNS1057E Unable to intialize the distributed session API (error code 0x*%08lx***)**

Explanation: Initialization of the distributed session API failed. This error should never occur. The error code in the message might reveal more information about the problem.

Administrator response: Look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide.

DPWNS1058E Unable to join the replica set '*%s***' (error code 0x***%08lx***)**

Explanation: The WebSEAL server attempted to join a particular replica set but the operation failed. The SMS might not be available, or may have prevented the WebSEAL server from joining the replica set for some reason.

Administrator response: Make sure the correct protocol, host name, and port for the SMS in the WebSEAL configuration file are correct. Make sure the SMS server is running and can be reached from the WebSEAL server machine. Make sure the SMS server is configured to host the specified replica set. Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWNS1059E Unable to shut down the distributed session API (error code 0x*%08lx***)**

Explanation: Shutdown of the distributed session API failed. This error should never occur. The error code in the message might reveal more information about the problem.

Administrator response: Look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide.

DPWNS1060E Unable to leave the replica set '*%s***' (error code 0x***%08lx***)**

Explanation: The WebSEAL server attempted to leave a particular replica set but the operation failed. The SMS might not be available or there might have been another problem when leaving the replica set.

Administrator response: Look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide.

DPWNS1061E An attempt to create a session failed with error code 0x*%08lx***.**

Explanation: An attempt to create a session at the SMS failed.

Administrator response: Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1062E An attempt to update a session failed with error code 0x*%08lx***.**

Explanation: An attempt to update a session at the SMS failed.

Administrator response: Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1063E An attempt to delete a session failed with error code 0x*%08lx***.**

Explanation: An attempt to delete a session at the SMS failed.

Administrator response: Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Access

Manager for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1064E Unknown replica set '*%s*'

Explanation: An attempt was made to locate a replica set that was not configured.

Administrator response: Check that the replica set requested is included in the WebSEAL configuration file as a replica set that the WebSEAL server should join.

DPWNS1065E Unknown replica set.

Explanation: An attempt was made to locate a replica set that was not configured.

Administrator response: Check that the replica set requested is included in the WebSEAL configuration file as a replica set that the WebSEAL server should join.

DPWNS1066E An error with code 0x*%08lx* occurred when decoding a session from the SMS.

Explanation: An attempt to decode a session from the SMS failed.

Administrator response: Look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide.

DPWNS1067E An attempt to generate a new external session ID failed with error code 0x*%08lx*.

Explanation: An attempt to generate a new external session ID for a session failed.

Administrator response: Repeat the operation. If the problem continues to occur, look up the error code included in the message in the IBM Security Access Manager for Web Troubleshooting Guide. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1068E An attempt to register an authentication failure for user '*%s*' failed with status code 0x*%08lx*.

Explanation: An attempt to notify the SMS of an authentication failure was unsuccessful.

Administrator response: Check the log file for additional errors. If necessary, look up the error code from the message in the IBM Security Access Manager for Web Troubleshooting Guide for additional troubleshooting steps.

DPWNS1070E Session version mismatch while deserializing session data.

Explanation: WebSEAL attempted to deserialize session data but encountered an invalid session version. This indicates that the session was not compatible with the WebSEAL server that generated this error. The session was discarded.

Administrator response: No action is necessary. A new session will be created as needed. Refer to the documentation for the server that generated the invalid session version for information on compatibility with the WebSEAL server that generated this error.

DPWNS1071E The max-concurrent-web-sessions policy value of '*%d*' is invalid.

Explanation: The max-concurrent-web-sessions policy returned from the IBM Security Access Manager Runtime had an unexpected value. A default value of 'unlimited' has been assumed.

Administrator response: Reset the max-concurrent-web-sessions policy for the user. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWNS1072W WebSEAL received notification that the distributed session cache for replica-set '*%s*' was cleared. All local references to sessions are being discarded to synchronize the local session cache with the distributed session cache.

Explanation: The DSC server notified the WebSEAL server that the distributed session cache was lost. Any sessions remaining on the WebSEAL server are no longer valid and will be removed. This message will also be displayed when the WebSEAL server first regains contact with the DSC server after WebSEAL is restarted.

Administrator response: No action is necessary.

DPWNS1074E The single sign-off attempt for the user '*%s*' failed because the single sign-off resource is unavailable.

Explanation: The single sign-off attempt failed because the configured single sign-off resource is not accessible by WebSEAL.

Administrator response: Check that the configured single sign-off resource URI points to a resource on a junction which is accessible by WebSEAL.

DPWNS1075E The single sign-off attempt to *%s* for user '*%s*' failed because the configured single sign-off resource is not responding.

Explanation: A single sign-off request was sent to the configured single sign-off resource but no response was received.

Administrator response: Check that the configured single sign-off application is running and functioning correctly.

DPWNS1076E The single sign-off attempt to *%s* for user '*%s*' failed because the configured single sign-off resource returned a response with the HTTP status code *%d*.

Explanation: An unexpected response was received from the configured single sign-off resource. WebSEAL expects a response with the HTTP status code 200.

Administrator response: Check that the configured single sign-off application is running and functioning correctly.

DPWNS1200W The application server you are accessing has been taken offline by the system administrator.

Explanation: The application server being accessed has been taken offline or throttled by the system administrator.

Administrator response: Try again at a later time or contact the system administrator for more information.

DPWNS1201E The server is temporarily unable to service your request. Try again later.

Explanation: The WebSEAL server is unable to service a request because a needed resource is unavailable.

Administrator response: The WebSEAL server log file will have more detailed information about why the WebSEAL server is unable to service the request. Check the WebSEAL server log file and correct the problem.

DPWNS1202E An error occurred processing a HTTP transformation.

Explanation: The WebSEAL server is unable to service a request because a HTTP transformation rule caused an error.

Administrator response: The WebSEAL server log file will have more detailed information about why the HTTP transformation failed. Check the WebSEAL server log file and correct the HTTP transformation rule.

DPWNS1203E An invalid XML message document was used as part of a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an invalid XML message document was used as part of a HTTP transformation operation.

Administrator response: The WebSEAL server log file will have more detailed information about the XML object used. Check the WebSEAL server log file and correct the HTTP transformation rule.

DPWNS1204E The XML element *%s* was missing from the document generated by a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an expected XML element was missing from the output document of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1205E The XML attribute *%s* was missing from the *%s* element for the document generated by a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an expected XML attribute was missing from the output document of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1206E The XML element *%s* was missing from the request change document generated by a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an expected XML element was missing from the request change document as part of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1207E The XML element *%s* was missing from the response change document generated by a HTTP transformation operation.

Explanation: The WebSEAL server is usable to service a request because an expected XML element was missing from the response change document as part of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule to ensure the rule includes all required elements.

DPWNS1208E The action attribute *%s* is unknown and therefore cannot be used by a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an unexpected action attribute was found as part of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule to ensure the rule outputs supported actions.

DPWNS1209W A configuration entry for the resource *%s* was not defined in the http-transformation stanza of the WebSEAL configuration file and therefore HTTP transformation cannot take place.

Explanation: A HTTPTransformation resource was defined as an extended attribute on a POP but the WebSEAL configuration does not include a transformation rule for this resource.

Administrator response: Correct the WebSEAL configuration or the POP HTTPTransformation attribute to ensure the resource references an appropriate transformation rule.

DPWNS1210E The cookie attribute *%s* is unknown and therefore cannot be used by a HTTP transformation operation.

Explanation: The WebSEAL server is unable to service a request because an unexpected cookie attribute was found as part of a HTTP transformation operation.

Administrator response: Correct the HTTP transformation rule so that it does not reference unsupported cookie attributes.

DPWNS1211W The cookie *%s* already exists in the HTTP message and as such it cannot be added by the transformation rule.

Explanation: The WebSEAL server is unable to add a cookie to a HTTP message as it already exists in the HTTP message being transformed.

Administrator response: Modify the HTTP transformation so that it either checks for the existence of the cookie before adding the new cookie, or specifies the update action so that the cookie is updated.

DPWNS1212W The authentication challenge type rules could not be applied because WebSEAL received a request without the User-Agent HTTP header.

Explanation: A client which did not present a User Agent header in their request has made a request to authenticate with WebSEAL. WebSEAL was unable to determine the authentication challenge type for this request.

Administrator response: No action required.

DPWNS1350W Failed to load ARM library '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled.

Explanation: WebSEAL attempted to dynamically load the ARM shared library and failed.

Administrator response: Check the shared library name is correct and present on the system. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza. If loading the ARM library is not desired set enable = no under the [arm] stanza.

DPWNS1351W ARM library is missing function '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled.

Explanation: WebSEAL dynamically loaded the ARM shared library and can not find a required function in it.

Administrator response: Check the shared library name is correct. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza.

DPWNS1352W Failed to register the WebSEAL application with ARM: error code *%d*: error message '*%s*'. ARM support will be disabled.

Explanation: WebSEAL was unable to register itself with ARM.

Administrator response: Check ARM setup is operational. Refer to the error message for more specific information.

DPWNS1353W Failed to register WebSEAL transaction '*%s*' with ARM: error code *%d*: error message '*%s*'. ARM support will be disabled.

Explanation: WebSEAL was unable to register the transaction with ARM.

Administrator response: Check ARM setup. Refer to the error message for more specific information.

DPWNS1354W Failed to start WebSEAL as an ARM application: error code *%d***: error message '***%s***'. ARM support will be disabled.**

Explanation: WebSEAL was unable to start as an ARM application.

Administrator response: Check ARM setup. Refer to the error message for more specific information.

DPWNS1356W Failed to stop WebSEAL running as an ARM application: error code *%d***: error message '***%s***'.**

Explanation: WebSEAL was unable to stop running as an ARM application using arm_stop_application().

Administrator response: Refer to the error message for more specific information.

DPWNS1357W Failed to unregister the WebSEAL application from ARM: error code *%d***: error message '***%s***'.**

Explanation: WebSEAL was unable to unregister as an ARM application using arm_destroy_application().

Administrator response: Refer to the error message for more specific information.

DPWNS1358W Failed to get ARM transaction '*%s***' arrival time: error code** *%d***: error message '***%s***'.**

Explanation: The call to ARM function arm_get_arrival_time() failed unexpectedly. The transaction will not be reported.

Administrator response: Refer to the error message for more specific information.

DPWNS1359W Failed to get the length of an ARM correlator: error code *%d***: error message '***%s***'.**

Explanation: The call to ARM function arm_get_correlator_length() failed unexpectedly. The correlator will not be used.

Administrator response: Refer to the error message for more specific information.

DPWNS1360W An invalid correlator string was passed to WebSEAL: '*%s***'. It will not be used for subsequent transactions.**

Explanation: An ARMCorrelator header was received by WebSEAL with an invalid value.

Administrator response: Check the application making the request to WebSEAL. Or disable WebSEAL from using incoming ARM Correlator by setting accept-correlators = no in the [arm] stanza.

DPWNS1361W Failed to start ARM transaction '*%s***': error code** *%d***: error message '***%s***'. The transaction will not be reported.**

Explanation: The call to ARM function arm_start_transaction() failed unexpectedly. The transaction will not be reported.

Administrator response: ARM can limit the number of concurrent transactions being reported. It may be possible to increase the limit. Also refer to the error message for more specific information.

DPWNS1362W Failed to stop ARM transaction '*%s***': error code** *%d***: error message '***%s***'.**

Explanation: The call to ARM function arm_stop_transaction() failed unexpectedly.

Administrator response: Refer to the error message for more specific information.

DPWNS1363W Unable to start ARM transaction reporting as ARM initialization failed. See log files for more information.

Explanation: The 'arm on' command cannot complete as the ARM initialization failed.

Administrator response: Examine the log files for the reason ARM initization failed. Correct this, restart WebSEAL and try again.

DPWNS1364W Unable to start ARM transaction reporting as WebSEAL ARM support has been disabled.

Explanation: The 'arm on' command cannot complete as the WebSEAL ARM support has been disabled in the configuration file.

Administrator response: To enable ARM support set enable = yes in the [arm] stanza and restart WebSEAL.

DPWNS1365W ARM transaction reporting is already on.

Explanation: The 'arm on' command is redundant and will be ignored as arm transaction reporting is already on.

Administrator response: Don't run the 'arm on' command while transaction reporting is on.

DPWNS1366W ARM transaction reporting is already off.

Explanation: The 'arm off' command is redundant and will be ignored as arm transaction reporting is already off.

Administrator response: Don't run the 'arm off' command while transaction reporting is off.

DPWNS1367W Failed to load ARM library '*%s*': error code *%d*: error message '*%s*'. ARM support will be disabled.

Explanation: WebSEAL attempted to dynamically load the ARM shared library and failed.

Administrator response: Check the shared library name is correct and present on the system. Refer to the error message for more specific information. The shared library name is specified by the library entry under the [arm] stanza. If loading the ARM library is not desired set enable-arm = no under the [arm] stanza.

DPWNS1368W Unable to start ARM transaction reporting as WebSEAL ARM support has been disabled.

Explanation: The 'arm on' command cannot complete as the WebSEAL ARM support has been disabled in the configuration file.

Administrator response: To enable ARM support set enable-arm = yes in the [arm] stanza and restart WebSEAL.

DPWNS1500E The interface '*%s*', defined in the [*%s*] stanza, contains an invalid value for '*%s*'. You must specify either 'http' or 'https'.

Explanation: The web-http-protocol and web-https-protocol interface settings can only contain 'http' or 'https'.

Administrator response: Set the value to either 'http' or 'https'

DPWNS1501E The option '*%s*', defined in the [*%s*] stanza, contains an invalid value. You must specify either 'http' or 'https'.

Explanation: The web-http-protocol and web-https-protocol settings can only contain 'http' or 'https'.

Administrator response: Set the value to either 'http' or 'https'

DPWNS1502E The option '*%s*' defined in the [*%s*] stanza contains an invalid port value.

Explanation: The port value provided is either out of the valid range, or is not a number.

Administrator response: Provide a valid value for a TCP/IP port in the range 1 to 65535.

DPWWA0150E Cannot allocate memory

Explanation: Memory allocation operation failed.

Administrator response: Check memory limits on your machine, and increase available memory if possible.

DPWWA0151E An insufficient amount of memory was supplied.

Explanation: An insufficient amount of memory was passed into a function.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA0305E The '*%s*' routine failed for '*%s*', errno = *%ld*

Explanation: This is a major internal server failure. An internal function call failed.

Administrator response: Contact customer support.

DPWWA0306E Error in configuration file: *%s*

Explanation: The configuration file contained an error.

Administrator response: Edit the configuration file to correct the error.

DPWWA0308W Function *name* failed with errno *value*

Explanation: This is a generic message used to identify specific non-fatal function calls failing.

Administrator response: Determine why the function call failed.

DPWWA0309E Badly formatted config entry for *%s* cache

Explanation: The configuration defined in the [content-cache] stanza was incorrect.

Administrator response: Correct the values in the [content-cache] stanza of the configuration file.

DPWWA0310E Could not open IBM Security Access Manager WebSEAL configuration file (*%s*)

Explanation: See message.

Administrator response: Correct problem preventing configuration file from being opened.

DPWWA0314E Initialization of authorization API failed. Major status=0x*%x*, minor status = 0x*%x*

Explanation: See message.

Administrator response: Look up the specified major/minor status codes either through the Error Message Reference Book or the pdadmin errtxt command. Analyze and fix the error based on that information.

DPWWA0315E Initialization of authentication layer failed: *%s*

Explanation: One of the authentication libraries failed to load.

Administrator response: Correct the entries for the authentication libraries in webseald.conf

DPWWA0316W Configuration item value has been assumed for *%s*

Explanation: The configuration item value did not make sense and a default value was assumed

Administrator response: Correct the configuration variable in webseald.conf

DPWWA0318E Error in configuration file, invalid accept-client-certs value: *%s*

Explanation: See message.

Administrator response: Correct the accept-client-certs parameter in webseald.conf

DPWWA0319E Error in configuration file. When accept-client-certs is set to optional or required, you must specify a library with the cert-ssl option, or you must specify an eai-uri option.

Explanation: See message.

Administrator response: Set the cert-ssl parameter in webseald.conf

DPWWA0320W Error in configuration. Clients and MPAs cannot use the same session types.

Explanation: Clients and MPAs cannot use the same session types.

Administrator response: Configure clients and MPAs to use different session types.

DPWWA0321E Value for stanza [*%s*] entry '*%s*' contains an illegal trailing backslash character.

Explanation: Backslash characters are used to remove any special meaning of the character following it. The end of line cannot be treated this way.

Administrator response: Remove the trailing \\ character from the the entries value.

DPWWA0322E Value for stanza [*%s*] entry '*%s*' contains an unmatched quote.

Explanation: Quote characters are used to allows values to have leading and trailing space characters. The values that have this requirement must have a quote at the begining and end of the region of chars. A unpaired quote is not legal unless its special meaning is removed using the backslash character.

Administrator response: Remove the unmatched " character from the the entries value or place a \\ char before it to remove its special meaning.

DPWWA0323E Value for stanza [*%s*] entry '*%s*' contains a 'name = value' with a missing name.

Explanation: Stanza entries of this type have a special format. This format consists of multiple name = value pairs separated by semicolon characters. In this case the name part of a pair is missing or empty.

Administrator response: Provide a name before the = character.

DPWWA0324E Value for stanza [*%s*] entry '*%s*' contains a 'name = value' with a missing = character.

Explanation: Stanza entries of this type have a special format. This format consists of multiple 'name = value' pairs separated by semicolon characters. In this case the = separating the pair is missing.

Administrator response: Insert the missing = character.

DPWWA0325E Value for stanza [*%s*] entry '*%s*' contains two name value pairs with the same name '*%s*'.

Explanation: Stanza entries of this type have a special format. This format consists of multiple 'name = value' pairs separated by semicolon characters. In this case there are two of these pairs with the same name. This is illegal as all names must be unique.

Administrator response: Remove or rename one of the name value pair with the duplicate name.

DPWWA0326E Stanza [%s] contains an illegal duplicate entry '%s'.

Explanation: This stanza expects entries with unique names.

Administrator response: Remove or rename one of the entry names.

DPWWA0327W The default WebSEAL TCP and SSL interfaces have both been disabled, which also disables the default WebSEAL worker threads.

Explanation: When both the default WebSEAL interfaces are disabled using [server] https = no and http = no the default worker threads are also not created. This will make WebSEAL unaccessable unless additional interfaces are defined under [interfaces] stanza. Note that these additional interfaces will not be able to share the 'default' worker threads as they will not have been created.

Administrator response: No action required, it just an unusual situation.

DPWWA0328E The interface '%s' defined in the [%s] stanza contains an illegal empty value for '%s'.

Explanation: The worker threads setting in the configuration of an interface must be set to either the number of worker threads to create, or the name of another interface to share worker threads with. Typically this entry will look like 'worker-threads = 50'

Administrator response: Supply a non-empty value for worker-threads.

DPWWA0329E The interface '%s' defined in the [%s] stanza contains an illegal value for '%s'.

Explanation: The worker threads setting in the configuration of an interface must be set to either the number of worker threads to create, or the name of another interface to share worker threads with. Typically this entry will look like 'worker-threads = 50'

Administrator response: Provide the name of an interface that has it's own worker threads or provide the number of worker threads it should create for itself.

DPWWA0330E The interface '%s' defined in the [%s] stanza contains an invalid value for '%s'.

Explanation: The port value provided is either out of the legal range or is not a number.

Administrator response: Provide a legal value for a TCP/IP port in the range 1 to 65535.

DPWWA0331E The interface '%s' defined in the [%s] stanza contains an illegal TCP/IP address value for '%s'.

Explanation: The TCP/IP value provided is either 255.255.255.255 or not a valid string for an TCP/IP address

Administrator response: Provide a legal value for a TCP/IP port.

DPWWA0332E Invalid certificate authentication configuration for interface '%s' defined in the [%s] stanza. Incompatible combination of accept-client-certs and ssl-id-sessions values.

Explanation: See message.

Administrator response: Change the accept-client-certs or ssl-id-sessions parameter in webseald.conf.

DPWWA0333E Invalid certificate cache configuration to support interface '%s' defined in the [%s] stanza.

Explanation: See message.

Administrator response: Change the values of the certificate cache configuration items.

DPWWA0334E Error in configuration file, invalid accept-client-certs value: %s for interface '%s' defined in the [%s] stanza.

Explanation: See message.

Administrator response: Correct the accept-client-certs parameter in webseald.conf

DPWWA0335E Error in configuration file relating to interface '%s' defined in the [%s] stanza. When accept-client-certs is set to optional, required, or prompt_as_needed, specify a library with the cert-ssl option or the eai-uri option.

Explanation: See message.

Administrator response: Set the cert-ssl parameter in webseald.conf

DPWWA0336E The interface '%s' defined in the [%s] stanza must have one of http-port or https-port enabled.

Explanation: An interface has no function unless at least one port is defined.

Administrator response: Assign a port to either or both of http-port or https-port.

DPWWA0337W The '*%s*' routine failed in '*%s*' for interface *%s*:*%d*, errno = *%d*

Explanation: A non-fatal error was reported from the specified function, called in a specified function in relation to the specified interface and port. The system error code is given to help diagnose the reason. WebSEAL will continue to function. Typically this occurs when a connection from a browser is ended abnormally.

Administrator response: Keep an eye on this and if this occurs too often contact WebSEAL customer support.

DPWWA0338E Not enough free file descriptors in the process to configure even one of the worker threads wanted by the worker pool named '*%s*'.

Explanation: Each interface defined can have it's own worker thread pool. If previous definintions have consumed all available resources in creating their own worker thread pools then there may be nothing left for this interface. Each worker thread requires 2 file descriptors. The number of available file descriptors is dependent on the Operating System WebSEAL is run on and is fixed when WebSEAL is constructed.

Administrator response: Reduce the number of worker threads used by other worker pools.

DPWWA0339W Worker list '*%s*' has configured *%d* worker threads which is greater than the system can support. It has automatically been reduced to *%d*.

Explanation: Each operation system has different levels of support for threads and open files. That combined with compile time options will provide limits on the configurable number of worker threads.

Administrator response: The software automatically reduced the value. However to stop this message appearing you may set the value in the configuration file lower.

DPWWA0340E Unable to listen on interface *%s*:*%d*, errno = *%d*

Explanation: The attempt to listen for connections on the specified interface and port failed. The system error code is given to help diagnose the reason.

Administrator response: It is likely the reason for failure is that another process or WebSEAL interface is already listening on the same port and network address. Change the port and/or network address to one not in use.

DPWWA0341E Error in configuration file, unknown setting '*%s*' for interface '*%s*' defined in the [*%s*] stanza.

Explanation: The interface has an unknown name=value pair in it's configuration. This could be due to a spelling error.

Administrator response: Remove the unknown setting in the WebSEAL configuration file

DPWWA0342W The configuration data for this WebSEAL instance has been logged in '*%s*'

Explanation: This is an informational message.

Administrator response: Informational. No action is required.

DPWWA0343E An error occurred trying to log the WebSEAL configuration data at startup.

Explanation: Check the server's error log file for specific error conditions that could have led to this failure. It is possible that there are permission issues with the configuration data log file or there are space limitations in the filesystem.

Administrator response: It is likely that logging the server's configuration data failed because the desired location for the log file is missing or was specified incorrectly in the server's configuration file.

DPWWA0345E The request was too large to store in the session cache.

Explanation: The request size exceeded request-max-cache or the message body exceeded request-body-max-read, so the request could not be stored in the session cache.

Administrator response: Re-submit the request after authentication or increase request-max-cache and/or request-body-max-read

DPWWA0600E The requested single sign-on service is not supported by this server

Explanation: Junction created with an SSO specification that the server was not built to support

Administrator response: Do not use the single-sign-on service specified by the junction definition

DPWWA0601E Could not fetch SSO info for user (*%s*,0x*%8lx*)

Explanation: Could not map from username/pwd to principal/target in SSO

Administrator response: Check mappings from principal/target to username/pwd in SSO

DPWWA0602E User '*%s*' does not have any associated SSO info

Explanation: SSO data either does not exist or is incorrect.

Administrator response: Check that SSO data for this user exists and is correct.

DPWWA0603E User '*%s*' does not have a matching SSO target

Explanation: The user was found in SSO, but no target exists for them.

Administrator response: Create a target in SSO for this user.

DPWWA0605E Can't perform single sign-on. User '*%s*' is not logged in

Explanation: User must be authenticated to use SSO.

Administrator response: Informative only. User must be logged in.

DPWWA0606E Could not sign user '*%s*' on due to incorrect target

Explanation: Could not sign user on due to incorrect target in SSO.

Administrator response: Check the target in SSO for this user

DPWWA0607E Received basic authentication challenge for junction where filtering is being applied

Explanation: The junction type filters out Basic Authentication data, but the junctioned server sent a BA challenge.

Administrator response: Either create the junction without the -filter flag or modify the junctioned server to not use Basic Authentication.

DPWWA0608E Unable to obtain binding to LDAP server

Explanation: Unable to obtain binding to LDAP server

Administrator response: Check that LDAP server is running and can be accessed.

DPWWA0609E Unable to obtain binding to LDAP-GSO server (0x*%8lx*)

Explanation: Unable to obtain binding to LDAP-GSO server

Administrator response: Check that LDAP-GSO server is running and can be accessed.

DPWWA0625E Either the configuration file is missing or it has errors.

Explanation: The iv.conf file is either missing, or the LDAP stanza does not have enough information to bind to the LDAP server.

Administrator response: Make sure that the configuration file has the ldap stanza and all the LDAP information is included in the stanza.

DPWWA0626E This script can only be used to decode form results.

Explanation: This error occurs when the user invokes the update password URL directly from the browser.

Administrator response: The user needs to invoke the cgi-bin program and change the password from the browser.

DPWWA0627E Could not get the LDAP distinguished name (DN) for the remote user.

Explanation: The ira_get_dn(), to get the distinguished name, failed.

Administrator response: Make sure that the LDAP entry is set for the remote user.

DPWWA0628E The selected resource or resource group does not exist.

Explanation: The user selected a resource or a resource group that does not exist in the LDAP database.

Administrator response: Make sure that the resource or the resource group exists for the user.

DPWWA0629E Could not bind to the LDAP server.

Explanation: The ira_rgy_init call failed. Contact your Administrator.

Administrator response: Make sure that the LDAP server can be reached and try again.

DPWWA0630E This script should be referenced with a METHOD of POST.

Explanation: This error occurs when the user invokes the update password URL directly from the browser.

Administrator response: The user needs to invoke the cgi-bin program and change the password from the browser.

DPWWA0631E Passwords don't match.

Explanation: The user attempted to change their GSO target password and failed to confirm the new password.

Administrator response: The user must correct their entries in the update password form, ensuring that the passwords match.

DPWWA0632E Unable to retrieve user identity.

Explanation: This error occurs because the REMOTE_USER cgi environment variable was not passed to the GSO chpwd program by WebSEAL.

Administrator response: Verify that the cgi-program is being invoked by WebSEAL and not called directly.

DPWWA0633E Either a user ID or a password must be specified.

Explanation: Either the user ID or a password must be specified to update the resource.

Administrator response: Enter the user ID or password and try again.

DPWWA0634E Select a resource or resource group.

Explanation: The required resource information was missing from the cgi form used to update a user's GSO target information.

Administrator response: The user must specify the proper resource information in the cgi form.

DPWWA0635E Completed successfully.

Explanation: Operation completed successfully.

Administrator response: No action required.

DPWWA0636E No TFIM single sign-on tokens were available.

Explanation: WebSEAL is correctly retrieving SSO tokens from TFIM, but these tokens have expired. The problem is most likely caused by the clocks on the WebSEAL server and the TFIM server being set to different times.

Administrator response: Check the time synchronization between the TFIM server and the WebSEAL server.

DPWWA1055E Operation has insufficient Quality of Protection

Explanation: This error occurs when a person tries to access an object that requires a secure communications channel over an insecure channel such as TCP.

Administrator response: Either access the object over SSL/TLS or modify the policy associated with the object to reduce the QOP required.

DPWWA1061E Provide your authentication details for method:

Explanation: This error is printed when a user attempts to access an object that requires a higher level of authentication than they have provided.

Administrator response: The user should either provide the higher level of authentication, or the policy associated with the object should be modified to reduce the level of authentication required.

DPWWA1062E An invalid authentication level has been detected in a POP object.

Explanation: A POP object specified an authentication level that is not supported by the current WebSEAL configuration.

Administrator response: Either modify the POP object to correct the authentication level, or modify the WebSEAL configuration file to specify an authentication method that can provide the required level.

DPWWA1076E Privacy required

Explanation: Indicates that requested object has the privacy bit set, but the request is not using privacy

Administrator response: The user must connect using privacy to access the resource.

DPWWA1082E Invalid HTTP status code present in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Explanation: An invalid status code was received in a response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response: Check the status code in the response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1083E Could not read HTTP status line in response. Possible causes: non-spec HTTP response, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Explanation: Data read failure. Possible causes: non-spec HTTP response, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response: Check response for a missing HTTP status line. Also investigate a possible connection timeout problem. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1084E Could not read HTTP headers in response. Possible causes: non-spec HTTP headers, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Explanation: Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response: Check response for bad HTTP headers. Also investigate a possible connection timeout problem. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1085E An HTTP message body sent in a response is too short. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Explanation: The actual length of the response body is shorter that indicated by the Content-length HTTP header in the response.

Administrator response: Correct problem with the response. The actual length of the response body is shorter that indicated by the Content-length HTTP header of the response.

DPWWA1086E Could not read request line. Possible causes: non-spec HTTP headers, connection timeout, no data returned

Explanation: Data read failure. Possible causes: non-spec HTTP data, connection timeout, no data returned

Administrator response: Check client request. Could contain bad HTTP headers or there might be a connection timeout problem.

DPWWA1087E Invalid URL

Explanation: A client request contained a URL that does not conform to HTTP specifications.

Administrator response: Check request from client. Does not conform to HTTP specifications.

DPWWA1088E Bad cookie header (or data read failure)

Explanation: Data read failure. Possible causes: timeout, connection problems, no data returned

Administrator response: Check response from either junctioned server or client. Could be bad Cookie header, Set-cookie header or a connection timeout problem.

DPWWA1089E Invalid date string in HTTP header

Explanation: Invalid date string in HTTP header in client request.

Administrator response: Check request from client. Contains invalid date string in HTTP header.

DPWWA1091W Failed to load portal map (0x*%8lx*)

Explanation: The portal service failed to load correctly due to a problem with the information in the [portal-map] stanza of the configuration file.

Administrator response: Correct errors in the [portal-map] stanza of the configuration file.

DPWWA1092E Unable to open stanza file to read portal information

Explanation: The configuration file containing the portal mapping service information could not be opened for reading.

Administrator response: Ensure that the configuration file exists and is readable.

DPWWA1093W Unable to find [portal-map] stanza

Explanation: The [portal-map] stanza was not found in the configuration file.

Administrator response: Ensure that the [portal-map] stanza has been added to the configuration file.

DPWWA1094E Unable to read the URL field of the portal map

Explanation: The URL attribute of a portal map entry in the configuration file was not found.

Administrator response: Ensure that the [portal-map] stanza of the configuration file contains the URL field.

DPWWA1095E Unable to read the Protected Object field of the portal map

Explanation: The Protected Object field of a portal map entry in the configuration file was not found.

Administrator response: Ensure that the [portal-map] stanza of the configuration file contains the Protected Object field.

DPWWA1096E Unable to read the Action field of the portal map

Explanation: The Action field of a portal map entry in the configuration file was not found.

Administrator response: Ensure that the [portal-map] stanza of the configuration file contains the Action field.

DPWWA1097E the Protected Object supplied to the portal map is invalid

Explanation: The Protected Object field in the [portal-map] stanza of the configuration file is not a valid Protected Object name

Administrator response: Correct the value entered in the Protected Object field of the [portal-map] stanza of the configuration file.

DPWWA1100W POST request larger than request-body-max-read, cannot apply dynurl matching.

Explanation: WebSEAL attempted to apply dynurl matching to a request, but received too much POST data from the client.

Administrator response: Increase the request-body-max-read in the configuration file or rearchitect your site so that WebSEAL does not need to apply dynurl rules to large POSTs.

DPWWA1110E Unable to build original URL for Attribute Retrieval Service

Explanation: WebSEAL was unable to obtain the hostname of the URL that client has requested. The result of this is that the original URL cannot be constructed for consumption by the Attribute Retrieval Service.

Administrator response: Ensure that configuraion is complete.

DPWWA1111E The SOAP client returned the error code: *%d*

Explanation: The SOAP request failed, and the gSOAP client returned the error code contained in the message text.

Administrator response: Consult gSOAP documentation for error code definitions.

DPWWA1112E Attribute Retrieval Service internal error: *%s*

Explanation: The SOAP request succeeded, but the Attribute Retrieval Service returned the error contained in the message text.

Administrator response: Ensure that the Attribute Retrieval Service is configured correctly.

DPWWA1113E URL specifies an invalid Win32 object name

Explanation: The client request specifies the object name using a Win32 alias that points to the actual object. The authorization check will have been performed on the alias, and not the actual object, so the request cannot be allowed.

Administrator response: Ensure that client requests do not use Win32 aliases.

DPWWA1114E URL contains invalid Win32 characters or abbreviations

Explanation: The client request contains Win32 abbreviations or '\' characters that are invalid.

Administrator response: Ensure that client requests do not contain invalid Win32 characters or abbreviations.

DPWWA1115E URL contains an illegal byte sequence

Explanation: The client request contains an illegal byte sequence, possibly from an attempted multibyte character encoding.

Administrator response: Ensure that client requests do not contain illegal byte sequences.

DPWWA1116E The requested method is not supported

Explanation: One of the supported HTTP methods (that is: GET, PUT, POST, etc...) must be specified by each client request. This request either contains an unsupported method, or none at all.

Administrator response: Ensure that client requests contain a valid method.

DPWWA1117E The content-length of the client request is invalid

Explanation: The content-length is either less than zero, or it doesn't accurately describe the length of the POST-body, or it should not be provided with the request.

Administrator response: Ensure that the content-length specified correctly describes the characteristics of the request, and that this is not a chunked request.

DPWWA1118E The 'host' header is not present in the client request

Explanation: The client request specifies an HTTP version of 1.1, but doesn't include the host header that is required for this version.

Administrator response: Ensure that the host header is present in request who's HTTP version is 1.1.

DPWWA1119E The HTTP version specified by the client request is not supported

Explanation: See Message.

Administrator response: Ensure that the HTTP version of the request is correct and supported.

DPWWA1120E The POST body of the client request contains misformated or invalid data

Explanation: See Message.

Administrator response: Ensure that the POST bodies of client requests contain valid data.

DPWWA1121E An error occurred while reading the POST body of the request

Explanation: See Message.

Administrator response: Ensure that the POST bodies of client requests are valid.

DPWWA1122W Corrupted session cookie: *%s*.

Explanation: A session cookie was presented that was corrupted. This could be a spoof attempt, a browser or network problem, or a WebSEAL internal problem.

Administrator response: Investigate spoof attempt or source of corruption.

DPWWA1123W The login data entered could not be mapped to an IBM Security Access Manager user

Explanation: A mapping function, such as that in a library or CDAS, failed to map the login information to an IBM Security Access Manager user.

Administrator response: Check the login data, registry, or mapping function.

DPWWA1124W A client certificate could not be authenticated

Explanation: A client certificate could not be authenticated

Administrator response: Check the client certificate

DPWWA1125W The data contained in the HTTP header *%s* **failed authentication**

Explanation: The request an HTTP header that IBM Security Access Manager was configured to use as authentication data. This data failed authentication.

Administrator response: Check the request, the proxy server (if one is used), and the mapping library

DPWWA1126W IP address based authentication failed with IP address: *%s*

Explanation: IBM Security Access Manager is configured to authenticate using the client IP address, which was either unavailable or invalid

Administrator response: Check IBM Security Access Manager configuration and/or authentication library

DPWWA1128E The current authentication method does not support reauthentication. Contact the IBM Security Access Manager WebSEAL Administrator.

Explanation: Reauthentication is not supported by the current WebSEAL authentication method. The user can abort the reauthentication process (by accessing another URL) and still participate in the secure domain by accessing other resources that do not require reauthentication.

Administrator response: Notify the IBM Security Access Manager WebSEAL Administrator.

DPWWA1129E A reauthentication operation was attempted with an initial authentication method for which reauthentication is not supported.

Explanation: A reauthentication misconfiguration has occurred. Administrators should not put a reauthentication POP on a resource for clients who cannot actually perform a reauthentication.

Administrator response: The resource requested requires reauthentication but reauthentication is supported only by Forms, Token, and EAI authentication.

DPWWA1130E Authentication level mismatch when performing reauthentication

Explanation: The authentication level supplied while reauthenticating does not match the authentication level of the existing authenticated user.

Administrator response: The user's authentication level must be the same when reauthenticating as when they originally authenticated.

DPWWA1131W An entry in the [portal-map] stanza is invalid.

Explanation: [portal-map] stanza in the configuration file contains an invalid entry.

Administrator response: Ensure that all entries in the [portal-map] stanza are valid.

DPWWA1132W Entry '*%s* = *%s*' in the [portal-map] stanza is invalid.

Explanation: [portal-map] stanza in the configuration file contains an invalid entry.

Administrator response: Correct the entry in the [portal-map] stanza.

DPWWA1133E The 'host' header presented in the client request does not conform to HTTP specifications.

Explanation: The client request contains a host header which does not conform to the HTTP specification.

Administrator response: Ensure that the host header conforms to the HTTP specification.

DPWWA1200E The requested junction type is not supported by this server

Explanation: The requested junction type is not supported by this server

Administrator response: Change junction definition.

DPWWA1201E Junction not found

Explanation: The named junction does not exist.

Administrator response: Verify the name, and if incorrect try the operation again.

DPWWA1202E Requested object does not exist

Explanation: Object on junctioned server does not exist.

Administrator response: Informational only.

DPWWA1203E Permission denied

Explanation: You do not have permission to mount or unmount at this location.

Administrator response: Check the acl at this location for mount or unmount permissions.

DPWWA1204E Requested object is not a directory

Explanation: Requested object is not a directory

Administrator response: Informational only.

DPWWA1205E No query-contents on this server

Explanation: To list object space, a query_contents cgi program must be configured on the junctioned server.

Administrator response: To list object space, configure a query_contents cgi program on the junctioned server.

DPWWA1206E Illegal name for a junction point

Explanation: The junction point is illegal.

Administrator response: Use a different junction point for the new junction.

DPWWA1207E Trying to add wrong type of server at this junction point

Explanation: Trying to add wrong type of server at this junction point

Administrator response: Change junction definition.

DPWWA1208E Trying to add two servers with the same UUID at a junction point

Explanation: Trying to add two servers with the same UUID at a junction point

Administrator response: Change junction definition

DPWWA1209E Trying to add the same server twice at the same junction point

Explanation: Trying to add the same server twice at the same junction point

Administrator response: Change junction definition

DPWWA1210E Could not open junction database (*%s*,0x*%8x*)

Explanation: Indicates a problem accessing the junction database maintained by the IBM Security Access Manager server.

Administrator response: Check junction database directory existance and permissions.

DPWWA1211E Could not load junction database (*%s*,0x*%8lx*)

Explanation: An error occured when loading the junction database.

Administrator response: Check that all of the files in the junction database can be read by the ivmgr user and are not corrupted. Check other error messages for other information about the error. If necessary, remove all of the files in the junction database and then add them back one by one to isolate the problem to a specific file.

DPWWA1212E Could not delete entry from junction database (*%s*,0x*%8lx*)

Explanation: The XML File representing the junction could not be deleted.

Administrator response: Check the file permissions on the junction XML file

DPWWA1213E Could not write entry to junction database (*%s*,0x*%8lx*)

Explanation: Internal status code only. Database was opened, but could not be written to.

Administrator response: Check system memory and disk space.

DPWWA1214W Could not fetch entry from junction database (*%s*,0x*%8lx*)

Explanation: Internal status code only. Database was opened, but this junction could not be read.

Administrator response: Check that the xml file representing the junction is not corrupt.

DPWWA1215E Invalid junction flags for this junction type

Explanation: Invalid junction flags for this junction type

Administrator response: Correct junction definition.

DPWWA1216E Invalid parameters for junction

Explanation: Invalid parameters for junction

Administrator response: Correct junction definition.

DPWWA1217E An error occurred when writing a request to a junction. WebSEAL was unable to dispatch the request to another junction server.

Explanation: WebSEAL tried to send a request to a junction server. Sending the request failed. When WebSEAL is unable to send a request to a junction, WebSEAL attempts to 'rewind' the request from the client so that it can be sent to another junction server. If the request from the client is large, it may not be possible to retry the request. In that case, this error is returned to the client.

Administrator response: Retry the request. If the problem continues to occur, attempt to discover why the request could not be written to the junction server. Check WebSEAL and junction server log files for unusual error messages. Try sending the request directly to the junction.

DPWWA1218E Unknown junction server host

Explanation: Could not resolve a hostname using gethostbyname()

Administrator response: Check the hostname in the junction configuration and make sure it is resolveable.

DPWWA1219E Could not build junction server URL mappings (0x*%8lx*)

Explanation: See message

Administrator response: Contact support.

DPWWA1220E Cannot delete the junction at the root of the Web space. Try replacing it instead

Explanation: Cannot delete the junction at the root of the Web space. Try replacing it instead

Administrator response: Cannot delete the junction at the root of the Web space. Try replacing it instead

DPWWA1221E Cannot add two servers with different options (case-sensitive, etc) at the same junction

Explanation: Cannot add two servers with different options (case-sensitive, etc) at the same junction

Administrator response: Change junction definition

DPWWA1222E A third-party server is not responding. Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server.

Explanation: A junctioned server is not responding to requests. Possible causes: junctioned server down, network problems, hung application on junctioned server.

Administrator response: Determine why the junctioned server is not responding and fix it.

DPWWA1224E Could not load junction database

Explanation: The database couldn't be loaded for some reason.

Administrator response: Check the log files for more details.

DPWWA1225E Could not delete entry from junction database

Explanation: The file representing the junction could not be deleted from the filesystem.

Administrator response: Check the log files for more details.

DPWWA1226E Could not write entry to junction database

Explanation: Internal status code only. Database was opened, but could not be written to.

Administrator response: Check system memory and disk space.

DPWWA1227W Could not fetch entry from junction database

Explanation: Internal status code only. Database was opened, but this junctio n could not be read.

Administrator response: Check that the xml file representing the junction is not corrupt.

DPWWA1228E Unable to contact junction server host at mount point: *%s*

Explanation: Could not resolve a hostname using gethostbyname()

Administrator response: Check for network conectivity with the junctioned server

DPWWA1229E Unable to load junction file *%s***:** *%s*

Explanation: An error occurred while loading a file from the junction database. The reason for the error is included in the message.

Administrator response: Correct the error.

DPWWA1230E Error building junction *%s* **from file** *%s***:** *%s*

Explanation: An error occurred while building a junction from an XML file loaded from the junction database. The XML file may have specified invalid junction options.

Administrator response: Fix the problem in the XML file.

DPWWA1231E No such junction.

Explanation: A particular junction was not found in the junction database.

Administrator response: Verify that the junction file exists.

DPWWA1232E Could not remove file.

Explanation: The junction database was unable to remove a file.

Administrator response: Verify that all files in the junction database are writable by the ivmgr user and group.

DPWWA1233E Invalid junction file name.

Explanation: The junction file name specified did not map to a valid junction name.

Administrator response: Make sure the junction file name ends with .xml and is a valid mime 64 encoding.

DPWWA1234E An invalid status code was received in a response sent by a third-party server. This is not a problem with the WebSEAL system.

Explanation: A junctioned server has sent an invalid status code in a response.

Administrator response: Check status code returned from junctioned server.

DPWWA1235E Could not read the response status line sent by a third-party server. Possible causes: non-spec HTTP headers, connection timeout, no data returned. This is not a problem with the WebSEAL server.

Explanation: Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned

Administrator response: Check response from junctioned server. Could be bad HTTP headers or a connection timeout problem.

DPWWA1236E Could not read the response headers sent by a third-party server. Possible causes: non-spec HTTP headers, connection timeout, no data returned. This is not a problem with the WebSEAL server.

Explanation: Data read failure. Possible causes: non-spec HTTP headers, connection timeout, no data returned

Administrator response: Check response from junctioned server. Could be bad HTTP headers or a connection timeout problem.

DPWWA1237E An invalid HTTP header was sent by a third-party server. This is not a problem with the WebSEAL server.

Explanation: An HTTP response from a junctioned server does not conform to HTTP specs.

Administrator response: Check response from junctioned server for non-spec HTTP headers.

DPWWA1238E An HTTP message body sent in a response by a third-party server is too short. This is not a problem with the WebSEAL server.

Explanation: The actual length of the response body sent by a junctioned server is shorter that indicated by the Content-length HTTP header in the response.

Administrator response: Correct problem with junctioned server response. The actual length of the response body is shorter that indicated by the Content-length HTTP header of the response.

DPWWA1239E A third-party server is not responding. Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server.

Explanation: A junctioned server is not responding to requests. Possible causes: junctioned server down, network problems, hung application on junctioned server.

Administrator response: Determine why the junctioned server is not responding and fix it.

DPWWA1240E Could not build Virtual Host Junction host mappings (0x*%8lx*)

Explanation: See message

Administrator response: Contact support.

DPWWA1241E Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*'. Virtual Host Junction skipped.

Explanation: An error occured when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified. The problem is the the Virtual Host Junction being loaded refers to one that also refers to another.

Administrator response: Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1242E Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*' that already has partner '*%s*'. Virtual Host Junction skipped.

Explanation: An error occured when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified.

Administrator response: Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1243E Virtual Host Junction '*%s*' loaded from database illegally partners Virtual Host Junction '*%s*' with different virtual hostname. Virtual Host Junction skipped.

Explanation: An error occured when loading the Virtual Host Junction from it's database file. It may have been incorrectly manually modified. Virtual Host Junctions that are partnered must have the same virtual hostname (excluding the ports).

Administrator response: Manually edit the offending Virtual Host Junction Database file and correct it.

DPWWA1244E Virtual Host Junction attempted to partner (-g) non-existant Virtual Host Junction

Explanation: See text.

Administrator response: Use 'virtualhost list' command to find a valid partner.

DPWWA1245E Virtual Host Junction attempted to partner (-g) a Virtual Host Junction with a different virtual hostname.

Explanation: See text.

Administrator response: Use 'virtualhost show' command to help match virtual hostnames.

DPWWA1246E Virtual Host Junction illegally attempted to partner (-g) itself.

Explanation: See text.

Administrator response: Choose another partner.

DPWWA1247E Virtual Host Junction can not be changed to partner (-g) another as it is currently being partnered.

Explanation: See text.

Administrator response: Do not use -g for this operation.

DPWWA1248E Could not write entry to Virtual Host Junction database

Explanation: Internal status code only. Database was opened, but could not be written to.

Administrator response: Check system memory and disk space.

DPWWA1249E Could not write entry to Virtual Host Junction database (*%s*,0x*%8lx*)

Explanation: Internal status code only. Database was opened, but could not be written to.

Administrator response: Check system memory and disk space.

DPWWA1250E Virtual Host Junction can not be deleted until it's partner is deleted.

Explanation: See text.

Administrator response: Delete the Partner Virtual Host Junction first.

DPWWA1251E Virtual Host Junctions created using -g don't have their own object space. List the partner's object space instead.

Explanation: Virtual Host Junctions created using -g share their partnered Virtual Host Junction's protected object space. They don't have their own.

Administrator response: List the partnered Virtual Host Junctions object space instead as this Virtual Host Junction uses it for access control.

DPWWA1252E Virtual Host Junctions partnered using -g must have different protocol types (TCP and SSL).

Explanation: The concept of -g is to have the same content but opposite protocol, this was violated in this attempt to create a Virtual Host junction using -g.

Administrator response: Either don't use -g or ensure the type of the Virtual Host junction are of complementry protocols. For example localtcp and localssl will partner successfully.

DPWWA1253E The Virtual Host junction you are attempting to partner with using -g is already in a partnership.

Explanation: The concept of -g is to have only two Virtual host junctions in partnership, a third is not permitted.

Administrator response: Either don't use -g or ensure the Virtual Host junction being partnered to is not already in a partnership.

DPWWA1254E Can't replace a Virtual Host junction being partnered too with a new junction having a different protocol type (TCP and SSL).

Explanation: The concept of -g is to have the same content but opposite protocol, this was violated in this attempt to replace an existing Virtual Host junction.

Administrator response: Ensure the type of the Virtual Host junction is the same protocol as the Virtual Host juntion being replaced.

DPWWA1255E Can't replace a Virtual Host junction being partnered too with a new junction having a different virtual hostname.

Explanation: See text.

Administrator response: Use 'virtualhost show' command to help match virtual hostnames.

DPWWA1256E Virtual Host junction has duplicate virtual hostname (specificed by -v) as another Virtual Host junction.

Explanation: Virtual Host junctions are selected based on the host header in the client request matching the virtual hostname (specified by -v) of the Virtual Host junction. Thus the virtual hostname must be unique to be able to uniquely identify a Virtual Host junction.

Administrator response: Remove the Virtual Host junction with the duplicate virtual hostname before adding this one.

DPWWA1257E Could not load the local junction, *%s*, as the local junction functionality has been disabled.

Explanation: Local Junctions are disabled for this instance and a previously configured local junction, "%s", could not be loaded.

Administrator response: Remove the local junction or enable local junctions in the WebSEAL configuration file.

DPWWA1350E Could not initialize mutex

Explanation: A resource required for proper concurrency could not be created. The global variable errno may provide more specific information.

Administrator response: This is a fatal error. No recovery is possible.

DPWWA1352E Could not lock mutex

Explanation: A resource required for proper concurrency could not be locked. The global variable errno may provide more specific information.

Administrator response: This is a fatal error. No recovery is possible.

DPWWA1353E Could not unlock mutex

Explanation: A resource required for proper concurrency could not be unlocked. The global variable errno may provide more specific information.

Administrator response: This is a fatal error. No recovery is possible.

DPWWA1503E SSL function *function* **failed, error 0x***error code*

Explanation: An SSL toolkit function has failed.

Administrator response: This is a fatal error. No recovery is possible. Contact Support

DPWWA1504W SSL function *function* **failed, error 0x***error code*

Explanation: An SSL toolkit function failed.

Administrator response: This is a warning message. Operation continues. If the warning persists contact support.

DPWWA1505W HTTP request does not contain authentication information

Explanation: HTTP request does not contain authentication information

Administrator response: Internal status code only.

DPWWA1506E Unknown HTTP authentication scheme

Explanation: An authorization header contained an invalid authentication scheme.

Administrator response: Check Authorization header in request.

DPWWA1507E No password supplied in HTTP authentication header

Explanation: No password supplied in HTTP Authorization header

Administrator response: Check Authorization header in request.

DPWWA1518W The specified certificate key label *%s* **is incorrect. The default one will be used instead.**

Explanation: The specified certificate key label cannot be retrieved from the key database

Administrator response: check the webseald.conf ssl-keyfile-label option and the key database

DPWWA1950E Stanza '*%s***' is missing from configuration file**

Explanation: A necessary stanza is missing from configuration file

Administrator response: The stanza should be added to the configuration file

DPWWA1951E Configuration item '[*%s***]***%s***' is missing from configuration file**

Explanation: A necessary configuration item is missing from configuration file

Administrator response: The configuration item should be added to the configuration file

DPWWA1952E Received invalid HTTP header in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Explanation: Response HTTP headers do not conform to HTTP specs. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

Administrator response: Check HTTP headers in response. The response could have been sent either by a third-party server or by a local resource, such as a CGI program.

DPWWA1953E HTTP document fetch failed with status *%d*

Explanation: Could not retrieve requested resource.

Administrator response: Check request for correctness.

DPWWA1954E HTTP list request failed

Explanation: Could not list directory on junctioned server

Administrator response: Check permissions and existence of directory being listed

DPWWA1955E Field missing from HTTP header

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1962W CGI Script Failed

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1964E Invalid Content-Length header returned by TCP junction server

Explanation: The content-length is either less than zero, or it doesn't accurately describe the length of the POST-body.

Administrator response: Ensure that the content-length specified correctly describes the characteristics of the request.

DPWWA1965E Overflow of output buffer

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1966E Overflow of HTML filter workspace

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1967E Overflow of HTTP filter workspace

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1968E HTTP response truncated

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1969E HTTP request truncated

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1970E Cannot rewind HTTP response to write error message (*%lx***)**

Explanation: An internal error has occoured trying to rewing the HTTP response.

Administrator response: MRQ Contact support

DPWWA1971E Cannot write HTTP error response to client (*%lx***,***%lx***)**

Explanation: An internal error has occoured trying to write the error response to the client.

Administrator response: MRQ Contact support

DPWWA1972E Cannot read HTTP request from client

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1973E HTTP response aborted

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1975W Unable to decode *%s*

Explanation: The decode of the specified token has failed.

Administrator response: Contact support.

DPWWA1976W Unable to encode *%s*

Explanation: The encode of the specified token has failed. This is an unexpected internal error.

Administrator response: Contact support.

DPWWA1977W *%s* **for user** *%s***, in domain** *%s* **has expired**

Explanation: cdsso authentication token for a user has expired

Administrator response: The token has expired. This could be due to clock skew, in which case fix the clocks or change the authentication token lifetime in configuration file. But beware of replay attacks

DPWWA1978W Badly formed single-sign-on URL

Explanation: Badly formed single-sign-on URL

Administrator response: Fix the cdsso link on the web page.

DPWWA1979W Failover cookie contents have expired

Explanation: Failover cookie contents for a user has expired

Administrator response: No action is required.

DPWWA1980W Could not retrieve key for failover cookie

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1981W An internal error occurred while encoding/decoding the *%s*

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1982W Could not find SSO key for server/domain *%s*

Explanation: The SSO key file has not been correctly configured for the server

Administrator response: Set up configuration to provide correct key file for the specified server.

DPWWA1983W CDSSO cryptography error ***%d*** **occurred**

Explanation: Internal status code only.

Administrator response: No action is required.

DPWWA1984W Unable to use failover cookies. No failover cookie key configured

Explanation: Failover cookies have been enabled, but no keyfile has been specified.

Administrator response: Either turn failover cookies off, or specify the keyfile for the failover cookie.

DPWWA1985W Unable to retrieve CDSSO referer from request

Explanation: Either the agent has not provided the referer header or the client has directly typed in the link and not been directed by a link

Administrator response: No action is required.

DPWWA1986W Error reading key file *%s*

Explanation: The CDSSO keyfile could not be read from

Administrator response: Check the keyfile for existence and permissions.

DPWWA1987W Error writing key file *%s*

Explanation: The CDSSO keyfile could not be written to

Administrator response: Check the keyfile for permissions.

DPWWA1988E This action requires HTTP forms to be enabled in the configuration file

Explanation: HTTP forms are required for this action but are not enabled in the configuration file

Administrator response: The forms-auth configuration item should be set to both

DPWWA1989W Invalid protection level for *%s*

Explanation: The received token is of an insufficent protection level

Administrator response: Ensure that vf-token-privacy and vf-token-integrity have the same settings on both WebSEAL servers.

DPWWA1990W The e-community name *%s* **does not match the configured name** *%s*

Explanation: Another WebSEAL has passed an e-community name which does not match this servers configured e-community name

Administrator response: Synchronize the e-community names

DPWWA1991W The e-community cookie passed has expired

Explanation: The contents of the e-community cookie passed have expired

Administrator response: No action is required.

DPWWA1992E Can't retrieve fully qualified host name for server. Disabling e-community single-sign-on

Explanation: The fully qualified host name could not be retrieved

Administrator response: Ensure that network configuration allows gethostbyname to retrieve the fully qualified name

DPWWA1993E Can't determine server domain name. Disabling e-community single-sign-on

Explanation: The domain name could not be determined

Administrator response: Specify value for ec-cookie-domain setting or ensure that gethostbyname returns the fully qualified host name

DPWWA1994E Disabling e-community single-sign-on

Explanation: An error occurred when looking up the key associated with the domain name for this server.

Administrator response: Ensure that network configuration allows gethostbyname to retrieve the fully qualified name. You may need to place the fully qualified host name of this server first in the hosts file.

DPWWA1995E Invalid master authentication server configuration. Disabling e-community single-sign-on

Explanation: master-authentication-server and is-master-authentication-serverare mutually exclusive settings

Administrator response: Correctly configure the settings for master authentication server

DPWWA1996E e-community-name has not been specified. Disabling e-community single-sign-on

Explanation: An e-community name was not specified. This is mandatory

Administrator response: Correctly configure an e-community name

DPWWA1997W The machine *%s* **could not vouch for the user's identity**

Explanation: The specified machine returned a token indicating that it could not vouch for the user's identity

Administrator response: Correct e-community configuration

DPWWA1998W Unable to open the LTPA key file for reading

Explanation: The LTPA key file configured for a junction could not be opened for reading

Administrator response: Check junction configuration

DPWWA1999W The version of the LTPA key file is not supported

Explanation: Only certain versions of LTPA keyfiles are supported

Administrator response: Obtain right version of the key file

DPWWA2000W Error parsing LTPA key file

Explanation: The LTPA Keyfile is either corrupt or the wrong version

Administrator response: Obtain new copy of keyfile

DPWWA2001W LTPA key file: password invalid or file is corrupt

Explanation: The password specified could not decrypt keyfile

Administrator response: Use correct key file password or ensure file is not corrupted

DPWWA2002W The LTPA cookie passed has expired

Explanation: An expired LTPA cookie was passed

Administrator response: No action is required

DPWWA2004W LTPA text conversion error

Explanation: An iconv routine failed

Administrator response: Check locale settings

DPWWA2005W An error occurred while encoding an LTPA token

Explanation: Internal Error

Administrator response: Contact support.

DPWWA2006W An error occurred while decoding an LTPA token

Explanation: Internal Error

Administrator response: Contact support.

DPWWA2008E Error reading stanza '[*%s***]':** *%s*

Explanation: One of the entries in the stanza couldn't be parsed.

Administrator response: Fix the malformed entry in the stanza.

DPWWA2009E The forms single-sign-on argument '*%s***' needs a colon.**

Explanation: One of the request arguments isn't formatted properly.

Administrator response: Fix the argument.

DPWWA2010E Forms single-sign-on GSO argument '*%s***' is not valid. GSO arguments must be either 'gso:username' or 'gso:password.'**

Explanation: One of the request arguments isn't formatted properly.

Administrator response: Fix the argument.

DPWWA2011E The forms single-sign-on argument '*%s***' is not valid.**

Explanation: Most likely a typo in the config file.

Administrator response: Fix the argument.

DPWWA2012E Forms single-sign-on configuration error.

Explanation: This is a summary of the problem, and will be preceded by a better explanation of the error.

Administrator response: Fix the configuration problem.

DPWWA2013E Forms single-sign-on URLs must be relative to the junction point.

Explanation: The fsso URL from the configuration file does not begin with a / character.

Administrator response: Make the fsso URL relative to the junction point.

DPWWA2014E An internal error in the forms single-sign-on module occurred.

Explanation: This should never happen - perhaps some kind of unexpected configuration problem has resulted in an internal error.

Administrator response: Call tech support.

DPWWA2015E A forms SSO authentication request would have been dispatched to a different junction than the login request. The request has been aborted.

Explanation: For security reasons, forms SSO does not allow an authentication request to be dispatched to a different junction than the login page was returned from.

Administrator response: Make sure that the application does not dispatch the authentication request to a different junction than returned the login page.

DPWWA2016E No HTML form for single-sign-on was found.

Explanation: This occurs when no HTML form with an action URI matching the login-form-action was found in the document returned from the junction.

Administrator response: Examine the login page being returned from the junction. Is it an HTML or WML document? Does it contain an HTML form? Does the form action URI match the login-form-action entry in the forms SSO configuration file?

DPWWA2017E The login form returned by the junction did not contain all required form attributes.

Explanation: This occurs when the login form returned from a junction did not cpontain an 'action' or 'method' attribute in the form start tag.

Administrator response: Examine the login form being returned from the junction. Did the login form contain both the action and method attributes? Does the form action URI match the form action URI specified in the configuration file?

DPWWA2018E The action URI in the login form returned by the junction did not match any WebSEAL junction.

Explanation: In order to dispatch a forms SSO authentication request, WebSEAL must match the action URI returned with the login form to a WebSEAL junction. That match could not be made.

Administrator response: Examine the login form being returned by the junction. You may need to create a junction to the host referenced by the actoin URI.

DPWWA2019E The action URI in the login form returned by the junction was invalid.

Explanation: An action URI such as '/../foo' will be rejected by WebSEAL because /.. is not a valid location.

Administrator response: Examine the login form. Does it contain any invalid characters, or is the path invalid?

DPWWA2020E One or more of the arguments passed to the SU authentication module were invalid.

Explanation: The suauthn library can take an argument to specify the authentication level for the credential. It prints this error if the arguments are incorrect.

Administrator response: Check the flags being passed to the authentication library.

DPWWA2021E The SU authentication method specified is not enabled.

Explanation: The POST to /pkmssu.form takes an auth_method parameter. This must correspond to an authentication mechanism that is enabled in the configuration file.

Administrator response: Check the auth_method field in the SU form submission.

DPWWA2023E Configuration item '[*%s*]*%s*' has an invalid value '*%s*'

Explanation: A configuration item in the configuration file has a bad value. For example it is expecting an integer and was provided with a string

Administrator response: The configuration item should be changed to a valid entry

DPWWA2024E *%s* [*%s*] *%s*: Value is out of range. It must be value from 0 to 100.

Explanation: WebSEAL will not start if the worker-thread-hard-limit or worker-thread-soft-limit is not in the range 0 to 100 inclusive

Administrator response: You must edit the configuration file and adjust the value to a valid one

DPWWA2025W IBM Security Access Manager WebSEAL has lost contact with junction server: *%s*

Explanation: See message.

Administrator response: Check the network conection between WebSEAL and the junctioned server, and that the backend application server is running.

DPWWA2026W IBM Security Access Manager WebSEAL has regained contact with junction server: *%s*

Explanation: WebSEAL has regained contact with a junctioned server that was previously unreachable.

Administrator response: No action is required.

DPWWA2027E One or more of the form arguments is either missing or invalid.

Explanation: One or more of the arguments passed in the form submission is either missing or invalid.

Administrator response: Check the completed fields in the form submission.

DPWWA2028E New password verification failed. Make sure both new password fields contain the same data.

Explanation: New password double-check failed. Make sure both new passwords are the same.

Administrator response: Check the new password fields in the form submission.

DPWWA2029E Pam Module Internal Error

Explanation: Error with the Pam Handle. This is an unexpected internal error.

Administrator response: Notifiy the IBM Security Access Manager WebSEAL Administrator.

DPWWA2030W Mismatch of Auth Token versions, check pre-410-compatible-tokens setting.

Explanation: A new encoding method for Auth tokens was introduced in version 4.1.0 which is enabled by default. This can be overridden and made compatable with earlier versions using the webseald.conf file entry, [server] pre-410-compatible. All WebSEAL servers must be using the same version.

Administrator response: Update all WebSEAL servers to use the same setting for [server] pre-410-compatible-tokens.

DPWWA2031W Mismatch of *%s* **Auth Token versions, check pre-410-compatible-tokens setting.**

Explanation: A new encoding method for Auth tokens was introduced in version 4.1.0 which is enabled by default. This can be overridden and made compatable with earlier versions using the webseald.conf file entry, [server] pre-410-compatible. All WebSEAL servers must be using the same version.

Administrator response: Update all WebSEAL servers to use the same setting for [server] pre-410-compatible-tokens.

DPWWA2032E CDSSO library error.

Explanation: The CDSSO library returned a failing status.

Administrator response: Check configuration and usage. See msg__webseald.log for details.

DPWWA2033E Invalid configuration file name.

Explanation: An invalid parameter was passed to a function, indicating an internal error.

Administrator response: Call support.

DPWWA2034E Some PKCS#11 options are missing. You must specify either all or none of the the options: pkcs11-driver-path, pkcs11-token-label, pkcs11-token-pwd

Explanation: WebSEAL will not start if only some of the PKCS#11 options are specified.

Administrator response: You must edit the configuration file and set all PKCS#11 settings

DPWWA2035E Credential generation failed during the credential refresh operation. Error code 0x*%lx*

Explanation: The azn-api function azn_id_get_creds was called to retrieve a new credential for a user. The operation failed.

Administrator response: Use the pdadmin 'errtext' command to look up the corresponding error code, and take further action from there.

DPWWA2036E Credential generation failed during the credential refresh operation.

Explanation: The azn-api function azn_id_get_creds was called to retrieve a new credential for a user. The operation failed.

Administrator response: Check error logs for further information on the failure.

DPWWA2037E An invalid result for a credential refresh rule was specified.

Explanation: Credential refresh rules require that the rule result be either 'preserve' or 'refresh.'

Administrator response: Verify that the syntax of credential refresh configuration in configuration files is correct.

DPWWA2038E An internal error occurred during the credential refresh operation.

Explanation: This error should not occur.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2039W A credential attribute value of type *%lu* not supported by credential refresh was found. The value was removed from the new credential.

Explanation: Credential attribute values can be of several types. Credential refresh is able to preserve string, buffer, unsigned long, and protected object values. Other value types are removed from the credential.

Administrator response: You may ignore this warning if you are not experiencing other difficulties involving credential refresh. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2040E User session IDs must be enabled in order to use the credential refresh feature.

Explanation: Refreshing a user's credential based on their username requires that user session IDs are enabled.

Administrator response: Enable User Session IDs in the WebSEAL configuration file.

DPWWA2041E An invalid session cache entry was found while refreshing a user's credential.

Explanation: This message indicates that the user session cache and the credential cache are inconsistent.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2042W The user is not logged in to the web server.

Explanation: If a user is not logged in to the web server, their credential cannot be refreshed. There is also no need to refresh their credential, since the next time they log in to the web server they will receive a new credential.

Administrator response: No action is necessary.

DPWWA2044E Invalid certificate authentication configuration. Incompatible combination of accept-client-certs and ssl-id-sessions values.

Explanation: See message.

Administrator response: Change the accept-client-certs or ssl-id-sessions parameter in webseald.conf

DPWWA2045W A client attempted to Step-up to certificates, but the server is not configured for Step-up to certificates.

Explanation: See message.

Administrator response: Change the accept-client-certs parameter to prompt_as_needed in webseald.conf or unconfigure the step-up POPs.

DPWWA2046E Invalid certificate cache configuration.

Explanation: See message.

Administrator response: Change the values of the certificate cache configuration items.

DPWWA2047E The activity timestamp is missing from the failover cookie.

Explanation: A request was made to update the last activity timestamp of the failover cookie, but the attribute was not found in the cookie.

Administrator response: An internal error occurred. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2048E The original authentication method in the failover cookie is not recognized for failover authentication on this server. The value *%s* is invalid.

Explanation: A request could not be authenticated using the supplied failover cookie because the authentication level specified in the cookie is not valid for this server.

Administrator response: Update the supported failover authentication methods in the configuration file or correct the configuration of the server that generated the failover cookie.

DPWWA2049E The original authentication method in the failover cookie is not recognized for failover authentication on this server.

Explanation: A request could not be authenticated using the supplied failover cookie because the authentication level specified in the cookie is not valid for this server.

Administrator response: Update the supported failover authentication methods in the configuration file or correct the configuration of the server that generated the failover cookie.

DPWWA2050E An authentication system failure has occurred.

Explanation: A call to the authentication system failed with an unexpected error.

Administrator response: Examine the log for the context of the failure and correct any indicated problem. In particular, ensure that your user registry is available and accessible. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2051E An authentication system failure has occurred: error: *%s* **(error code:** *%#lx***).**

Explanation: A call to the authentication system failed with an unexpected error.

Administrator response: Examine the log for the context of the failure and correct any indicated problem. In particular, ensure that your user registry is available and accessible. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2052E The cross domain single sign-on operation failed.

Explanation: A call into the cross domain single sign-on system failed with an unexpected error.

Administrator response: Examine the log for the context of the failure. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2053E The cross domain single sign-on system failed with an unexpected error: *%#x*

Explanation: A call into the cross domain single sign-on system failed with an unexpected error.

Administrator response: Examine the log for the context of the failure. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2054E No default HTTP method permission map has been specified.

Explanation: A default HTTP method permission map must be specified in the configuration file but none has been.

Administrator response: Specify a value for the default HTTP method permission map in the configuration file.

DPWWA2055E The HTTP method permission map configuration information could not be found in the configuration file.

Explanation: No HTTP method permission map configuration information could be found in the configuration file.

Administrator response: Ensure that HTTP method permission map configuration information is present in the configuration file.

DPWWA2056E HTTP method permission map validation failed: API error: *%s* **(API error code: [***%#x***:***%#x***]).**

Explanation: The authorization API failed while validating the configured HTTP method permission map.

Administrator response: Perform the action required to resolve the problem indicated by the identified API error. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2057E The SSO token module configuration data was missing or invalid.

Explanation: The process using the SSO token modules must provide some input data to configure the modules. This data was not provided correctly. This is an unexpected internal error.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/

support/index.html?ibmprd=tivman

DPWWA2058E The integer value '*%s*' for the '*%s*' entry in the '*%s* stanza is not valid.

Explanation: The specified value is required to be a non-negative integer.

Administrator response: Correct the invalid configuration value.

DPWWA2059W The *%s* attribute could not be extracted from a credential: API error: *%s* (API error code [*%x*:*%x*]).

Explanation: The specified attribute could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2060W The *%s* attribute could not be extracted from a credential: API error code [*%x*:*%x*].

Explanation: The specified attribute could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2061W The number of values for the *%s* attribute could not be retrieved from an attribute list: API error: *%s* (API error code [*%x*:*%x*]).

Explanation: The number of values for the specified attribute could not be retrieved from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2062W The number of values for the *%s* attribute could not be retrieved from an attribute list: API error code [*%x*:*%x*].

Explanation: The number of values for the specified attribute could not be retrieved from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2063W The type of value *%d* for the *%s* attribute from an attribute list could not be determined: API error: *%s* (API error code [*%x*:*%x*]).

Explanation: The type of a values for the specified attribute in an attribute list could not be determined. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2064W The type of value *%d* for the *%s* attribute from an attribute list could not be determined: API error code [*%x*:*%x*].

Explanation: The type of a values for the specified attribute in an attribute list could not be determined. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2065W Value *%d* of the *%s* attribute cannot be included in an SSO token, as it is of type *%s*.

Explanation: The specified attribute value cannot be included in an SSO token, because it is of the wrong type. Only string and unsigned long data types can be included in SSO tokens.

Administrator response: Remove the token attribute specification which matched this attribute, or, for custom attributes, change the attribute type to one suitable for inclusion in tokens.

DPWWA2066W The *%s* attribute could not be extracted from an attribute list: API error: *%s* (API error code [*%x*:*%x*]).

Explanation: The specified attribute could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2067W The *%s* attribute could not be extracted from an attribute list: API error code [*%x*:*%x*].

Explanation: The specified attribute could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2068W The attribute list could not be retrieved from a credential: API error: *%s* (API error code [*%x*:*%x*]).

Explanation: The attribute list could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2069W The attribute list could not be retrieved from a credential: API error code [*%x*:*%x*].

Explanation: The attribute list could not be extracted from a credential. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2070W The list of entry names could not be retrieved from an attribute list: API error: *%s* (API error code: [*%x*:*%x*]).

Explanation: The list of entry names could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2071W The list of entry names could not be retrieved from an attribute list: API error code [*%x*:*%x*].

Explanation: The list of entry names could not be extracted from an attribute list. This may be due to resource exhaustion, and as such be transient.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2072E No cryptographic keys are configured for cross domain single sign-on in the stanza '*%s*'.

Explanation: No keys are configured for Cross Domain Single Sign-On in the specified stanza. For Cross Domain Single Sign-On to operate, keys must be configured in this stanza.

Administrator response: Correct the configuration, or use the cdsso_key_gen utility to create keys for use by CDSSO. CDSSO keys must be securely shared by, and installed on, all CDSSO participant servers.

DPWWA2073E No cryptographic keys are configured for e-community single sign-on in the stanza '*%s*'.

Explanation: No keys are configured for e-Community Single Sign-On in the specified stanza. For e-Community Single Sign-On to operate, keys must be configured in this stanza.

Administrator response: Correct the configuration, or use the cdsso_key_gen utility to create keys for use by eCSSO. eCSSO keys must be securely shared by and installed on all servers participating in the e-Community.

DPWWA2074W The machine '*%s*' could not vouch for the user's identity: error: *%s* (error code: *%#lx*)

Explanation: The specified machine returned a token indicating that it could not vouch for the user's identity. This means that either the user's account is disabled, or that the user was unable to authenticate to the specified machine.

Administrator response: If the message indicates that the user's account is disabled, check whether this should be the case. If the message indicates an authentication failure, the user may need to have their password changed. If possible, check the log messages on the specified machine for more information.

DPWWA2075E The stanza '*%s*' contains an invalid SSO token incoming attribute configuration item: '*%s* = *%s*'.

Explanation: The SSO token incoming attribute stanzas specify attributes that are accepted and rejected from incoming eCSSO or CDSSO tokens. The right hand side of the items in this stanza must be either 'accept' or 'reject'.

Administrator response: Locate and correct the invalid configuration item and try again.

DPWWA2076E Failed to construct a credential from a PAC supplied by an EAI server. Major status = 0x*%x*, minor status = 0x*%x*.

Explanation: An EAI server constructed a PAC to authenticate a user, but the PAC could not be converted to a credential.

Administrator response: Investigate the PAC construction and verify that the PAC data is valid for IBM Security Access Manager.

DPWWA2077E Could not authenticate user. An EAI server returned invalid authentication data.

Explanation: An EAI server failed to return proper authentication data in an authentication response. This is typically due to a misconfigured EAI server.

Administrator response: Investigate and correct any problems with the authentication headers returned by the EAI server.

DPWWA2078E Could not authenticate user. An external authentication service did not return required authentication data.

Explanation: An EAI server did not return required authentication data in an authentication response. This is typically due to a misconfigured EAI server not returning attributes that it must return.

Administrator response: Investigate and correct any problems with the authentication headers returned by the EAI server.

DPWWA2079E Configuration of the SSO create and/or consume authentication module(s) failed: *%s*'.

Explanation: ECSSO and/or CDSSO is configured to create and/or consume authentication tokens, but the modules could not be configured. This means that they are either not properly loaded, or there is a fatal problem with the current configuration settings.

Administrator response: Ensure that the sso-create/sso-consume libraries are properly specified in the configuration file.

DPWWA2080E The session inactivity timestamp is missing from the failover cookie.

Explanation: WebSEAL is configured to require inactivity timestamps in all received failover cookies, and a failover cookie was received that did not have the session inactivity timestamp.

Administrator response: Set failover-validate-inactivity-timestamp to optional.

DPWWA2081E The session lifetime timestamp is missing from the failover cookie.

Explanation: WebSEAL is configured to require lifetime timestamps in all received failover cookies, and a failover cookie was received that did not have the session inactivity timestamp.

Administrator response: Set failover-validate-lifetime-timestamp to optional.

DPWWA2082E This system error code could not be converted to an error string.

Explanation: The system error code has no equivalent error string.

Administrator response: No action is required.

DPWWA2083E The shared library could not be opened.

Explanation: The shared library could not be opened.

Administrator response: Examine earlier messages in the log containing this message to identify the module that could not be opened. Check that the identified library exists and is found within the configured library path.

DPWWA2084E Could not find the requested symbol.

Explanation: The requested symbol was not found within the shared library.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2085E The shared library file '*%s*' could not be opened: *%s*

Explanation: The specified shared library file could not be opened. The system error string is given.

Administrator response: Ensure the specified shared library file exists and has appropriate permissions. Restart the process.

DPWWA2086E The symbol '*%s*' could not be resolved in the shared library '*%s*': *%s*

Explanation: The specified symbol could not be resolved. The system error string is given.

Administrator response: Ensure the specified shared library file is the appropriate type of library file. Restart the process. If the problem persists, check IBM

Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2087E The '%s' flag to the authentication module requires an argument.

Explanation: The authentication module flag must have an argument.

Administrator response: Add an argument to the specified flag.

DPWWA2088E Unknown authentication module flag '%s'.

Explanation: An invalid option was provided to the authentication module.

Administrator response: Provide correct authentication module option.

DPWWA2089E The authentication module flag '%s' requires an integer argument.

Explanation: The argument of the authentication module flag must be an integer.

Administrator response: Ensure that the argument of the authentication module flag is an integer.

DPWWA2090E The session activity timestamp is missing from the failover cookie.

Explanation: WebSEAL is configured to require activity timestamps in all received failover cookies, and a failover cookie was received that did not have the session activity timestamp.

Administrator response: Set failover-require-activity-timestamp-validation to no.

DPWWA2091E Bad EAI trigger URL pattern '%s' in configuration file.

Explanation: The EAI trigger is not formatted correctly. If it is a Virtual Host junction trigger it must begin with HTTP[S]://hostname[:port]/.

Administrator response: Correct the syntax of the EAI trigger.

DPWWA2092E Could not reset the cache session lifetime because the EAI server provided a bad value ('%s') in the 'am_eai_xattr_session_lifetime' header.

Explanation: WebSEAL could not reset the cache session lifetime because the header value returned by the EAI server is invalid. The value must contain only numeric digits.

Administrator response: Investigate and correct any problems with the 'am_eai_xattr_session_lifetime' extended attribute header returned by the EAI server.

DPWWA2093E Configuration item '[%s]%s' has an invalid value '%s'

Explanation: A configuration item in the configuration file has a bad value. For example it is expecting an integer and was provided with a string

Administrator response: The configuration item should be changed to a valid entry

DPWWA2100E The new user ID does not match the user ID previously presented to authenticate.

Explanation: In the event of a step-up operation with verify-step-up-user set to true, the user ID presented to this authentication level must match the user ID authenticated to the previous level.

Administrator response: The user must present the same user ID provided in the previous authentication level.

DPWWA2101E The new user ID (%s) does not match the user ID (%s)previously presented to authenticate.

Explanation: In the event of a step-up operation with verify-step-up-user set to true, the user ID presented to this authentication level must match the user ID authenticated to the previous level.

Administrator response: The user must present the same user ID provided in the previous authentication level.

DPWWA2250E The ACL attached to the requested resource does not permit the Traverse operation.

Explanation: The ACL attached to the requested resource does not permit the Traverse operation.

Administrator response: Modify the ACL if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2251E The ACL attached to the requested resource does not allow access by this user.

Explanation: The ACL attached to the requested resource does not allow access by the client.

Administrator response: Modify the ACL if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2252E The requested resource is protected by a policy that restricts access to specific time periods. This request is prohibited at this time.

Explanation: A time-of-day POP is attached to the requested resource that has prohibited access at the time of the request.

Administrator response: Modify the POP if necessary, or inform the user of the policy details.

DPWWA2253E An External Authorization Server has denied access to the requested resource.

Explanation: An External Authorization Server has denied access to the requested resource.

Administrator response: Modify the EAS if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2254E The requested resource is protected by a policy that restricts access to specific clients. This request is prohibited for this client.

Explanation: Step-up is configured for the requested resource, but the client IP address is forbidden to step-up.

Administrator response: Modify the POP if necessary, or inform the user that they are not permitted to access the resource.

DPWWA2255E This user does not have permissions to perform a delegated operation.

Explanation: This user does not have permissions to perform a delegated operation.

Administrator response: Modify the ACL attached to the resource to grant the user delegation permissions, or inform the user that they are not permitted to perform the requested operation.

DPWWA2400E Invalid challenge header

Explanation: SPNEGO Authentication requires decoding a challenge header from the client. That header had an invalid format.

Administrator response: Make sure that the client is one supported by WebSEAL.

DPWWA2401E An internal error occurred during SPNEGO processing.

Explanation: SPNEGO authentication failed because of an internal error. This indicates a serious problem.

Administrator response: If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2402E Initialization of Kerberos authentication failed.

Explanation: Initialization of Kerberos authentication failed.

Administrator response: Check for additional error messages in log files. Check your SPNEGO configuration entries to make sure they match the documentation.

DPWWA2403E Your browser supplied NTLM authentication data. NTLM is not supported by WebSEAL. Make sure your browser is configured to use Integrated Windows Authentication.

Explanation: If a browser is improperly unconfigured, it will supply NTLM authentication data instead of SPNEGO data.

Administrator response: Make sure that the browser is located in the same domain as the WebSEAL server. Refer to your browser documentation to make sure it is configured properly for Integrated Windows Authentication.

DPWWA2404E An error occurred when creating the SPNEGO token.

Explanation: An error occurred when creating the SPNEGO token for the GSS-API token.

Administrator response: This problem is most likely due to an internal error or misconfiguration. Check the SPNEGO related configuration items in your server for errors.

DPWWA2405W Cannot update failover cookie for switch-user admins

Explanation: A switch-user admin cannot get a failover cookie for the user impersonated; this is a known limitation of failover with switch-user

Administrator response: No action is required.

DPWWA2406W Could not find the failover session ID in the user's failover token

Explanation: A user is trying to authenticate with a failover token that should have a session ID encoded from another WebSEAL replica. The session ID is missing from the token, indicating a configuration error at one of the replicas.

Administrator response: Ensure failover-include-session-id configuration settings are correct.

DPWWA2407W The failover session ID in the user's failover token does not match the session ID in the user's session cookie.

Explanation: When trying to establish a session with failover-include-session-id enabled, the session ID stored in the session cookie and the user's failover token must match. A mismatch indicates a possible security breach. WebSEAL will issue new session and failover cookies for the user.

Administrator response: Ensure failover-include-session-id configuration settings are correct.

DPWWA2408W Cannot find the session cookie in the user's request for use in comparing with the failover cookie.

Explanation: When attempting to establish a nonsticky failover session, WebSEAL could not find the user's session cookie. The cookie is required for a comparison with the session id in the failover token. Ensure configuration settings are correct.

Administrator response: Check cookie and nonsticky failover settings.

DPWWA2409W Reverse lookup for host '*%s*' returned an alternate host name '*%s*'. This might prevent SPNEGO authentication from functioning properly.

Explanation: The SPNEGO authentication module attempted to validate the SPNEGO principal name by checking that the reverse lookup for the specified host name resolves to the same host name as the original. The host name returned for the reverse lookup did not match the original host name.

Administrator response: If server startup succeeds and SPNEGO authentication functions properly, no action need be taken. If there are problems with SPNEGO authentication, make sure that your host name resolution is properly configured. Refer to the TAM WebSEAL Administration Guide for additional information about the problem.

DPWWA2410E Initialization of Kerberos authentication for server principal '*%s*' failed.

Explanation: Initialization of Kerberos authentication for the specified principal failed.

Administrator response: Check for additional error messages in log files. Refer to the TAM WebSEAL Administration Guide for additional information.

DPWWA2411E No SPNEGO service principal credential found for Virtual Host Junction '*%s*'.

Explanation: SPNEGO authentication cannot complete unless the SPNEGO keytab file contains a service principal matching the host name of the virtual host junction and the service principal is listed in the WebSEAL configuration file.

Administrator response: Verify that the client is using the correct hostname to contact the virtual host. Verify that the WebSEAL configuration file contains an entry '[spnego]spnego-krb-service-name = HTTP@<hostname>' for the virtual host. The SPNEGO keytab file must contain a key for the principal.

DPWWA2550E Error initializing the credential policy entitlements service

Explanation: An error occurred when loading the credential policy entitlements service.

Administrator response: Check the log file for additional error messages. The other error messages contain more information about the problem.

DPWWA2551E Policy retrieval for user *%s* failed: *%s* (error code: 0x*%lx*)

Explanation: An error occurred when trying to retrieve credential policy attributes for the specified user.

Administrator response: Examine the status message and code embedded in this message to identify the root cause of the problem.

DPWWA2734W The authentication type is unknown. The audit event will not be recorded.

Explanation: An authentication event has occurred. However, the authentication type utilized is not a known value and, as such, the audit event will not be recorded.

Administrator response: No action is required

DPWWA2735W The reason for the session termination is unknown. The audit event will not be recorded.

Explanation: A session has been terminated. The reason for this termination, however, is unknown. Because of this the audit record of this event could be considered broken and, as such, will not be audited.

Administrator response: No action is required

DPWWA2850E A general failure has occured within the SOAP client.

Explanation: An error has occured within the SOAP client.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2851E An error was returned from the SOAP server in cluster *%s* when calling the *%s* interface: *%s* (code: 0x*%x*).

Explanation: The web service returned an error.

Administrator response: Examine messages within the session management server log. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2852E An error occurred when attempting to communicate with the SOAP server URL *%s*: *%s* (error code: *%d*/0x*%x*).

Explanation: An attempt was made to communicate with the SOAP server and a failure occured within the underlying communications layer.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Ensure that the SOAP server is running and reachable. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWA2853E The SOAP client failed to initialized.

Explanation: The SOAP client for a Web service could not be initialized.

Administrator response: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman

DPWWM1299E Invalid flag '-*%c*'

Explanation: An invalid flag was passed to a command.

Administrator response: Read the manual to identify the flag you want to use.

DPWWM1300E Flag '-*%c*' does not take an argument

Explanation: An invalid argument was passed to a command.

Administrator response: Correct the syntax of the command.

DPWWM1301E Missing argument for '-*%c*' flag

Explanation: An argument is required for the option used.

Administrator response: Correct the syntax of the command.

DPWWM1302E Basic authentication type must be one of: ignore, filter,supply or gso

Explanation: An invalid argument followed the -b flag.

Administrator response: Correct the syntax of the command.

DPWWM1314E Must specify the junction type using the '-t' flag

Explanation: The junction type was not passed with the create command.

Administrator response: Pass the junction type as an argument to the -t flag.

DPWWM1315E Must specify a junction point

Explanation: No junction point was passed as an argument.

Administrator response: Correct the syntax of the command.

DPWWM1316W WARNING: A junction already exists at *%s*

Explanation: A junction already exists at the specified junction point.

Administrator response: Either replace the existing junction or specify a different junction point.

DPWWM1318E Cannot create junction

Explanation: A junction create command failed.

Administrator response: This message is preceded by a detailed explanation of why the junction could not be created. Correct the problem and try to create the junction again.

DPWWM1320E Must specify the junction server hostname using the '-h' flag

Explanation: No hostname was passed to the add or create command.

Administrator response: Include the hostname in the command.

DPWWM1321E Invalid port *%s*

Explanation: The port number specified was invalid. Port numbers must be integers greater than zero.

Administrator response: Specify a valid port number.

DPWWM1322E Invalid proxy port *%s*

Explanation: An invalid port number was passed using the -P flag. Port numbers must be integers greater than zero.

Administrator response: Pass a valid port number to the create or add command.

DPWWM1323E A proxy TCP port must be supplied with the -P option

Explanation: No -P argument was specified to the add or create command even though the -H argument was specified.

Administrator response: Include the -P argument in the command.

DPWWM1324E Can only use -T flag when using '-b gso'

Explanation: The -T flag was specified to the create command without the -b flag.

Administrator response: If you want to use GSO for the junction, pass -b gso as an argument to the junction create command. If you do not want to use GSO, then do not pass the -T flag to the create command.

DPWWM1325E Must also use -T flag when using '-b gso'

Explanation: The -b gso flag was passed to the create command without a corresponding -T flag.

Administrator response: Include the name of the GSO target which should be used for the junction.

DPWWM1327E Must specify a file system directory using the '-d' flag

Explanation: No directory was specified when trying to create a local junction.

Administrator response: If you want to create a local junction, pass the full path to the directory to use with the -d flag. If you want to create another type of junction, pass the correct type using the -t flag.

DPWWM1330E Must specify a server to remove using the '-i' flag

Explanation: No -i flag was passed to the 'remove' command.

Administrator response: If you want to delete the junction entirely, use the 'delete' command. If you want to remove a particular server, use the 'show' command to loook up the UUID of the server to remove, and then pass the UUID as the argument to the -i flag.

DPWWM1332E Invalid server ID

Explanation: The argument passed to -i was not a valid UUID.

Administrator response: Obtain the correct UUID by using the 'show' command and pass a valid UUID as an argument to the 'remove' command.

DPWWM1333E Could not fetch junction definition

Explanation: This message is followed by an explanation of the problem.

Administrator response: Correct the problem described by the following message.

DPWWM1334E Can only remove servers from a TCP, SSL or mutual junction

Explanation: It is not possible to remove a server from a local junction.

Administrator response: Correct the junction point specified in the remove command. The junction point should belong to a TCP, SSL or mutual junction.

DPWWM1335E Server *%s* **not found at junction** *%s*

Explanation: An attempt was made to remove a junction server based on a UUID which did not match any of the servers on the junction point.

Administrator response: Use the 'show' command to find the correct UUID and pass the correct UUID to the 'remove' command.

DPWWM1336E Could not delete junction

Explanation: This message is followed by an explanation of why the junction could not be deleted.

Administrator response: Correct the problem described in the message displayed after this message.

DPWWM1337E Could not update junction

Explanation: This message is followed by an explanation of why the junction could not be modified.

Administrator response: Correct the problem described in the message displayed after this message.

DPWWM1339E Junction not found at *%s***.**

Explanation: An attempt was made to add or remove a server from a junction point which does not exist.

Administrator response: Use the 'list' and 'show' commands to figure out which junction point you should use.

DPWWM1341E Create junction

Explanation: This message is followed by an explanation of why the creation failed.

Administrator response: Fix the problem described in the message following this message.

DPWWM1342E Can't add servers to this type of junction

Explanation: It is not possible to add servers to local junctions.

Administrator response: Only add servers to TCP, SSL, TCP proxy, SSL proxy or mutual junctions. Figure out which junction you wish to add a server to using the 'list' and 'show' commands, and then pass the correct junction point to the 'add' command.

DPWWM1343E Add server

Explanation: An attempt to add a server failed.

Administrator response: This message is followed by an explanation of why the server could not be added. Correct the problem.

DPWWM1345E Cannot list junctions

Explanation: This message is followed by an explanation of why junctions could not be listed. Correct the problem described in that message.

Administrator response: Correct the problem described in the following message.

DPWWM1346E Cannot show junction

Explanation: This message is followed by an explanation of the problem. Correct the problem described in that message.

Administrator response: Correct the problem described in the following message.

DPWWM1392E Bad value for path attribute.

Explanation: An item from a configuration file which should be set to a path name is an empty string instead.

Administrator response: Add the path to the configuration file.

DPWWM1416E Error: No filename specified in request.

Explanation: WebSEAL was unable to locate a template file to return to the user. The file may have been specified using the /pkms.....?filename=name.html construct or may have been one of the default response files.

Administrator response: If the link which produced this error was a PKMS page that included a ?filename=-name- query, make sure the format of the query portion of the link is correct. If the link which produced this error was not a PKMS page that included a file name specification, make sure that all files in the www/lib/-lang- directories are readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.)

DPWWM1417E Error: Could not retrieve file data.

Explanation: WebSEAL was unable to locate a template file to return to the user. The file may have been specified using the /pkms.....?filename=name.html construct or may have been one of the default response files.

Administrator response: If the link which produced this error was a PKMS page that included a ?filename=-name- query, verify that the file specified by -name- is located in the www/lib/-lang- (where -lang- is the language appropriate to the user's browser) directory and is readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.) If the link which produced this error was not a PKMS page that included a file name specification, make sure that all files in the www/lib/-lang- directories are readable by the ivmgr user (on UNIX systems) or by all users (on Windows systems.)

DPWWM1419E You can only use the -u flag with a stateful junction.

Explanation: The -u flag was passed to the add or create command without the -s flag. UUIDs can only be specified for stateful junctions.

Administrator response: If you wish to specify the UUID of the junction, then specify the -s flag as well as the -u flag.

DPWWM1420E The UUID specified with the -u flag is in an invalid format.

Explanation: An invalid UUID was specified with the -u flag to the 'add' or 'create' commands.

Administrator response: Correct the format of the UUID. If you are unsure of the proper format for a UUID, examine the output of the 'show' command for a junction. The 'ID' entry will contain a valid UUID.

DPWWM1427E -D flag only supported with ssl, sslproxy or mutual junctions.

Explanation: The -D flag can only be used for SSL, SSL proxy or mutual junctions.

Administrator response: Either make this an SSL/SSL Proxy or Mutual junction or do not specify the DN of the junctioned server.

DPWWM1432W NOTE: Ensure the CA root certificate used to sign the junctioned server certificate is installed in the WebSEAL certificate key database.

Explanation: WebSEAL was unable to communicate with an SSL junction because the junction presented a certificate WebSEAL could not validate.

Administrator response: See message.

DPWWM1435E -C flag only supported with ssl or sslproxy junctions.

Explanation: The -C flag can only be used for SSL or SSL proxy junctions.

Administrator response: Either make this an SSL or SSL Proxy junction or do not make the junction a WebSEAL to WebSEAL junction.

DPWWM1436E Either -K or -B can be defined for a junction.

Explanation: Both -K and -B were specified in the junction creation command. The two options cannot be used simultaneously on the same junction.

Administrator response: Read the manual and figure out whether you want to use -K, -B, or neither.

DPWWM1437E Both -K and -B flag only supported with ssl, sslproxy or mutual junctions.

Explanation: The -K and -B flags can only be used for SSL, SSL proxy or mutual junctions.

Administrator response: Either make this an SSL/SSL Proxy or Mutual junction or do not make the junction mutually authenticated.

DPWWM1438E The -b option cannot be specified with the -B option.

Explanation: Both -b and -B were specified in the junction creation command. The two options cannot be used simultaneously on the same junction.

Administrator response: Read the manual and figure out whether you want to use -b, -B, or neither.

DPWWM1439E -U <username> and -W <password> must be supplied with the -B option.

Explanation: The -B flag was specified without the -U and -W flags.

Administrator response: Specify the username and password for the junction with the -U and -W flags.

DPWWM1451W Too few authentication methods configured.

Explanation: Too few authentication methods have been specified.

Administrator response: Add 1 or more authentication methods to the authentication levels stanza configuration.

DPWWM1452W No unauthenticated method configured.

Explanation: The unauthenticated method has not been specified

Administrator response: Ensure that the unauthenticated method occurs first in the authentication levels stanza configuration.

DPWWM1453E Invalid authentication method.

Explanation: The specified authentication method is either invalid or unsupported in the current product configuration.

Administrator response: Verify the validity of the specified authentication method.

DPWWM1454E The requested operation is not valid

Explanation: IBM Security Access Manager was unable to perform a requested operation beca use it is not valid. An example would be a token authentication user attempting to change their password

Administrator response: Consult documentation for operation.

DPWWM1461E Failed loading JMT table

Explanation: The JMT file could not be read from disk.

Administrator response: Make sure the JMT file specifed in webseald.conf is present in the installation directory and is readable by the ivmgr user.

DPWWM1490E No dynurl.conf file found. No changes were made.

Explanation: No dynurl.conf file was present when the dynurl update command was issued.

Administrator response: Create the dynurl.conf file.

DPWWM1493E Junction '*%s*' has reached it's worker thread hard limit.

Explanation: The configured maximum number of worker threads for this junction has been reached. The overloaded requests are being retured with 503, Service Unavailable. This could be due to either a slow junction or too many requests.

Administrator response: Increase number of worker threads, increase hard limit or decrease load.

DPWWM1494W Junction '*%s*' has reached it's worker thread soft limit

Explanation: A configured warning level has been reached for this junction on the number of worker threads currently active on it. This could be due to either a slow junction or too many requests.

Administrator response: Prepare to increase number of worker threads, increase soft limit or decrease load.

DPWWM1499W The configured number of worker threads, *%d*, is greater than the system can support, *%d*. It has automatically been reduced.

Explanation: Each operation system has different levels of support for threads and open files. That combined with compile time options will provide limits on the configurable number of worker threads.

Administrator response: The software automatically reduced the value. However to stop this message appearing you may set the value in the configuration file lower.

DPWWM1510E One or more entries in dynurl.conf do not specify URLs

Explanation: See message.

Administrator response: Examine dynadi.conf for formatting and content errors.

DPWWM1513W The stanza '*%s*' in the configuration file contains an unrecognised P3P compact policy element: '*%s*'.

Explanation: The given entry is not a valid P3P HTTP header configuration entry.

Administrator response: Correct the configuration file entry. The list of valid P3P compact policy elements is given in the documentation.

DPWWM1514W The stanza '*%s*' in the configuration file contains an unrecognised value for the P3P compact policy element '*%s*': '*%s*'.

Explanation: The specified P3P HTTP header configuration entry contains an invalid value.

Administrator response: Correct the configuration file entry. The list of accepted values for each P3P compact policy element is given in the documentation.

DPWWM1515E The configuration for P3P HTTP header insertion is invalid.

Explanation: One or more aspects of the P3P HTTP header configuration are invalid. Earlier log messages give more specific details.

Administrator response: Examine other log messages to determine the specific error or errors in the configuration file, and correct the configuration.

DPWWM1516W No P3P policy elements are configured in the stanza '*%s*', but P3P header insertion has been enabled.

Explanation: P3P header insertion has been enabled in the configuration file, but no P3P policy has been configured. P3P headers cannot be inserted until the P3P policy is configured.

Administrator response: Either add P3P policy elements to the stanza, or disable P3P header insertion.

DPWWM1517E The -H and -P flags are valid only for tcpproxy and sslproxy type junctions.

Explanation: The -H and -P parameters are only valid for tcpproxy or sslproxy type junctions. Either create one of those types of junctions or remove the -H and -P parameters from this command.

Administrator response: Create a tcpproxy or sslproxy type junction.

DPWWM1518E A proxy hostname must be supplied with the -H option

Explanation: No -H argument was specified to the add or create command even though the -P argument was specified.

Administrator response: Include the -H argument in the command.

DPWWM1522E Only 'onfocus', 'inhead', 'xhtml10' and 'trailer' are supported with the -J option.

Explanation: An invalid option was supplied with the -J flag.

Administrator response: Correct the syntax of the command.

DPWWM1523E You can not specify both -C and -B flags when creating a junction.

Explanation: The -C and -B flags use the same method to transmit authentication data and thus would overwrite each other if used together.

Administrator response: Do not specify both flags when creating the junction.

DPWWM1524E The -P flag is valid only for mutual, tcpproxy and sslproxy type junctions.

Explanation: The -P parameter is only valid for mutual, tcpproxy or sslproxy type junctions. Either create one of those types of junctions or remove the -P parameter from this command.

Administrator response: Create a mutual, tcpproxy or sslproxy type junction.

DPWWM1527E The supplied TCP and SSL ports must be different.

Explanation: The TCP and SSL port values which have been supplied point to the same port. This is not a valid configuration.

Administrator response: Specify different port values for the TCP and SSL port options.

DPWWM1528E The -V flag is valid only for mutual junctions.

Explanation: The -V parameter is only valid for mutual type junctions. Either create one of those types of junctions or remove the -V parameter from this command.

Administrator response: Remove the -V flag or create a mutual type of junction.

DPWWM1531W Error: The supplied keyfile must not contain any path information.

Explanation: A base path for LTPA keyfiles has been statically configured and as such the supplied file name should not contain any path information.

Administrator response: Specify the name of the keyfile without any path information.

DPWWM1532W Error: The supplied FSSO configuration file must not contain any path information.

Explanation: A base path for FSSO configuration files has been statically configured and as such the supplied file name should not contain any path information.

Administrator response: Specify the name of the FSSO configuration file without any path information.

DPWWM2041E Cannot create Virtual Host Junction

Explanation: A virtualhost create command failed.

Administrator response: This message is preceded by a detailed explanation of why the Virtual Host Junction could not be created. Correct the problem and try to create the Virtual Host Junction again.

DPWWM2044E Create Virtual Host Junction

Explanation: This message is followed by an explanation of why the creation failed.

Administrator response: Fix the problem described in the message following this message.

DPWWM2045E Can't add servers to this type of Virtual Host Junction

Explanation: It is not possible to add servers to local Virtual Host Junctions.

Administrator response: Only add servers to TCP, SSL, TCP proxy, or SSL proxy Virtual Host Junctions. Figure out which Virtual Host Junction you wish to add a server to using the 'virtualhost list' and 'virtualhost show' commands, and then pass the correct Virtual Host Junction label to the 'virtualhost add' command.

DPWWM2047E Must specify the Virtual Host Junction type using the '-t' flag

Explanation: The Virtual Host Junction type was not passed with the create command.

Administrator response: Pass the Virtual Host Junction type as an argument to the -t flag.

DPWWM2050W WARNING: A Virtual Host Junction already exists using label *%s*

Explanation: A Virtual Host Junction already exists using the specified Virtual Host Junction label.

Administrator response: Either replace the existing Virtual Host Junction or specify a different Virtual Host Junction label.

DPWWM2051E -C flag only supported with ssl or sslproxy Virtual Host Junctions.

Explanation: The -C flag can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response: Either make this an SSL/SSL Proxy Virtual Host Junction or do not make the Virtual Host Junction a WebSEAL to WebSEAL Virtual Host Junction.

DPWWM2052E Can only use -T flag when using '-b gso'

Explanation: The -T flag was specified to the virtualhost create command without the -b flag.

Administrator response: If you want to use GSO for the Virtual Host Junction, pass -b gso as an argument to the virtualhost create command. If you do not want to use GSO, then do not pass the -T flag to the virtualhost create command.

DPWWM2053E Must also use -T flag when using '-b gso'

Explanation: The -b gso flag was passed to the virtualhost create command without a corresponding -T flag.

Administrator response: Include the name of the GSO target which should be used for the Virtual Host Junction.

DPWWM2054E Either -K or -B can be defined for a Virtual Host Junction.

Explanation: Both -K and -B were specified in the virtualhost create command. The two options cannot be used simultaneously on the same Virtual Host Junction.

Administrator response: Read the manual and figure out whether you want to use -K, -B, or neither.

DPWWM2055E Both -K and -B flag only supported with ssl or sslproxy Virtual Host Junctions.

Explanation: The -K and -B flags can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response: Either make this an SSL/SSL Proxy Virtual Host Junction or do not make the Virtual Host Junction mutually authenticated.

DPWWM2056E -U <username> and -W <password> must be supplied with the -B option.

Explanation: The -B flag was specified without the -U and -W flags.

Administrator response: Specify the username and password for the Virtual Host Junction with the -U and -W flags.

DPWWM2057E The -b option cannot be specified with the -B option.

Explanation: Both -b and -B were specified in the virtualhost create command. The two options cannot be used simultaneously on the same Virtual Host Junction.

Administrator response: Read the manual and figure out whether you want to use -b, -B, or neither.

DPWWM2058E Must specify the Virtual Host Junction server hostname using the '-h' flag

Explanation: No hostname was passed to the virtualhost add or create command.

Administrator response: Include the hostname in the command.

DPWWM2059E The -H and -P flags are valid only for tcpproxy and sslproxy type Virtual Host Junctions.

Explanation: The -H and -P parameters are only valid for tcpproxy or sslproxy type Virtual Host Junctions. Either create one of those types of Virtual Host Junctions or remove the -H and -P parameters from this command.

Administrator response: Create a tcpproxy or sslproxy type Virtual Host Junction.

DPWWM2060E A proxy hostname must be supplied with the -H option

Explanation: No -H argument was specified to the virtualhost add or create command even though the -P argument was specified.

Administrator response: Include the -H argument in the command.

DPWWM2062E You can only use the -u flag with a stateful Virtual Host Junction.

Explanation: The -u flag was passed to the virtualhost add or create command without the -s flag. UUIDs can only be specified for stateful Virtual Host Junctions.

Administrator response: If you wish to specify the

UUID of the Virtual Host Junction, then specify the -s flag as well as the -u flag.

DPWWM2063E -D flag only supported with ssl or sslproxy Virtual Host Junctions.

Explanation: The -D flag can only be used for SSL or SSL proxy Virtual Host Junctions.

Administrator response: Either make this an SSL/SSL Proxy Virtual Host Junction or do not specify the DN of the Virtual Host Junctioned server.

DPWWM2064E The UUID specified with the -u flag is in an invalid format.

Explanation: An invalid UUID was specified with the -u flag to the 'virtualhost add' or 'virtualhost create' commands.

Administrator response: Correct the format of the UUID. If you are unsure of the proper format for a UUID, examine the output of the 'virtualhost show' command for a Virtual Host Junction. The 'ID' entry will contain a valid UUID.

DPWWM2065W NOTE: Ensure the CA root certificate used to sign the Virtual Host Junctioned server certificate is installed in the WebSEAL certificate key database.

Explanation: WebSEAL was unable to communicate with an SSL Virtual Host Junction because the Virtual Host Junction presented a certificate WebSEAL could not validate.

Administrator response: See message.

DPWWM2067E Must specify a virtual hostname using the '-v' flag

Explanation: No virtual hostname was specified when trying to create a localtcp or localssl Virtual Host Junction.

Administrator response: If you want to create a localtcp or localssl Virtual Host Junction, you must set it's virtual hostname using the -v flag.

DPWWM2068E Must specify a file system directory using the '-d' flag

Explanation: No directory was specified when trying to create a localtcp or localssl Virtual Host Junction.

Administrator response: If you want to create a localtcp or localssl Virtual Host Junction, pass the full path to the directory to use with the -d flag. If you want to create another type of Virtual Host Junction, pass the correct type using the -t flag.

DPWWM2069E Must specify a server to remove using the '-i' flag

Explanation: No -i flag was passed to the 'virtualhost remove' command.

Administrator response: If you want to delete the Virtual Host Junction entirely, use the 'virtualhost delete' command. If you want to remove a particular server, use the 'virtualhost show' command to loook up the UUID of the server to remove, and then pass the UUID as the argument to the -i flag.

DPWWM2071E Could not delete Virtual Host Junction

Explanation: This message is followed by an explanation of why the Virtual Host Junction could not be deleted.

Administrator response: Correct the problem described in the message displayed after this message.

DPWWM2072E Invalid server ID

Explanation: The argument passed to -i was not a valid UUID.

Administrator response: Obtain the correct UUID by using the 'virtualhost show' command and pass a valid UUID as an argument to the 'virtualhost remove' command.

DPWWM2073E Virtual Host Junction not found with label *%s***.**

Explanation: An attempt was made to add or remove a server from a Virtual Host Junction which does not exist.

Administrator response: Use the 'virtualhost list' and 'virtualhost show' commands to figure out which Virtual Host Junction point you should use.

DPWWM2074E Could not fetch Virtual Host Junction definition

Explanation: This message is followed by an explanation of the problem.

Administrator response: Correct the problem described by the following message.

DPWWM2075E Can only remove servers from a TCP or SSL Virtual Host Junction

Explanation: It is not possible to remove a server from a local Virtual Host Junction.

Administrator response: Correct the Virtual Host Junction label specified in the remove command. The Virtual Host Junction label should belong to a TCP or SSL Virtual Host Junction.

DPWWM2076E Server *%s* not found at Virtual Host Junction *%s*

Explanation: An attempt was made to remove a Virtual Host Junction server based on a UUID which did not match any of the servers on the Virtual Host Junction.

Administrator response: Use the 'virtualhost show' command to find the correct UUID and pass the correct UUID to the 'virtualhost remove' command.

DPWWM2077E Could not update Virtual Host Junction

Explanation: This message is followed by an explanation of why the Virtual Host Junction could not be modified.

Administrator response: Correct the problem described in the message displayed after this message.

DPWWM2080E Cannot list Virtual Host junctions

Explanation: This message is followed by an explanation of why Virtual Host junctions could not be listed. Correct the problem described in that message.

Administrator response: Correct the problem described in the following message.

DPWWM2081E Cannot show Virtual Host Junction

Explanation: This message is followed by an explanation of the problem. Correct the problem described in that message.

Administrator response: Correct the problem described in the following message.

DPWWM2088E Must specify a Virtual Host Junction label

Explanation: No Virtual Host Junction label was passed as an argument.

Administrator response: Correct the syntax of the command.

DPWWM2089E A Virtual Host Junction label cannot contain the '/' character

Explanation: See text.

Administrator response: Correct the syntax of the command and try again.

DPWWM2090E A junction mount point must begin with '/'

Explanation: See text.

Administrator response: Correct the syntax of the command and try again.

DPWWM2091E The existing Virtual Host Junction is in an inconsistent state as it is missing it's virtual host name.

Explanation: See text.

Administrator response: Contact product support.

DPWWM4023E Error reading configuration file *%s*: *%s*

Explanation: There was an error opening a configuration file.

Administrator response: Make sure the file exists and is readable.

DPWWM4024E Stanza '*%s*' is missing from configuration file.

Explanation: A needed stanza was not found.

Administrator response: The stanza should be added to the configuration file

DPWWM4025E Unknown configuration item '[*%s*]*%s*' in configuration file.

Explanation: Probably a typo of the configuration item in the configuration file.

Administrator response: Correct the configuration item in the configuration file.

DPWWM4041E Unable to read the stanza [*%s*]. Add the stanza to theWebSEAL configuration file to enable TFIM SSO for the junction '*%s*'.

Explanation: See Message.

Administrator response: Add the configuration options to the WebSEAL config file and restart the WebSEAL server.

DPWWM4042E Unable to enable TFIM junction SSO.

Explanation: See Message.

Administrator response: Add the configuration options to the WebSEAL config file and restart the WebSEAL server.

DPWWM4045E The address supplied with the -a option, *%s*, is not a valid local address.

Explanation: See Message.

Administrator response: Ensure that the address which is supplied is a valid local address for the WebSEAL server.

Chapter 3. Protocol Service Messages

These messages are provided by the protocol service component.

FBTADM002E The invoked command failed.

Explanation: The executed command did not complete successfully.

System action: Command execution halted.

Administrator response: Check the log files or examine any returned exceptions.

FBTADM004E There are no SAML Artifact Services configured.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM005E There are no SAML Artifact Services configured with the given configuration identifier.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM006E The given name for the creation of the new Tivoli Federated Identity Manager domain already exists. Supply a different domain name or remove the existing domain first.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM007E A Tivoli Federated Identity Manager domain name is required for this operation to complete.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify the domain name using the parameter fimDomainName

FBTADM008E A WebSphere cluster or server name is required for this operation. If the target environment is on a cluster, enter the clustername. If the target environment is not a cluster, provide the name of the application server (typically server1). To find the name of the cluster or the server use the Application Servers panel on the WebSphere administrative console.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM009E One or more parameters have to be provided for this operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: View the usage and pass the required parameters to the command.

FBTADM010E The Tivoli Federated Identity Manager domain specified for this operation does not exist.

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the list operation of the command manageItfimDomain to view the domain name.

FBTADM011E The Tivoli Federated Identity Manager runtime is not currently deployed into the selected domain. To deploy the runtime use the deploy operation of this command.

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the deploy operation of the command manageItfimDomain to deploy the runtime.

FBTADM013E A file name to read from or write to needs to be provided for this command.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify a file name for this command.

FBTADM014E Required Tivoli Access Manager parameters were not passed to this operation. When a Tivoli Federated Identity Manager domain uses Tivoli Access Manager the following parameters are required, tamAdminId, tamtamPolicyServer, tamAuthzServers, tamAuthzPorts.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the documentation or view the command help for usage.

FBTADM017E The following error ocurred while reloading the Tivoli Federated Identity Manager Management Service.

Explanation: Errors from the Tivoli Federated Identity Manager Management Service is returned as a result of executing the reloadItfimManagementService command.

System action: Command execution halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for the exception details.

FBTADM018E One of the parameters passed needs to be an integer but it is not.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM019E One or more parameters passed are in an incorrect format.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM020E The configuration type passed to the command is in an unrecognized format. Acceptable values are ldap or jdbc.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the documentation or view the command help for usage.

FBTADM021E This operation requires that the configuration type for the alias service is set to ldap but the current configuration is jdbc. Run the configure operation to change the configuration to ldap.

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the configure operation of the manageItfimNameIdSvc command.

FBTADM022E The provided server, hostname and port, already exists in the configuration. If you need to modify the parameters use the modifyHost operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the modifyHost operation of the manageItfimNameIdSvc command.

FBTADM023E The provided server, hostname and port, is not defined in the configuration. Create this server entry using the addHost operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the addHost operation of the manageItfimNameIdSvc command.

FBTADM024E The parameter *insert* **is required for this operation.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the documentation or view the command help for usage.

FBTADM025E The partner *insert* **associated to federation** *insert* **was not found. Check that both partner and federation names are correct. You can use the list operation of the manageItfimPartner commands to get a list of existing partners and federations.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Run the list operation of the manageItfimPartner command.

FBTADM026E The property *insert* is required for this operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the documentation for response file property requirements for this operation.

FBTADM028E The parameter *insert* is required for this operation but it was not given.

Explanation: The command requires parameters that were not passed in.

System action: Command execution halted.

Administrator response: Check the documentation or view the command help for usage.

FBTADM029E The Tivoli Federated Identity Manager domain name, server name, server port, and report name are not specified.

Explanation: The command requires parameters that were not passed in.

System action: Command execution halted.

Administrator response: View the usage and pass the required parameters to the command.

FBTADM030E The Tivoli Federated Identity Manager domain name, server name, and server port are not specified.

Explanation: The command requires parameters that were not passed in.

System action: Command execution halted.

Administrator response: View the usage and pass the required parameters to the command.

FBTADM031E No runnable reports were found.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTADM032E The Report Engine could not be started. Check the log files or examine any returned exceptions.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTADM033E The Report Engine could not be shut down. Check the log files or examine any returned exceptions.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTADM034E No reports are currently running.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTADM035E The Tivoli Federated Identity Manager domain name, server name, and server port are not specified.

Explanation: The command requires parameters that were not passed in.

System action: Command execution halted.

Administrator response: View the usage and pass the required parameters to the command.

FBTADM036E No archived reports were found.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTADM037E The Tivoli Federated Identity Manager domain name, server name, and server port are not specified.

Explanation: The command requires parameters that were not passed in.

System action: Command execution halted.

Administrator response: View the usage and pass the required parameters to the command.

FBTADM038E A report design is required for this operation to complete.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify the report design using the reportDesign parameter.

FBTADM039E A hostname is required for this operation to complete.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify the host name using the hostName parameter.

FBTADM040E A port is required for this operation to complete.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify the port using the hostPort parameter.

FBTADM041E A render type is required for this operation to complete.

Explanation: See message.

System action: Command execution halted.

Administrator response: Specify the render type using the renderType parameter.

FBTADM042E The supplied keystore was not found in the domain. Verify that the kesytore name is correct and that it does exist.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM043E No keys are defined inside the supplied Key Store.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM044E The domain supplied does not have any keystores defined.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM045E The supplied response file does not contain a valid federation name to be created.

Explanation: See message.

System action: Command execution halted.

Administrator response: Add the FedName property to the response file.

FBTADM046E The federation *insert* already exists. Specify a different name in the response file.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM047E Unable to create partner response file. Verify that the parameters supplied were correct and verify the logs.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTADM048E The file *insert* specified in property *insert* does not exist.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the path to the file.

FBTADM049E This operation requires the Tivoli Access Manager administrator password in order to complete. Provide this password by specifying the -tamAdminPwd option.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM050E Unable to create federation response file. Verify that the parameters supplied were correct and verify the logs.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTADM051E A Tivoli Federated Identity Manager domain already exists in the target cluster or server *insert*. Remove that domain before attempting to create a new one.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM052E The federation *insert* is not an identity provider. A query requester partner can only be added to an identity provider federation.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM053E Unable to import the key *insert* into keystore *insert*. Make sure that the keystore name and supplied password are correct.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM054E The export operation failed to write the domain to the supplied file. Check the name and path of the supplied file and that its location can be written.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM055E Unable to undeploy runtime from: *insert*.

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTADM056E This operation is not supported for the specified Single Sign-On protocol.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM057E The callback id: *insert* is not defined. Publish the Point of Contact callback plug-ins to the runtime node if creating a custom point of contact or check the existing callback names using the listCallbacks operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM058E The callback property: *insert* for callback *insert* is not defined. Check the available properties for a callback using the listCallbacks operation.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM059E The specified Point of Contact profile: *insert* was not found.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM060E The specified Chain Request Mapping with uuid: *insert* was not found.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM061E The module instance with uuid: *insert* was not found.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM062E The module type with uuid: *insert* was not found.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM063E The module chain with uuid: *insert* was not found.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM064E The number of instances provided does not match the number of modes provided. These two numbers must match.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM065E The mode: ***insert*** **for module instance:** ***insert*** **is not supported.**

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM066E The chain mapping for chain: ***insert*** **was not found.**

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM067E The custom properties cannot be loaded into the specified domain.

Explanation: The custom properties cannot be imported.

System action: Command execution halted.

Administrator response: No response required.

FBTADM068E The given name for the Tivoli Federated Identity Manager domain does not exist. Supply a different domain name.

Explanation: The specified domain name does not exist.

System action: Command execution halted.

Administrator response: No response required.

FBTADM069E A Tivoli Federated Identity Manager federation name is required for this operation to complete.

Explanation: This operation requires the name of an existing federation.

System action: Command execution halted.

Administrator response: Specify the federation name using the parameter federationName

FBTADM070E The federation ***insert*** **does not exist. Specify a different name.**

Explanation: The specified federation name does not exist.

System action: Command execution halted.

Administrator response: No response required.

FBTADM071E The operation ***operation*** **is unknown for the current command.**

Explanation: An operation was specified that is not implemented for the current command.

System action: Command execution halted.

Administrator response: Please enter a valid operation for this command.

FBTADM072E A key with alias '*key alias*' was not found in the keystore '*keystore*'.

Explanation: An alias was specified for a signing or encryption key, but no key with that alias was found in the specified keystore.

System action: Command execution halted.

Administrator response: Please enter a valid alias.

FBTADM073E The partner role value ***insert*** **specified on parameter** ***insert*** **is not supported for this operation.**

Explanation: The partner role specified is not supported by the federation.

System action: Command execution halted.

Administrator response: Check the documentation or view the command help for usage.

FBTADM074E The migration type is required for this operation to complete.

Explanation: This operation requires the migration type to be performed.

System action: Command execution halted.

Administrator response: Specify the migration type using the parameter migrationType

FBTADM075E The migration type value ***insert*** **specified on parameter** ***insert*** **is not supported by the runtime.**

Explanation: The migration type specified is not supported by the runtime.

System action: Command execution halted.

Administrator response: List the supported migration types for the runtime.

FBTADM076E The migration type ***insert*** **does not support the use of a response file.**

Explanation: The migration type specified does not support the use of a response file.

System action: Command execution halted.

Administrator response: Execute the operation without using a response file.

FBTADM077E The federation name can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Specify a different name in the response file using only the valid characters.

Explanation: See message.

System action: Command execution halted.

Administrator response: No response required.

FBTADM078E A module chain with the display name *name* already exists.

Explanation: A module chain with the specified name already exists. Module chain display names must be unique.

System action: Command execution halted.

Administrator response: Specify a different name for the new module chain.

FBTADM079E A module instance with the name *name* already exists.

Explanation: A module instance with the specified name already exists. Module instance names must be unique.

System action: Command execution halted.

Administrator response: Specify a different name for the new module instance.

FBTADM080E The module instance *instance* is protected and cannot be deleted.

Explanation: The specified module instance cannot be deleted because it is a protected instance.

System action: Command execution halted.

Administrator response: No response required.

FBTADM081E The module instance *instance* cannot be deleted because it is currently used in one or more module chains.

Explanation: The specified module instance cannot be deleted because it is used in one or more module chains.

System action: Command execution halted.

Administrator response: If the module instance must be deleted, remove it from the module chains that use it, or delete those module chains.

FBTADM082E The module type for module instance *instance* cannot be changed from *oldtype* to *newtype*.

Explanation: The module type for a module instance cannot be changed.

System action: Command execution halted.

Administrator response: Create a new module instance with the required type, then reconfigure any module chains using the existing module instance to use the new one. If the existing module instance is no longer required, it may then be deleted.

FBTADM083E The name of module instance *instance* cannot be changed from *oldname* to *newname*.

Explanation: The name of a module instance cannot be changed.

System action: Command execution halted.

Administrator response: Create a new module instance with the specified name. If the existing module instance is no longer required, delete it.

FBTADM084E The minimum length for client identifier is <*number*> characters.

Explanation: The length of the client identifier in the response file does not meet the required length.

System action: No action taken.

Administrator response: Ensure the client identifier meets the minimum length requirement.

FBTADM085E The client identifier can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Specify a different client identifier using the valid characters.

Explanation: The client identifier in the response file contains a character that is not valid.

System action: No action taken.

Administrator response: Provide the valid client identifier in the response file.

FBTADM086E An error occurred when verifying the client identifier. A client with the specified client identifier already exists.

Explanation: The client identifier in the response file is not valid because it is already in use.

System action: No action taken.

Administrator response: Ensure the client identifier specified is unique for this federation.

FBTADM087E The minimum length for the client shared-secret is <*number*> characters.

Explanation: The length of the client shared-secret in the response file does not meet the required length.

System action: No action taken.

Administrator response: Ensure that the client shared-secret meets the minimum length requirement.

FBTADM089E The client callback URI is not valid. Specify a valid client callback URI. If this is not applicable, specify 'oob'.

Explanation: The client callback URI in the response file is not valid.

System action: No action taken.

Administrator response: Provide the valid client callback URI in the response file.

FBTADM090E The client identifier cannot be modified.

Explanation: The client identifier in the response file is different from the registered one.

System action: No action taken.

Administrator response: Provide the registered client identifier in the response file.

FBTADM091E The minimum length for client identifier is <*number*> characters.

Explanation: The length of the client identifier in the response file does not meet the required length.

System action: No action taken.

Administrator response: Ensure the client identifier meets the minimum length requirement.

FBTADM092E The client identifier can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Specify a different client identifier using the valid characters.

Explanation: The client identifier in the response file contains a character that is not valid.

System action: No action taken.

Administrator response: Provide a valid client identifier in the response file.

FBTADM093E An error occurred when verifying the client identifier. A client with the specified client identifier already exists.

Explanation: The client identifier in the response file is not valid because it is already in use.

System action: No action taken.

Administrator response: Ensure the client identifier specified is unique for this federation.

FBTADM094E The minimum length for the client shared-secret is <*number*> characters.

Explanation: The length of the client shared-secret in the response file does not meet the required length.

System action: No action taken.

Administrator response: Ensure that the client shared-secret meets the minimum length requirement.

FBTADM096E The client redirection URI is not valid. Specify a valid client redirection URI.

Explanation: The client redirection URI in the response file is not valid.

System action: No action taken.

Administrator response: Provide a valid client redirection URI in the response file.

FBTADM097E The client identifier cannot be modified.

Explanation: The client identifier in the response file is different from the registered one.

System action: No action taken.

Administrator response: Provide the registered client identifier in the response file.

FBTADM098E An OAuth partner cannot be created for the federation *insert*.

Explanation: An external client provider was selected for the federation. IBM Tivoli Federated Identity Manager internal partners are not allowed when an external client provider is selected.

System action: No action taken.

Administrator response: Add clients externally based on your implementation, or change the OAuth client provider configuration to add partners to IBM Tivoli Federated Identity Manager.

FBTADM099E The partner *insert* that is associated to federation *insert* cannot be deleted.

Explanation: Global entity partners are used in an OAuth 2.0 flow. You must not delete any of the global entity partners. Note that if an OAuth 2.0 federation is deleted, its associated global entity partners are also deleted.

System action: Command execution halted.

Administrator response: No action taken.

FBTADM100E The partner *insert* that is associated to federation *insert* cannot be deleted.

Explanation: Global entity partner is used in an OAuth 1.0 flow. You must not delete the global entity partner. Note that if an OAuth 1.0 federation is deleted, its associated global entity partner is also deleted.

System action: Command execution halted.

Administrator response: No action taken.

FBTADM101E The XML file format is not valid for *insert*.

Explanation: The XML file that you provided is not formatted correctly.

System action: Command execution halted.

Administrator response: Check your XML file for syntax errors, and fix the errors.

FBTADM102E Error occured when writing the file *insert*.

Explanation: There are several causes of this error. Some of these causes are the following. First, the file that you provided is a directory. Second, the file that you provided cannot be created. Third, the file that you provided but cannot be opened. Check the log files to determine the cause of the error.

System action: Command execution halted.

Administrator response: Check the log files to determine the cause of the error.

FBTADM103E Error occurred when reading the file *insert*.

Explanation: There are several possible causes of this error. Some of these causes are the following. First, the file that you provided is a directory. Second, the file that you provided cannot be opened for reading. Please check the log files to determine the cause of the error.

System action: Command execution halted.

Administrator response: Check the log files to determine the cause of the error.

FBTADM104E The mapping rule type specified in the property *insert* is not valid.

Explanation: You specified a mapping rule type that is not valid.

System action: Command execution halted.

Administrator response: Specify the correct mapping rule type.

FBTADM105E The *insert* mapping rule specified in the property *insert* is not syntactically valid.

Explanation: The mapping rule is not syntactically valid.

System action: Command execution halted.

Administrator response: Specify a syntactically valid mapping rule. Check the log files for more details about this error.

FBTADM106E The OTP Type or the OTP Provider Module Id *insert* specified in the property *insert* does not correspond to any OTP Type or any OTP Provider Module Id specified in the property *insert*.

Explanation: See message.

System action: Command execution halted.

Administrator response: Ensure that the specified OTP Type or OTP Provider Module Id is valid.

FBTADM107E The Delivery Type or the OTP Delivery Module Id *insert* specified in the property *insert* does not correspond to any Delivery Type or any OTP Delivery Module Id specified in the property *insert*.

Explanation: See message.

System action: Command execution halted.

Administrator response: Ensure that the specified Delivery Type or OTP Delivery Module Id is valid.

FBTADM108E The format of the response file *insert* is not valid.

Explanation: You used a response file with invalid format.

System action: Command execution halted.

Administrator response: Specify a response file with a valid format. Check the log files for more details about this error.

FBTADM109E An error occurred while committing your changes. The changes have been rolled back. Check the log files to determine the cause of the error.

Explanation: Changes were not commited because of an error.

System action: Changes have been rolled back.

Administrator response: Check the log files to determine the cause of this error.

FBTADM110E Error occurred while rolling back your changes. Check the log files to determine the cause of the error.

Explanation: Your changes were rolled back because an error occurred while committing them. While rolling back your changes, another error occurred. Check the log files to determine the cause of these errors.

System action: Command execution halted.

Administrator response: Check the log files to determine the cause of this error.

FBTADM111E OTP Provider Module with Id *insert* **does not exist. Specify a different OTP Provider Module Id.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Ensure that the OTP Provider Module with the specified Id exist.

FBTADM112E OTP Delivery Module with Id *insert* **does not exist. Specify a different OTP Delivery Module Id.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Ensure that the OTP Delivery Module with the specified Id exist.

FBTADM113E Error occurred while obfuscating the property *insert***. Check the log files to determine the cause of the error.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Check the log files to determine the cause of this error.

FBTADM114E Error occurred while unobfuscating the property *insert***. Ensure that the property is a valid obfuscated value. Otherwise, check the log files to determine the cause of the error.**

Explanation: See message.

System action: Command execution halted.

Administrator response: Ensure that the property is a valid obfuscated value. Otherwise, check the log files to determine the cause of this error

FBTAUD001E Check the audit configuration to ensure that it is correct.

Explanation: The audit configuration settings might contain errors or ommissions.

System action: System will not audit.

Administrator response: Check the audit properties or try restarting the server.

FBTAUD002E The passed-in audit provider is not supported.

Explanation: This error occurs due to problems in the audit configuration.

System action: System will not audit.

Administrator response: Check the audit properties or try restarting the server.

FBTAUD003E The audit configuration property *insert* **is not defined or is incorrect.**

Explanation: This error occurs due to problems in the audit configuration.

System action: System will not audit.

Administrator response: Correctly specify the property and restart the server.

FBTAUD004E An error was encountered while initializing the file logger.

Explanation: This error occurs due to problems in the audit configuration.

System action: System will not audit.

Administrator response: Check the file logger properties and the encapsulated exception to solve the problem.

FBTAUD005E An error was encountered while initializing context to the Common Audit Serivice server. Check the JNDI connection property and emitter profile for possible errors.

Explanation: This error occurs due to problems in the audit configuration.

System action: System will not audit.

Administrator response: Check the properties mentioned in the error and the encapsulated exception to solve the problem.

FBTAUD006E An error was encountered while sending the audit event to the Common Audit Service server.

Explanation: This error occurs because of problems in the audit configuration, or because of connectivity problems with the Common Audit Service server.

System action: System will not audit this particular event.

Administrator response: Ensure that the Common Audit Service server is running and check the encapsulated exception to solve the problem.

FBTAUD007E An error was encountered while initializing the audit component.

Explanation: This error occurs because of problems in the audit configuration, or because of connectivity problems with the Common Audit Service server.

System action: System will not audit this particular event.

Administrator response: Ensure that the Common Audit Service server is running and check the previous exceptions in the log to determine the cause of the problem.

FBTAUD008E An event completion exception was encountered because all of the event data is not filled in correctly.

Explanation: This error occurs if any of the required elements in the event are not set.

System action: System will not audit this particular event and will log an exception.

Administrator response: Check the encapsulated exception to solve the problem.

FBTAUD009E System could not audit a call because a required parameter to the API is not available.

Explanation: This error occurs if any of the required elements in the event are not set.

System action: System will not audit this particular event and will log an exception.

Administrator response: Check the parameter that is not being passed correctly.

FBTAUD010E An event validation exception was encountered because all of the event data is not correctly filled in.

Explanation: This error occurs if any of the required elements in the event are not set.

System action: System will not audit this particular event and log an exception.

Administrator response: Check the encapsulated exception to solve the problem.

FBTCDS001E The received request is missing the required parameter: *parameter*

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTCDS002E Token exchange failed.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration. In addition, examine the trace logs to see why the token exchange failed.

FBTCDS003E The security token could not be decrypted.

Explanation: The encrypted security token could not be decrypted.

Administrator response: Ensure that the decryption keys and decryption parameters are configured properly for the provider that sent the message.

FBTCDS004E The security token signature could not be validated.

Explanation: The security token signature could not be validated.

Administrator response: Ensure that the validation keys are configured properly for the provider that sent the message.

FBTCDS005E The request was missing the TARGET parameter.

Explanation: The login page must contain a TARGET parameter either in the Query string or in a hidden input field.

System action: The operation will be halted.

Administrator response: Modify the login page to contain a TARGET parameter, which should point to the target SSO URL.

FBTCDS006E While processing action: *action* **the following configuration parameter was determined to be missing or incorrect:** *param*

Explanation: The current request could not be completed because the configuration is not valid.

System action: The request will be halted.

Administrator response: Validate that the system is configured correctly.

FBTCDS007E The current user making the request is not authenticated.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTCDS008E The Security Token Service was unable to generate a token for this request.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message, and the system configuration.

FBTCDS009E The card used for authentication to the STS mapped to the alias: ***action*** **and could not be mapped to a local user account.**

Explanation: The alias service could not resolve the alias generated from the token presented for authentication to a local user account. This may be because the alias was not written correctly when the card was created, or that the alias has been deleted from the alias service.

System action: The request will be halted.

Administrator response: Validate that the alias server is configured and working, and that the alias for the user exists.

FBTCDS010E The incoming request to the InfoCard STS has an AppliesTo address which does not contain the identity information of the relying party: *appliesTo*

Explanation: The AppliesTo element from the client should either not contain an AppliesTo element, or if it does, it must contain the identity information (including the X509 certificate) of the relying party. This can be caused if the metadata policy response to InfoCard does not contain the <wsaw:UsingAddressing/> directive.

System action: The request will be halted.

Administrator response: Validate that the configured metadata policy contains <wsaw:UsingAddressing/>

FBTCDS011E The incoming request to the InfoCard STS does not contain a valid authentication token for this federation.

Explanation: The incoming request may contain no authentication token, or it may contain an authentication token which does not match the authentication mechanism supported by this federation.

System action: The request will be halted.

Administrator response: Validate that the incoming request contains the correct authentication token.

FBTCDS012E The incoming metadata exchange request contains an invalid 'action' header in the SOAP request: *action*

Explanation: The incoming request contained an 'action' header other than: http://schemas.xmlsoap.org/ws/2004/09/transfer/Get

System action: The request will be halted.

Administrator response: Validate that the client is sending a valid metadata exchange request.

FBTCDS013E The incoming metadata exchange request contains an invalid 'to' header in the SOAP request: *to***. We were expecting our metadata exchange endpoint:** *mexEndpoint*

Explanation: The incoming request contained a 'to' header which did not match our metadata exchange endpoint.

System action: The request will be halted.

Administrator response: Validate that the client is sending a valid metadata exchange request.

FBTCDS014E The request for a card contained a support claim parameter in an invalid format: *sClaim*

Explanation: The incoming request contained a supported claim in an invalid format.

System action: The request will be halted.

Administrator response: Validate that the getcard HTML template has supported claims in the correct format.

FBTCDS015E The supplied card alias, *ppid***, is already in-use by another user.**

Explanation: The user supplied a self-issued card that is already associated with another user's account.

System action: The request will be halted.

Administrator response: No administrative response is necessary.

FBTCFG001E An error occurred while reading a configuration document.

Explanation: An attempt to read a configuration stream has failed.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager configuration.

FBTCFG002E The expected root for this document, type *documentroottype* was not found in the document.

Explanation: The expected document root was missing because the parsed configuration file does not contain the correct configuration document.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager configuration.

FBTCFG003E The configuration for the component *component* was not found in this document.

Explanation: The expected document root was missing because the parsed configuration file does not contain the correct configuration document.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager configuration.

FBTCFG004E An error occurred while saving a configuration document.

Explanation: An attempt to save a configuration stream has failed.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager environment configuration.

FBTCFG005E An error occurred while reading configuration information from file: *filename*.

Explanation: An attempt to read a configuration stream has failed.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager configuration.

FBTCFG006E The configuration file parser has encountered an unexpected exception: *exception text*.

Explanation: An attempt to read a configuration stream has failed.

System action: The configuration request will be halted.

Administrator response: Validate the Tivoli Federated Identity Manager configuration.

FBTCLI001E The configuration entry *entry* is not correct or not supported.

Explanation: The configuration entry is either not correct or not supported.

System action: The processing has been halted.

Administrator response: Check the documentation and ensure that the specified configuration entry is correct and supported.

FBTCLI002E The configuration entry *entry* is required and was not given.

Explanation: The required configuration entry was not given.

System action: The processing has been halted.

Administrator response: Check the documentation and ensure that all required configuration entries are given.

FBTCLI003E The *entry* entry and *entry* entry are not correct.

Explanation: The specified configuration entries are not correct.

System action: The processing has been halted.

Administrator response: Check the documentation and ensure that all required configuration entries are given correctly.

FBTCLI005E The properties file [*filename*] was not found.

Explanation: A required properties file was not given.

System action: The processing has been halted.

Administrator response: Ensure that the path given to the properties file is correct.

FBTCLI008E The upgrade finished with errors. Enable a more detailed trace to determine the problem.

Explanation: The upgrade of the configuration files failed.

System action: The processing has been halted.

Administrator response: To determine the problem, enable finer tracing and re-execute the upgrade tool.

FBTCLI010E The given source JAR is not the expected version.

Explanation: The given JAR file was not exported from the expected product version.

System action: The processing has been halted.

Administrator response: Ensure that the source JAR is from the expected product version.

FBTCLI026E Unable to create domain (*domain*)

Explanation: An error occurred creating the domain.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI032E Federation(*fed*) does not exist

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI033E Unable to create file (*file*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the name and path of the supplied file and make sure it can be written to.

FBTCLI034E File (*file*) not found

Explanation: See message.

System action: The processing has been halted.

Administrator response: Verify the file exists.

FBTCLI036E Partner (*partner*) does not exist in federation (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI043E The property you are trying to set, (*prop*), is not appropriate for role=(*fed*) and protocol=(*fed*) federation.

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI051E Unable to parse property (*lhs*=*rhs*) in file (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Verify the file exists.

FBTCLI054E Unable to import federation (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI055E Unable to import partner (*part*) into federation (*fed*) in domain *domain*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI056E Unable to get federation (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI058E Unable to delete federation (*fed*) in domain (*domain*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI059E No federations exist in domain (*domain*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI060E No partners exist for federation (*fed*) in domain (*domain*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI062E Federation (*fed*) does not exist in domain (*domain*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI065E Unable to delete partner (*partner*) in federation (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI066E Unable to delete all partners in federation (*fed*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Check the log files on the Tivoli Federated Identity Manager Management Service machine for errors.

FBTCLI068E Domain (*domain*) already exists

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI069E No domains exist

Explanation: See message.

System action: The processing has been halted.

Administrator response: Cerate a domain to proceed.

FBTCLI070E EAR File [*EAR File*] does not exist. The installation failed.

Explanation: The given EAR file did not exist, the installation could not continue.

System action: The processing has been halted.

Administrator response: Ensure that the EAR file is located at the expected location.

FBTCLI071W The IVT application failed to install, attempting to recover by removing any existing IVT applications.

FBTCLI074E Installation of IVT application failed.

Explanation: An error occurred while installing the IVT application and the installation did not complete.

System action: The processing has been halted.

Administrator response: Check the log for the cause of the error. If the error was not logged, enable debug tracing to determine the cause of the problem.

FBTCLI075E Usage: java -jar itfimbgha.jar -action <mode> [options] The itfimbgha tool has two modes of operation. Each mode uses different command line options. -action export: Used to gathering required configuration from the exported federation configuration archive. This option is used when running the tool on the node being replicated, to gather the required files. Options: -inputfile <file> (Required): The jar file created by federation configuration export. -outputfile <file> (Optional): The resultant archive containing the files needed to create a replica node. If it is not specified the output file will be ./bg_ha_files.jar. -action import: Used to import the configuration files from the archive file to the replica node. This option is used when running the tool on the replica node to put the required configuration files into place. Options: -inputfile <file> (Required): The jar file containing the output from running the tool in export mode. -wasprofiledir <directory> (Required): The absolute filepath to the WebSphere profile directory that Federated Identity Manager is running in.

Explanation: The options provided to the HA tool were not valid.

System action: The tool will exit without updating any configuration files.

Administrator response: Specify valid options to the spokeHA tool.

FBTCLI076E Directory (*directory*) does not exist

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI077E An unexpected error occurred: (*exception*)

Explanation: An unexpected error occurred. Check the logs for any errors.

System action: The processing has been halted.

Administrator response: No response required.

FBTCLI078E Could not delete: (*file*)

Explanation: See message.

System action: The processing has been halted.

Administrator response: Verify the file exists and can be deleted.

FBTCLI081E The input jar file (*file*) was not created by the Federated Identity Manager export function.

Explanation: The input jar file was not determined to have been created by the export feature in the Federated Identity Manager console.

System action: The Federated Identity Manager high availability tool will not continue.

Administrator response: Re-export the Federated Identity Manager configuration jar and run the high availability tool again.

FBTCLI082E The output jar file (*file*) could not be created by the high availability tool.

Explanation: An error occurred which prevented the high availability tool from completing successfully.

System action: The Federated Identity Manager high availability tool will not continue.

Administrator response: Check the log file for more details.

FBTCLI083E Failed to backup the Federated Identity Manager configuration files.

Explanation: An error occurred which prevented the high availability tool from backing up the current configuration.

System action: The Federated Identity Manager high availability tool will not continue.

Administrator response: Check the log file for more details.

FBTCLI088E The domain (*domain*) does not exist.

Explanation: See message.

System action: The processing has been halted.

Administrator response: No response required.

FBTCON001E An error occurred while modifying component host names and ports.

Explanation: This error occurs due to a problem writing to the console properties file.

System action: The system will leave the properties file unchanged.

Administrator response: Check the file console properties or try restarting the server.

FBTCON002E An error occurred retrieving the ISC launch service.

Explanation: The ISC launch service could not be retrieved.

System action: The system might have problems launching some pages and portlets.

Administrator response: See the exception stack trace.

FBTCON003E An error occurred while loading component host names and ports from the properties file.

Explanation: This error occurs due to a problem loading the console properties file.

System action: The console will be unable to communicate with the various components.

Administrator response: Check that the console properties file is in your classpath.

FBTCON004E The ISC launch service could not find the following page: *insert*

Explanation: An error occurred while launching a page using the ISC launch service.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON005E An error occurred while setting the trust service endpoint.

Explanation: This error can occur if the protocol is missing from the trust service endpoint (for example http://) or if your management context was invalidated.

System action: Trust service endpoint is left unchanged. The system rolls back the session to try to create a valid context.

Administrator response: Make sure the trust service endpoint is correctly formatted and includes the protocol (for example http://).

FBTCON006E An error occurred setting the identity service endpoint.

Explanation: This error can occur if the identity service endpoint is incorrectly formatted.

System action: The identity service endpoint is left unchanged

Administrator response: Make sure the identity service endpoint is correct.

FBTCON007E Error setting the Key Service endpoint

Explanation: This error can occur if the key service endpoint is incorrectly formatted.

System action: The key service endpoint is left unchanged.

Administrator response: Make sure that the key service endpoint is correct.

FBTCON008E An error occurred retrieving the component endpoint.

Explanation: This error occurs if there is a problem retrieving the trust service, identity service, or key service endpoint from the single sign-on protocol service.

System action: The console is unable to display the endpoint.

Administrator response: See the exception stack trace.

FBTCON009E An error occurred while creating a federation.

Explanation: A single sign-on protocol service encountered a problem creating a federation.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON010E An error occurred while committing the session in the single sign-on protocol service.

Explanation: The configuration changes could not be saved to the single sign-on protocol service.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON011E The token list could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON012E The partner list could not be retrieved from the single sign-on protocol service.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON013E The federation with ID *insert* could not be retrieved from the single sign-on protocol service.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON014E The list of identity mappings could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON015E The partner configurations could not be applied.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON016E The federation partners table could not be refreshed.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON017E The token table could not be filtered.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON018E An error occurred while creating a federation partner.

Explanation: The single sign-on protocol service encountered a problem while creating a federation partner.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON019E An error occurred while getting a list of federations from the single sign-on protocol service.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON020E An error occurred while deleting a federation: ***insert*****.**

Explanation: The single sign-on protocol service was unable to delete this federation.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON021E The list of token types could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON022E The identity mapping with ID *insert* **could not be retrieved from the trust service.**

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON023E An error occurred while committing a session in the trust service.

Explanation: The configuration changes could not be saved to the trust service.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON024E An error occurred while creating an identity mapping.

Explanation: The trust service encountered a problem while creating an identity mapping.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON025E The XSLT is not valid. The rule could not be applied.

Explanation: This error occurs if there was a problem parsing the XSLT.

System action: No action taken.

Administrator response: Check that your rule is correctly formatted XSL.

FBTCON026E The token with ID *insert* could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON027E The token configurations could not be applied.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON028E The token configuration could not be laid out.

Explanation: This error occurs when the console is unable to retrieve the configuration XML from the trust service.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON029E The type of the token could not be retrieved.

Explanation: An error occurred while trying to retrieve the type of this token from the trust service.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON030E The federation configurations could not be applied.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON031E The identity mapping configurations could not be applied.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON032E An error occurred while deleting identity mapping: *insert*.

Explanation: This error can occur if the identity mapping is being used in a module chain for a federation.

System action: No action taken.

Administrator response: Check that this identity mapping is not being used in any federations before deleting it.

FBTCON033E An error occurred while deleting token: *insert*.

Explanation: This error can occur if the token is being used in a module chain for a federation.

System action: No action taken.

Administrator response: Check that this token is not being used in any federations before deleting it.

FBTCON034E An error occurred while creating a token.

Explanation: A trust service encountered a problem while trying to create a token.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON035E An error occurred while rendering the token configuration layout.

Explanation: This error occurs when there is a problem parsing the token configuration XML that was retrieved from the trust service.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON036E The token type with id *insert* could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service or if the module type is not in the config repository.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running. Publish all module plugins to the config repository.

FBTCON037E The token type configurations could not be applied.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON038E An error occurred while deleting token type: *insert*.

Explanation: This error can occur if the token type is being used as the type for existing tokens.

System action: No action taken

Administrator response: Check that there are no existing tokens of this token type before deleting.

FBTCON039E An error occurred while creating a token type.

Explanation: This error can occur if the classname for the token module is not valid.

System action: No action taken.

Administrator response: Make sure that your classname specifies the full package name and class.

FBTCON040E You must enter a name for this federation.

Explanation: You cannot create a federation without a display name.

System action: No action taken.

Administrator response: Enter a display name for the federation in the appropriate text entry.

FBTCON041E You must select your role.

Explanation: You cannot select a federation without specifying your role (Identity Provider or Service Provider).

System action: No action taken.

Administrator response: Select the radio button corresponding to your role in the federation.

FBTCON042E You must select at least one federation service.

Explanation: You cannot create a federation without selecting at least one federation service (Web Single Sign-On, Provisioning, or SOAP Security, or a combination of these services).

System action: No action taken.

Administrator response: Select the check boxes corresponding to your desired federation services.

FBTCON043E You must select Single Sign-On protocol.

Explanation: You cannot configure this federation without selecting the Single Sign-On protocol (Liberty, WS-Federation, or SAML).

System action: No action taken.

Administrator response: Select the radio button corresponding to the protocol that you want to use for this federation.

FBTCON044E You must select a Liberty Single Sign-On profile.

Explanation: You cannot configure this federation without selecting a Liberty Single Sign-On profile (Browser Post, Browser Artifact).

System action: No action taken.

Administrator response: Select the liberty profiles that you want to use for this federation.

FBTCON045E You must select the federation to which you want to add a new partner.

Explanation: You cannot create a partner without selecting an existing federation.

System action: No action taken

Administrator response: Select the federation to which you want to add a partner from the table. If no federations exist, you must create one before creating a partner.

FBTCON046E Must enter the name of your partner company

Explanation: The company name you enter is used as a display name for this partner, and is thus a required field.

System action: No action taken

Administrator response: Enter the name of your partner company in the appropriate text entry field.

FBTCON047E You must select an identity mapping instance for this federation.

Explanation: The identity mapping is required to map your source token to the federated token.

System action: No action taken.

Administrator response: Select an existing identity mapping instance from the table or create a new one.

FBTCON048E You must enter the WS-Federation Realm.

Explanation: The WS-Federation realm is a required field.

System action: No action taken.

Administrator response: Enter the WS-Federation realm in the appropriate text entry field.

FBTCON049E You must enter the WS-Federation Endpoint.

Explanation: The WS-Federation endpoint is a required field.

System action: No action taken.

Administrator response: Enter the WS-Federation endpoint in the appropriate text entry field.

FBTCON050E You must enter the Provider ID.

Explanation: The Provider ID is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Provider ID in the appropriate text entry field.

FBTCON051E You must enter the SOAP Endpoint.

Explanation: The SOAP Endpoint is required for the Liberty profile you selected.

System action: No action taken.

Administrator response: Enter the SOAP Endpoint in the appropriate text entry field.

FBTCON052E You must enter the Single Sign-On Service URI.

Explanation: The Single Sign-On Service URI is required for the Liberty protocol.

System action: No action taken

Administrator response: Enter the Single Sign-On Service URI in the appropriate text entry field.

FBTCON053E You must enter the Register Name Identifier Service URI.

Explanation: The Register Name Identifier Service URI is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Register Name Identifier Service URI in the appropriate text entry field.

FBTCON054E You must enter the Single Logout Service URI.

Explanation: The Single Logout Service URI is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Single Logout Service URI in the appropriate text entry field.

FBTCON055E You must enter the Single Logout Service Return URI.

Explanation: The Single Logout Service Return URI is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Single Logout Service Return URI in the appropriate text entry field.

FBTCON056E You must enter the Assertion Consumer URI.

Explanation: The Assertion Consumer URI is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Assertion Consumer URI in the appropriate text entry field.

FBTCON057E You must select a token for this federation.

Explanation: A token instance is required.

System action: No action taken.

Administrator response: Select an existing token instance from the table or create a new one.

FBTCON058E You must enter a name for this identity mapping.

Explanation: A display name for the mapping instance is required.

System action: No action taken.

Administrator response: Enter a name for the identity mapping in the appropriate text entry field.

FBTCON059E You must select the token type for this token instance.

Explanation: The token type is required for configuration.

System action: No action taken.

Administrator response: Select a token type from the table.

FBTCON060E You must enter a name for this token.

Explanation: A display name for the token is required.

System action: No action taken.

Administrator response: Enter a name for this token in the appropriate text entry field.

FBTCON061E You must enter a name for this token type.

Explanation: A display name for the token type is required.

System action: No action taken.

Administrator response: Enter a name for this token type in the appropriate text entry field.

FBTCON062E You must enter the classname for the module.

Explanation: The full classname including package name must be specified.

System action: No action taken.

Administrator response: Enter the classname in the appropriate text entry field.

FBTCON063E Class not found: *insert*

Explanation: The trust service was unable to find the class that you specified for this module.

System action: No action taken.

Administrator response: Check that you have entered the full and correct classname, including package name. Check that this class exists at the trust service.

FBTCON064E An error occurred while deleting partner: *insert***.**

Explanation: The single sign-on protocol service was unable to delete this partner.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON065E You must enter a name for this mapping rule.

Explanation: A display name for the mapping rule is required.

System action: No action taken.

Administrator response: Enter a name for the XSLT rule in the appropriate text entry field.

FBTCON066E The service manager cannot determine whether trace is enabled for component *insert***.**

Explanation: An exception was thrown when trying to get trace information from the service manager.

System action: No action taken.

Administrator response: Make sure that the serviceability management EAR is deployed on this server.

FBTCON067E The maximum trace file size for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the maximum trace file size from the service manager.

System action: No action taken.

Administrator response: Make sure that the serviceability management EAR is deployed on this server.

FBTCON068E The maximum message file size for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the maximum message file size from the service manager.

System action: No action taken.

Administrator response: Make sure that the serviceability management EAR is deployed on this server.

FBTCON069E The trace level for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the trace level from the service manager.

System action: No action taken.

Administrator response: Make sure that the serviceability management EAR is deployed on this server.

FBTCON070E The message level for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the message type from the service manager.

System action: No action taken.

Administrator response: Make sure the serviceability management EAR is deployed on this server.

FBTCON071E An error occurred when trying to apply logging configurations.

Explanation: An exception was thrown by the service manager when trying to apply logging configurations.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON072E The maximum audit file size for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the maximum audit file size from the service manager.

System action: No action taken.

Administrator response: Make sure the serviceability management EAR is deployed on this server.

FBTCON073E The audit level for this server cannot be retrieved.

Explanation: An exception was thrown when trying to get the audit level from the service manager.

System action: No action taken.

Administrator response: Make sure the serviceability management EAR is deployed on this server.

FBTCON074E An error occurred when trying to apply auditing configurations.

Explanation: An exception was thrown by the service manager when trying to apply auditing configurations.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON075E The ISC launch service could not find the following portlet: *insert*

Explanation: An error occurred launching a portlet using the ISC launch service.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON076E The trace configuration for component *insert* **cannot be applied.**

Explanation: An exception was thrown by the service manager when trying to set trace information.

System action: No action taken.

Administrator response: Make sure the serviceability management EAR is deployed on this server.

FBTCON077E You must select the metadata input option.

Explanation: You cannot proceed without selecting the metadata input option.

System action: No action taken.

Administrator response: Select the appropriate button.

FBTCON078E You must enter LECP Provider Name.

Explanation: The LECP Provider Name is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the LECP Provider Name in the appropriate text entry field.

FBTCON079E You must enter the RNI Return URL.

Explanation: The RNI Return URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the RNI Return URL in the appropriate text entry field.

FBTCON080E You must enter the RNI Service URL.

Explanation: The RNI Service URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the RNI Service URL in the appropriate text entry field.

FBTCON081E You must enter the FTN Return URL.

Explanation: The FTN Return URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the FTN Return URL in the appropriate text entry field.

FBTCON082E You must enter the FTN Service URL.

Explanation: The FTN Service URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the FTN Service URL in the appropriate text entry field.

FBTCON083E You must enter SLO Return URL.

Explanation: The SLO Return URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the SLO Return URL in the appropriate text entry field.

FBTCON084E You must enter SLO Service URL.

Explanation: The SLO Service URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the SLO Service URL in the appropriate text entry field.

FBTCON085E You must enter IPI Service URL.

Explanation: The IPI Service URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the IPI Service URL in the appropriate text entry field.

FBTCON086E You must enter the Common DNS Domain.

Explanation: The Common DNS Domain is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Common DNS Domain in the appropriate text entry field.

FBTCON087E You must enter the name of your company.

Explanation: The company name you enter is used as a display name, and is therefore a required field.

System action: No action taken.

Administrator response: Enter the name of your company in the appropriate text entry field.

FBTCON088E You must enter a base URL for your protocol endpoints.

Explanation: A common base URL is required for all protocol endpoints.

System action: No action taken.

Administrator response: Enter your base URL in the appropriate text entry field.

FBTCON089E You must enter a Signing Key Identifier.

Explanation: An identifier for your signing key is required.

System action: No action taken.

Administrator response: Enter your Signing Key Identifier in the appropriate text entry field.

FBTCON090E An error occurred when trying to retrieve SAML properties.

Explanation: An exception was encountered when trying to retrieve SAML properties. This error could be caused by improperly formatted endpoint URLs.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON091E An error occurred while importing the Liberty metadata file. Check that the file contains correctly formatted Liberty metadata.

Explanation: The specified metadata file could not be imported. This error could be the result of malformed metadata.

System action: No action taken.

Administrator response: Check that your metadata file conforms to the Liberty 1.1 metadata schema. See the exception stack trace for more details.

FBTCON092E An error occurred while exporting the Liberty metadata file.

Explanation: An exception was encountered when trying to export this federation to a Liberty metadata file.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON093E You must specify the metadata file to import.

Explanation: No metadata file was specified to import. Enter the file location in the file chooser.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON094E The partner's status could not be updated.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON095E You must enter Provider ID.

Explanation: The provider ID is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Provider ID in the appropriate text entry field.

FBTCON096E All endpoints must begin with base URL: ***insert*****.**

Explanation: Every protocol endpoint must be prefixed with the base URL defined on the previous screen.

System action: No action taken.

Administrator response: Make sure all endpoints begin with the same base URL defined on the previous screen.

FBTCON097E The Liberty Message Lifetime must be at least 60 seconds.

Explanation: The Liberty Protocols and Schema Specification defines a minimum Liberty Message Lifetime of 60 seconds.

System action: No action taken.

Administrator response: Enter a value of 60 seconds or greater for the Liberty Message Lifetime.

FBTCON098E Liberty Artifact Lifetime must be at least 120 seconds.

Explanation: The Liberty Protocols and Schema Specification defines a minimum Liberty Artifact Lifetime of 120 seconds.

System action: No action taken.

Administrator response: Enter a value of 120 seconds or greater for the Liberty Artifact Lifetime.

FBTCON099E The SOAP Client Authentication Key Password and Re-enter SOAP Client Authentication Key Password fields must match.

Explanation: The SOAP Client Authentication Key Password must be entered twice for accuracy. The two password fields contain different values.

System action: No action taken.

Administrator response: Re-enter your SOAP Client Authentication Key Password in both password fields.

FBTCON100E The New SOAP Client Authentication Key Password and Re-enter New SOAP Client Authentication Key Password fields must match.

Explanation: The New SOAP Client Authentication Key Password must be entered twice for accuracy. The two password fields contain different values.

System action: No action taken.

Administrator response: Re-enter your New SOAP Client Authentication Key Password in both password fields.

FBTCON101E The New SOAP Client Authentication Key Password field cannot be blank.

Explanation: You must enter a value for the New SOAP Client Authentication Key Password.

System action: No action taken.

Administrator response: Enter your New SOAP Client Authentication Key Password in both password fields or click 'Cancel' if you do not want to change the password.

FBTCON102E The Signing Key Password and Re-enter Signing Key Password fields must match.

Explanation: The Signing Key Password must be entered twice for accuracy. The two password fields contain different values.

System action: No action taken.

Administrator response: Re-enter your Signing Key Password in both password fields.

FBTCON103E An error occurred while setting the SOAP Client Authentication Key Password.

Explanation: An exception was encountered when trying to set the SOAP Client Authentication Key Password.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON104E An error occurred while deleting a module chain: ***insert*****.**

Explanation: This error can occur if the module chain is being used in a federation.

System action: No action taken.

Administrator response: Check that this module chain is not being used in any federation before deleting.

FBTCON105E The chain mapping list could not be retrieved from the trust service.

Explanation: This error can occur if the console is unable to communicate with the trust service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the trust service. Check that the trust service is running.

FBTCON106E The New Signing Key Password and Re-enter New Signing Key Password fields must match.

Explanation: The New Signing Key Password must be entered twice for accuracy. The two password fields contain different values.

System action: No action taken.

Administrator response: Re-enter your New Signing Key Password in both password fields.

FBTCON107E The New Signing Key Password field cannot be blank.

Explanation: You must enter a value for the New Signing Key Password.

System action: No action taken.

Administrator response: Enter your New Signing Key Password in both password fields or click 'Cancel' if you do not want to change the password.

FBTCON108E An error occurred while setting the Signing Key Password.

Explanation: An exception was encountered when trying to set the Signing Key Password.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON109E You must enter a Verification Key Identifier.

Explanation: An identifier for the key that will be used to verify your partner's signature is required.

System action: No action taken.

Administrator response: Enter the Verification Key Identifier in the appropriate text entry field.

FBTCON110E You must enter the Common Domain Cookie Service URL.

Explanation: The Common Domain Cookie Service URL is required for the Liberty protocol.

System action: No action taken.

Administrator response: Enter the Common Domain Cookie Service URL in the appropriate text entry field.

FBTCON111E The Common Domain Cookie Service URL must use the Common DNS Domain.

Explanation: The Common Domain Cookie Service URL must include the Common DNS Domain.

System action: No action taken.

Administrator response: Modify the Common Domain Cookie Service URL, or Common DNS Domain, or both so that the Common Domain Cookie Service URL includes with the Common DNS Domain.

FBTCON112E Error deleting key: ***insert*****.**

Explanation: This error can occur if the key is being used in a federation.

System action: No action taken

Administrator response: Check that this key is not being used in any federations before deleting.

FBTCON113E Error committing session in Key Encryption Signature Service

Explanation: Could not save the configuration changes to the Key Encryption Signature Service

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON114E Error deleting keystore: ***insert*****.**

Explanation: This error can occur if the keys in this keystore are being used in a federation.

System action: No action taken

Administrator response: Check that there are no keys in this keystore that are being used in any federations before deleting.

FBTCON115E Must enter a name for this module chain.

Explanation: A display name for the module chain is required.

System action: No action taken

Administrator response: Enter a name for this module chain in the appropriate text entry field.

FBTCON116E Must enter at least one of the following: Applies To URI, Issuer URI

Explanation: Either an Applies To URI or an Issuer URI is required.

System action: No action taken

Administrator response: Enter an Applies To URI, an Issuer URI, or both in the appropriate text entry fields.

FBTCON117E Could not get chain mapping request type list from the Trust Service

Explanation: This error can occur if the console is unable to communicate with the Trust Service

System action: No action taken

Administrator response: Check the Service Configurations to ensure that you have the correct hostname and port for the Trust Service. Check that the Trust Service is running.

FBTCON118E Error adding module chain

Explanation: Trust Service encountered a problem adding module chain.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON119E Could not get chain mapping with id *insert* **from the Trust Service**

Explanation: This error can occur if the console is unable to communicate with the Trust Service

System action: No action taken

Administrator response: Check the Service Configurations to ensure that you have the correct hostname and port for the Trust Service. Check that the Trust Service is running.

FBTCON120E Error occurred when trying to retrieve the Module Chain properties.

Explanation: An exception was encountered when trying to retrieve the Module Chain properties.

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON121E Could not apply module chain properties

Explanation: This error can occur if the console is unable to communicate with the Trust Service

System action: No action taken

Administrator response: Check the Service Configurations to ensure that you have the correct hostname and port for the Trust Service. Check that the Trust Service is running.

FBTCON122E Could not upload file

Explanation: Encountered a FileUploadException

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON123E Error creating a WSSM Partner

Explanation: Encountered a problem creating a WSSM partner

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON124E Error getting list of Web Services Security partners from the Management Service

Explanation: This error can occur if the console is unable to communicate with the Management Service

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON125E Error rolling back session

Explanation: Could not save the configuration changes to the Management Service

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON127W In order to change the current domain, all open Management pages must be closed. Continue?

Explanation: If all open pages are closed, unsaved changed may be lost.

System action: The system will close any open Management pages and change the current management domain to the selected domain.

Administrator response: Press OK to proceed, or Cancel to leave all Management pages open and not change the current management domain.

FBTCON128E No management domains are defined. You must define and activate a domain in order to proceed.

Explanation: There are no management domains defined. In order to manage a domain, a domain must be defined and activated.

System action: No action taken

Administrator response: Press the Change Domain button to define and activate a domain.

FBTCON129E No domain is currently active. You must activate a domain in order to proceed.

Explanation: There are defined domains, but none are currently active. In order to manage a domain, a domain must be activated.

System action: No action taken

Administrator response: Press the Change Domain button to activate a domain.

FBTCON130E Error loading the partner properties.

Explanation: Exception encountered while loading the partner properties.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON131E Error loading the federation properties.

Explanation: Exception encountered while loading the federation properties.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON137E An error occurred during the deploy operation.

Explanation: The Runtime could not be deployed to all nodes in the domain.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON138E An error occurred during the configure operation. If the domain is using Tivoli Access Manager check that the policy server is reachable and that you have provided the correct username and password.

Explanation: The configure operation failed while configuring one of the specified nodes.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON139E An error occured during the enable operation.

Explanation: The configure operation failed while enabling one of the specified nodes.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON140E An error occured during the remove operation.

Explanation: The Runtime could not be removed from all nodes in the domain.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON141E An error occured during the unconfigure operation.

Explanation: The configure operation failed while unconfiguring one of the specified nodes.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON142E An error occured during the disable operation.

Explanation: The configure operation failed while disabling one of the specified nodes.

System action: No action taken

Administrator response: Check the exception stack trace in the logs.

FBTCON143E Could not get the list of Web Services Security Applications

Explanation: Unable to retrieve the property sets for the WSSM applications.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON144E Error exporting key

Explanation: Management Service encountered an exception exporting the key.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON145E Error importing key. Please make sure that the correct file format was provided.

Explanation: Management Service encountered an exception importing the key.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON146E Error listing keys

Explanation: Management Service encountered an exception listing keys.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON147E Error listing keystores

Explanation: Management Service encountered an exception listing keystores.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON148W Remove domain *insert* from server?

Explanation: Deleting a domain from the server will delete configuration files on the domain. You have the option to remove the domain from the console without deleting the domain configuration from the server.

System action: No action taken

Administrator response: Choose the appropriate action from the message box.

FBTCON149E One or more nodes in domain *insert* are configured or have the Runtime deployed. Unconfigure all nodes and remove the Runtime before deleting this domain.

Explanation: A domain cannot be removed without ensuring that all nodes are unconfigured and the Runtime is removed from the nodes.

System action: No action taken

Administrator response: Go to the Runtime Node Management task and ensure all nodes are unconfigured and the Runtime is removed from the domain.

FBTCON150E Error committing session changes

Explanation: Could not save the configuration changes to the Management Service

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON151E The field *insert* requires a value

Explanation: The field specified in the message is empty and requires a value. Please enter an appropriate value.

System action: No action taken

Administrator response: Enter the appropriate value for the field marked invalid.

FBTCON152E The port number specified for field *insert* must be between 0 and 65536

Explanation: The value entered for a port is outside of the legal values for port numbers. The port must be between 0 and 65536.

System action: No action taken

Administrator response: Enter the appropriate port number.

FBTCON153E A Domain cannot be named default. Please choose another name.

Explanation: While creating a domain, the name default is reserved for system use. Please choose a different domain name.

System action: No action taken

Administrator response: Choose a domain name other than default

FBTCON154E Please select the type of WebSphere environment.

Explanation: You must choose either a clustered or single server environment for the Domain. The choice must match the environment where the Management Service is deployed.

System action: No action taken

Administrator response: Choose the appropriate environment type.

FBTCON155E The server *insert* listening on port *insert* cannot be contacted. Check the server settings and try again.

Explanation: Cannot open a socket to the server and port specified. This indicates ether incorrect server settings or the server is unreachable.

System action: No action taken

Administrator response: Check the server settings and try again.

FBTCON156E An error occured while importing the domain configuration archive. Check the server logs for more information.

Explanation: An unknown error occured while importing the domain configuration archive. An error will be logged in the server logs.

System action: No action taken

Administrator response: Check the logs on the console and server for an exception.

FBTCON159E A federation with display name *insert* already exists.

Explanation: An existing federation uses the display name that you entered. Each federation must have a unique display name.

System action: No action taken

Administrator response: Please enter a different display name for this federation.

FBTCON160E Error occurred when verifying the display name.

Explanation: An exception was encountered when checking the uniqueness of the display name you entered.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON161E Error occurred when creating domain *insert*.

Explanation: An exception was encountered when creating the specified domain.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON162E The Assertion Consumer Service URL *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an AppliesTo field that matches the Assertion Consumer Service URL you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different Assertion Consumer Service URL.

FBTCON163E The WS-Federation Realm *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an Issuer field that matches the WS-Federation Realm you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different WS-Federation Realm.

FBTCON164E The WS-Federation Endpoint *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an AppliesTo field that matches the WS-Federation Endpoint you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different WS-Federation Endpoint.

FBTCON165E The Provider ID *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an Issuer field that matches the Provider ID you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different Provider ID.

FBTCON166E An error was encountered while retrieving environment settings. Check the environment settings and try again.

Explanation: There was an error communicating with the management service endpoint while attempting to list the clusters or servers in the environment. This error can be caused by: 1) Incorrect WebSphere Global Security settings. Check the WebSphere Global Security settings (if applicable) and try again. 2) An unstable WebSphere environment. Restart the WebSphere environment and try again.

System action: No action taken

Administrator response: Ensure all settings are correct and try again. If this message reappears, restart the WebSphere environment and try again.

FBTCON167E One or more nodes in this domain are configured. Unconfigure all nodes before undeploying the Runtime.

Explanation: The Runtime cannot be undeployed without ensuring that all nodes are unconfigured.

System action: No action taken

Administrator response: Ensure all nodes are unconfigured before attempting to remove the Runtime.

FBTCON168E The Issuer address *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an Issuer field that matches the issuer you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different Issuer address.

FBTCON169E The Applies To address *insert* is already being used.

Explanation: An existing Trust Service Chain Mapping contains an AppliesTo field that matches the Applies To you entered. This field must be unique in order for the Trust Service to invoke the correct module chain.

System action: No action taken

Administrator response: Please enter a different WS-Federation Endpoint.

FBTCON170E Must select a file format

Explanation: Must select a format (PEM or PKCS#12) for the keystore file you want to import.

System action: No action taken

Administrator response: Make the appropriate radio button selection for the format of the file you want to import.

FBTCON171E Must select a keystore for your partner's key.

Explanation: The liberty metadata that you imported for your partner contains KeyInfo that must be saved in a keystore. Please choose the keystore where you would like to store it.

System action: No action taken

Administrator response: Select a keystore from the table.

FBTCON172E Must enter a keystore password.

Explanation: A password for the keystore must be supplied in order to perform operations on this keystore.

System action: No action taken

Administrator response: Enter the keystore password in the appropriate text entry field.

FBTCON173E Must supply a label for your partner's key.

Explanation: Your partner's key will be stored in the keystore you select under the label that you give it. Please enter the label that you would like to give to your partner's key.

System action: No action taken

Administrator response: Enter a label for your partner's key in the appropriate text entry field.

FBTCON174E More than one key alias exists in this file. Please restart the wizard and select the Contains multiple key pairs checkbox.

Explanation: If your file contains multiple key aliases, the wizard does not know which alias to import. Checking the appropriate checkbox to indicate that multiple aliases exist allows the wizard to prompt you for the specific alias that you would like to import.

System action: No action taken

Administrator response: Restart the wizard and select the Contains multiple key pairs checkbox.

FBTCON175E Must enter a New Key Label.

Explanation: The key you are importing must be stored under a key label. You can choose any label you like for this key.

System action: No action taken

Administrator response: Enter a label for this key in the appropriate text entry field.

FBTCON176E Must enter the name of the key that you want to import.

Explanation: You selected the Contains multiple key pairs checkbox, which means that you must specify the key pair you want to import by providing the key label. If there are no key labels in the file, you should restart the wizard and unselect the Contains multiple key pairs checkbox.

System action: No action taken

Administrator response: Enter the name of the key that you want to import in the appropriate text entry field.

FBTCON177E Key label does not exist in this file.

Explanation: The key label that you specified does not exist in the keystore file you provided, so the Key Service is unable to import this key.

System action: No action taken

Administrator response: Verify that you have the correct key label. If there are no key aliases in the file, leave the field blank.

FBTCON178E Must provide a valid keystore file to upload.

Explanation: You entered an empty keystore file to upload or the keystore file could not be found. Please verify the location and contents of the keystore file you want to upload and try again.

System action: No action taken

Administrator response: Browse to a valid keystore file on your local system to upload.

FBTCON179E Incorrect keystore password.

Explanation: The password you supplied for the keystore is incorrect. Please try again.

System action: No action taken

Administrator response: Enter the correct keystore password in the appropriate text entry field.

FBTCON180E Must enter a Module Name.

Explanation: You must enter the name a of a plugin module that exists in the configuration repository for the current domain.

System action: No action taken

Administrator response: Please enter a Module Name in the appropriate text entry field.

FBTCON181E Must enter a Module Version.

Explanation: You must enter the version number of the module.

System action: No action taken

Administrator response: Please enter a Module Version in the appropriate text entry field.

FBTCON182E Error creating keystore.

Explanation: The system encountered an error while trying to create a new keystore.

System action: No action taken

Administrator response: Please check the console and Management Service logs for more information.

FBTCON183E Keystore import failed. The keystore is invalid or the password is incorrect.

Explanation: The system encountered an error while trying to import the keystore.

System action: No action taken

Administrator response: Please check the console and Management Service logs for more information.

FBTCON184W Was not able to import all the keys in the keystore because the keystore password does not match the password for all contained keys.

Explanation: The Key Service only supports keystores with a single password. All keys in the keystore must have the same password as the keystore itself.

System action: No action taken

Administrator response: Please view the keys in the newly imported keystore to verify the contents.

FBTCON185E Must enter an Exposed Class ID.

Explanation: You must enter the Exposed Class ID that is used to identify this module in module.xml.

System action: No action taken

Administrator response: Please enter an Exposed Class ID in the appropriate text entry field.

FBTCON186E *insert* **is not a valid key identifier. Please use the Key Service management page to view all existing keys.**

Explanation: You have entered a key identifier for a key does not exist in the Key Service. Use the Key Service management to find an existing key.

System action: No action taken

Administrator response: Please enter a valid key identifier in the appropriate text entry field.

FBTCON187E Must fill in all required values.

Explanation: You have left a required field blank on the token configuration screen. Please fill in all required fields.

System action: No action taken

Administrator response: Please fill in all required fields

FBTCON188E Must select a signing key. Select a key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a signing key.

FBTCON189E Must select a key for SOAP Server Certificate Validation. Select a key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a key for validating your partner's server certificate.

FBTCON190E Must select a client certificate for SOAP. Select a key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You selected the check box for Client Certificate Authentication, which means that you are required to choose a client certificate. You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a key for client certificate authentication.

FBTCON191E Must enter a username for Client Basic Authentication.

Explanation: You have selected the checkbox for Client Basic Authentication, which requires a username and password. You must enter input values for both of these fields.

System action: No action taken

Administrator response: Please enter the username for Client Basic Authentication in the appropriate text entry field.

FBTCON192E Must enter a password for Client Basic Authentication.

Explanation: You have selected the checkbox for Client Basic Authentication, which requires a username and password. You must enter input values for both of these fields.

System action: No action taken

Administrator response: Please enter the password for Client Basic Authentication in the appropriate text entry field.

FBTCON193E Must enter a keystore name.

Explanation: You must give a name to the keystore you are importing.

System action: No action taken

Administrator response: Enter a name for the keystore in the appropriate text entry field.

FBTCON194E Must select a keystore type.

Explanation: Must specify what this keystore will be used for. It can be designated for either Signing/Encryption Keys or CA Certificates.

System action: No action taken

Administrator response: Make a radio button selection for the keystore type.

FBTCON195E Must select a key for validating your partner's signature. Select a key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a key for validating your partner's signature.

FBTCON196E *insert* **field cannot contain whitespace.**

Explanation: You have entered whitespace in a field that should not contain whitespace characters.

System action: No action taken

Administrator response: Please remove all whitespace from this field.

FBTCON197W Recent configuration changes need to be reloaded to the Tivoli Federated Identity Manager runtime. All configuration changes will not take effect until the reload completes.

Explanation: In order for the configuration changes made to take effect, you must restart WebSphere.

System action: No action taken

Administrator response: Please select whether to restart WebSphere now, or dismiss this message. If you dismiss this message, you will not be reminded again. If you have deployed FIM in a cluster, your cluster will be ripple started; single servers will be restarted individually. See the Runtime Node Management page for node status.

FBTCON198E An error ocurred when modifying the domain properties on the server.

Explanation: An attempt to modify domain properties on the server failed. Check that the Management Service is running and try again.

System action: No action taken

Administrator response: Check the server logs for more information about the error.

FBTCON199E A chain mapping with the given AppliesTo and Issuer values already exists.

Explanation: A chain mapping with the given AppliesTo-Issuer pairing already exists. Remove the existing mapping or choose a different pairing.

System action: No action taken

Administrator response: Determine if the new chain mapping is different from the one that already exists. Resolve the error by either removing the current mapping or using the current mapping.

FBTCON200W Warning: This domain is currently being managed by multiple users.

Explanation: When multiple users are working on the same domain, this may cause undesireable results. For example, someone could restart the domain while you are working on it. Make sure when you are finished working to log out of the console so this message is cleared immediately for other people.

System action: No action taken

Administrator response: Make sure you coordinate with the other console users so you don't clobber each others work.

FBTCON201E You must enter the Artifact Resolution Service URL.

Explanation: The Artifact Resolution Service URL is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the Artifact Resolution Service URL in the appropriate text entry field.

FBTCON202E You must enter the Artifact Cache Lifetime.

Explanation: The Artifact Cache Lifetime is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the Artifact Cache Lifetime in the appropriate text entry field.

FBTCON203E You must enter the Intersite Transfer Service URL.

Explanation: The Intersite Transfer Service URL is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the Intersite Transfer Service URL in the appropriate text entry field.

FBTCON204E You must enter the Source ID.

Explanation: The Source ID is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the Source ID in the appropriate text entry field.

FBTCON205E You must enter the Assertion Consumer Service URL.

Explanation: The Assertion Consumer Service URL is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the Assertion Consumer Service URL in the appropriate text entry field.

FBTCON206E You must enter the SOAP Server Validation Certificate.

Explanation: The SOAP Server Validation Certificate is required for the SAML profile you selected.

System action: No action taken.

Administrator response: Enter the SOAP Server Validation Certificate in the appropriate text entry field.

FBTCON207E You must enter the SOAP Client Certificate for Authentication.

Explanation: You have selected the checkbox for Client Certificate Authentication, which requires a SOAP Client Certificate for Authentication name. You must enter a value.

System action: No action taken.

Administrator response: Enter the SOAP Client Certificate for Authentication in the appropriate text entry field.

FBTCON208E An error occurred while exporting the SAML metadata file.

Explanation: An exception was encountered when trying to export this federation to a SAML metadata file.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON209E An error occurred while importing the SAML metadata file. Check that the file contains correctly formatted SAML metadata.

Explanation: The specified metadata file could not be imported. This error could be the result of malformed metadata.

System action: No action taken.

Administrator response: Check that your metadata file conforms to the SAML 2.0 metadata schema. See the exception stack trace for more details.

FBTCON211E Failed to upload the mapping rule.

Explanation: Encountered a problem when uploading the mapping rule.

System action: No action taken

Administrator response: See the exception stack trace.

FBTCON212E Failed to build the Federation Summary panel.

Explanation: Encountered a problem when building the summary panel.

System action: No action taken

Administrator response: See the exception stack trace and try to build the federation again.

FBTCON213E A partner with the AppliesTo, *insert*, and Issuer, *insert*, already exists.

Explanation: A partner with the given AppliesTo-Issuer pairing already exists. Remove the existing partner or choose a different pairing.

System action: No action taken

Administrator response: Determine if the new partner is different from the one that already exists. Resolve the error by either removing the current partner or ensuring that your partner's configuration is correct.

FBTCON214E The Source ID does not meet the requirements for a SAML Source ID.

Explanation: The Source ID must be a valid Base64 encoded value, 28 characters long.

System action: No action taken.

Administrator response: Ensure that the string is of the correct format and try again.

FBTCON215E Must select at least one Single Sign-On Binding (Browser Artifact, Browser POST, Browser Redirect, Enhanced Client Proxy)

Explanation: No binding was selected for Single Sign-On.

System action: No action taken.

Administrator response: Select one or more bindings for Single Sign-On.

FBTCON216E Must select at least one Name Identifier Management Binding (HTTP Redirect, HTTP POST, Artifact, SOAP)

Explanation: The checkbox to enable Name Identifier Management was checked, but no binding was selected.

System action: No action taken.

Administrator response: Select one or more bindings for Name Identifier Management or uncheck the Name Identifier Management enablement checkbox if you do not want to support this profile.

FBTCON217E Must select at least one Single Logout Binding (HTTP Redirect, HTTP POST, Artifact, SOAP)

Explanation: The checkbox to enable Single Logout was checked, but no binding was selected.

System action: No action taken.

Administrator response: Select one or more bindings for Single Logout or uncheck the Single Logout enablement checkbox if you do not want to support this profile.

FBTCON218E Must enter a value for Common Domain Name

Explanation: No value was entered for Common Domain Name.

System action: No action taken.

Administrator response: Enter a value for Common Domain Name.

FBTCON219E Must enter a value for Common Domain Service Host

Explanation: No value was entered for Common Domain Service Host.

System action: No action taken.

Administrator response: Enter a value for Common Domain Service Host.

FBTCON220E Must enter a value for Common Domain Cookie Lifetime

Explanation: No value was entered for Common Domain Cookie Lifetime.

System action: No action taken.

Administrator response: Enter a value for Common Domain Cookie Lifetime.

FBTCON221E Must enter an integer value for Common Domain Cookie Lifetime

Explanation: The value entered for Common Domain Cookie Lifetime is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for Common Domain Cookie Lifetime.

FBTCON222E Must enter a value for Message Lifetime

Explanation: No value was entered for Message Lifetime.

System action: No action taken.

Administrator response: Enter a value for Message Lifetime.

FBTCON223E Must enter a value for Artifact Lifetime

Explanation: No value was entered for Artifact Lifetime.

System action: No action taken.

Administrator response: Enter a value for Artifact Lifetime.

FBTCON224E Must enter a value for Session Timeout

Explanation: No value was entered for Session Timeout.

System action: No action taken.

Administrator response: Enter a value for Session Timeout.

FBTCON225E Must enter an integer value for Message Lifetime

Explanation: The value entered for Message Lifetime is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for Message Lifetime.

FBTCON226E Must enter an integer value for Artifact Lifetime

Explanation: The value entered for Artifact Lifetime is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for Artifact Lifetime.

FBTCON227E Must enter an integer value for Session Timeout

Explanation: The value entered for Session Timeout is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for Session Timeout.

FBTCON228E Must enter a value for SOAP Endpoint URL

Explanation: SOAP Endpoint URL is a required value.

System action: No action taken.

Administrator response: Enter a value for SOAP Endpoint URL.

FBTCON229E Must select a keystore for your partner's key.

Explanation: The metadata that you imported for your partner contains KeyInfo that must be saved in a keystore. Please choose the keystore where you would like to store it.

System action: No action taken

Administrator response: Select a keystore from the table.

FBTCON230E Must enter a value for Default Post-Authentication Target URL

Explanation: Default Post-Authentication Target URL is a required value.

System action: No action taken

Administrator response: Enter a value for Default Post-Authentication Target URL.

FBTCON231E One of appliesTo address, issuer address or token type field must have a value.

Explanation: The appliesTo address or issuer address must have a value if the token type is not specified.

System action: No action taken.

Administrator response: Enter a value for the appropriate fields.

FBTCON232E The table cannot be reordered. The order entry *insert* is not a number.

Explanation: The text field for ordering the table must be a number.

System action: No action taken.

Administrator response: Enter a number for the appropriate fields.

FBTCON233W The module chain you have assembled does not meet the recommended Trust Service module chain structure. It is recommended that either one of the following 2 conditions be met: 1.The chain consists of only one module and the mode on that module is either Issue or Validate. 2.The chain consists of modules matching the following mode sequence: Validate-Map-...-MapN-Issue

Explanation: Press continue to go to the next wizard step or press cancel to change the module chain structure to meet the specifications.

System action: No action taken.

Administrator response: Enter a number for the appropriate fields.

FBTCON234E Error modifying the module chain

Explanation: Trust Service encountered a problem modifying the module chain.

System action: No action taken

Administrator response: Check the exception stack trace.

FBTCON235W This chain was automatically generated by TFIM. Modifying this chain could break the associated functionality. Review TFIM documentation for typical Trust Service chain structures and examples.

Explanation: Modify chains automatically generated by TFIM at your own risk.

System action: No action take

Administrator response: Review TFIM documentation for typical Trust Service chain structures and examples.

FBTCON236E Must select a keystore for your partner's encryption key.

Explanation: The liberty metadata that you imported for your partner contains encryption KeyInfo that must be saved in a keystore. Please choose the keystore where you would like to store it.

System action: No action taken

Administrator response: Select a keystore from the table.

FBTCON237E The web service URL is not properly formatted.

Explanation: The web service URL you entered is the wrong format.

System action: No action taken

Administrator response: Enter the URL in the proper format, [protocol]://[host]:[port]/[path].

FBTCON238E Must select a module instance.

Explanation: Select a module instance to continue or use the default XSL transformation map module.

System action: No action taken

Administrator response: Select a module instance from the table.

FBTCON239E You must enter the Single Sign-On Service URL.

Explanation: The Single Sign-On Service URL is required for the protocol.

System action: No action taken

Administrator response: Enter the Single Sign-On Service URL in the appropriate text entry field.

FBTCON240E You must enter the Name Identifier Management Service URL.

Explanation: The Name Identifier Management Service URL is required for the bindings you have selected.

System action: No action taken

Administrator response: Enter the Name Identifier Management Service URL in the appropriate text entry field.

FBTCON241E You must enter the Single Logout Service URL.

Explanation: The Single Logout Service URL is required for the bindings you have selected.

System action: No action taken

Administrator response: Enter the Single Logout Service URL in the appropriate text entry field.

FBTCON242E You must specify the mapping rule file to import.

Explanation: No mapping rule file was specified to import. Enter the file location in the file chooser.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON244E Must select an encryption key. Select a key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select an encryption key.

FBTCON245E Must enter a value for Number of seconds before the issue date that an assertion is considered valid

Explanation: Missing value from a required field.

System action: No action taken.

Administrator response: Enter a value for Number of seconds before the issue date that an assertion is considered valid in the appropriate text entry field

FBTCON246E Must enter a value for Amount of time the assertion is valid after being issued

Explanation: Missing value from a required field.

System action: No action taken.

Administrator response: Enter a value for Amount of time the assertion is valid after being issued in the appropriate text entry field

FBTCON247E Must enter an integer value for *insert*

Explanation: The value entered is not an integer.

System action: No action taken.

Administrator response: Enter an integer value.

FBTCON248E The web service URL is using https. You must select a signing key for SSL Settings.

Explanation: When using https you must select a signing key for SSL.

System action: No action taken.

Administrator response: Select a signing key in the table.

FBTCON249E You must select a signing key for client certification authentication.

Explanation: A signing key is required when using client certificate authentication.

System action: No action taken.

Administrator response: Select a signing key in the table.

FBTCON250E A number greater than 0 is required for ***insert*****.**

Explanation: A number must be entered greater than 0

System action: No action taken.

Administrator response: Enter a number greater than 0

FBTCON251E The web service URL is using http. Certificate authentication is not valid. Select basic authentication or none for the authentication type.

Explanation: Certificate authentication is not valid for http.

System action: No action taken.

Administrator response: Use basic authentication or none.

FBTCON252E The web service URL is using http. SSL Settings are not supported. Unselect the signing key for SSL.

Explanation: SSL is not valid for http.

System action: No action taken.

Administrator response: None

FBTCON253E The Common Domain Cookie Service URL must be a valid URL that begins with http:// or https://.

Explanation: The Common Domain Cookie Service URL must be a valid URL that begins with http:// or https://.

System action: No action taken.

Administrator response: Modify the Common Domain Cookie Service URL so that it is a valid URL that begins with http:// or https://.

FBTCON254E Metadata for Identity Provider partner must contain an IDPSSODescriptor element

Explanation: The specified metadata file could not be used to create an Identity Provider partner.

System action: No action taken.

Administrator response: Check that you are importing the correct metadata file and that it conforms to the SAML 2.0 metadata schema.

FBTCON255E Metadata for Service Provider partner must contain an SPSSODescriptor element

Explanation: The specified metadata file could not be used to create an Service Provider partner.

System action: No action taken.

Administrator response: Check that you are importing the correct metadata file and that it conforms to the SAML 2.0 metadata schema.

FBTCON256E Partner metadata protocolSupportEnumeration attribute does not specify SAML *insert* protocol

Explanation: The specified metadata file is not compatible with the SAML protocol for this federation.

System action: No action taken.

Administrator response: Check that you are importing the correct metadata file and that the protocolSupportEnumeration attribute value is correct.

FBTCON257E An error occurred communicating with the Management Service. Check the server log files for more information.

Explanation: An error occurred while the console was communicating with the domain. Check the server log files for the specific exception.

System action: No action taken.

Administrator response: Check the server log files for the specific exception. Check that the server is running.

FBTCON258E The portlet page could not be displayed. Check the server log files for more information.

Explanation: An error occurred while creating the portlet page. Check the server log files for the specific exception.

System action: No action taken.

Administrator response: Check the server log files for the specific exception.

FBTCON259E Failed to upload the keytab file. The keytab file format is invalid.

Explanation: An error occurred uploading the keytab file. The keytab file is generated with the ktpass command, which is part of the Windows Support Tools shipped on the Windows 2003 Server CD.

System action: No action taken.

Administrator response: Generate a valid keytab file using the ktpass command and import the file. See the Tivoli Federated Identity Manager documentation for more details.

FBTCON260E You must specify the keytab file to import.

Explanation: No keytab file was specified to import. Enter the file location in the file chooser.

System action: No action taken.

Administrator response: None.

FBTCON261E There are no federations created. You must create a federation before creating a partner.

Explanation: You cannot create a partner without selecting an existing federation

System action: No action taken.

Administrator response: Select the federation to which you want to add a partner from the table. If no federations exist, you must create one before creating a partner.

FBTCON262E No clusters or servers are available for use with Federated Identity Manager.

Explanation: You must create a cluster or server before trying to create a Federated Identity Manager Domain.

System action: No action taken.

Administrator response: Bring up the WebSphere Administrator Console and create cluster or server.

FBTCON263E An error occurred when connecting to domain *insert*.

Explanation: An exception was encountered when connecting to the specified domain.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON264E The Tivoli Federated Identity Manager Business Gateway domain *insert* was not found.

Explanation: You can only connect to an existing Tivoli Federated Identity Manager Business Gateway domain.

System action: No action taken.

Administrator response: Change the host and/or port to point to an existing Tivoli Federated Identity Manager Business Gateway Management Service.

FBTCON265E No management domains are defined. Click Domain Properties to connect to an existing domain or click Domains to create a new domain.

Explanation: There are no management domains defined. In order to manage a domain, a domain must be defined and activated. Use the Domain Properties panel to connect to an existing domain, or create a new domain.

System action: No action taken

Administrator response: Click Domain Properties to connect to an existing domain.

FBTCON266E Tivoli Federated Identity Manager was not found on the target WebSphere. The FIM Management Service could be down or may not be installed.

Explanation: You need to install the FIM Management Service on the target WebSphere

System action: No action taken

Administrator response: Install the FIM Management Service

FBTCON267E The domain name *insert* already exists. Specify another domain name.

Explanation: The console will not allow you to create a domain with the same name as an existing domain the console is currently managing. You need to specify a different name for the domain.

System action: No action taken

Administrator response: Specify a different domain name.

FBTCON268E The contact information cannot contain a comma.

Explanation: The console will not allow you to enter contact information with a comma. Change the contact information to not use any commas.

System action: No action taken

Administrator response: Change the contact information.

FBTCON269E The keystore does not contain any private keys. Try another keystore or use the Key Service to import a private key.

Explanation: The console is looking in the keystore for a private key to sign or encrypt with and the keystore selected does not contain one. Use the Key Service to add a private key to the keystore or try another keystore.

System action: No action taken

Administrator response: Select another keystore.

FBTCON270E The keystore does not contain any public keys. Try another keystore or use the Key Service to import a public key.

Explanation: The console is looking in the keystore for a public key to validate with and the keystore selected does not contain one. Use the Key Service to add a public key to the keystore or try another keystore.

System action: No action taken

Administrator response: Select another keystore.

FBTCON273E An error occurred publishing to the domain.

Explanation: An error occurred publishing files to the domain.

System action: No action

Administrator response: Check the exception stack trace in the logs.

FBTCON274E An error occurred applying the alias service configuration

Explanation: An error occurred applying the alias service configuration. The configuration type is stored in the idservice.xml for the domain.

System action: No action

Administrator response: Check the exception stack trace in the logs.

FBTCON275E The *insert* is required. Select from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a key.

FBTCON276E The point of contact profiles could not be retrieved from the single sign-on protocol service.

Explanation: This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON277E An error occurred while deleting a point of contact profile: *insert*.

Explanation: This error will occur if the point of contact profile is readonly or the current active profile. It can also occur if the profile does not exist.

System action: No action taken.

Administrator response: Check that this profile is not the current active profile and not readonly.

FBTCON278E An error occurred activating the point of contact profile: *insert*.

Explanation: Check to make sure the profile exists and is configured correctly. This error can also occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check to make sure the profile contains at least a Sign In and Local ID callback. Check the status of management service.

FBTCON279E An error occurred retrieving the properties for the point of contact profile: *insert*.

Explanation: Check to make sure the profile exists. Close the portlet page and try again. This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON280E An error occurred modifying the properties for the point of contact profile: *insert*.

Explanation: Check to make sure the profile exists. Close the portlet page and try again. This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running. See the exception stack trace.

FBTCON281E The list of available point of contact callbacks could not be retrieved from the single sign-on protocol service.

Explanation: Close the portlet page and try again. This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service.

Check that the single sign-on protocol service is running. See the exception stack trace.

FBTCON282E An error occurred while creating a point of contact profile.

Explanation: A single sign-on protocol service encountered a problem creating a point of contact profile.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON283E An error occurred retrieving the properties of the point of contact profile with ID: ***insert*****.**

Explanation: A single sign-on protocol service encountered a problem creating a point of contact profile.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON284E A decryption key must be selected. Select the Point-of-Contact SSL key from the table after using the List Keys button to display the keys contained in a keystore.

Explanation: You have not selected any key in the table. You must first choose a keystore and enter the keystore password to display the keys for this keystore in the table. Then, you must select a key from the table.

System action: No action taken

Administrator response: Please use the key selection layout to select a decryption key.

FBTCON285E You must select one of the choices presented on this dialog.

Explanation: You cannot configure this federation without selecting whether or not to add a standard partner.

System action: No action taken.

Administrator response: Select the radio button corresponding to your choice.

FBTCON286E You must enter the URL for the issuer of the Security token.

Explanation: The URL identifier of the Identity Provider is required for the Information Card protocol.

System action: No action taken.

Administrator response: Enter the Provider ID in the appropriate text entry field.

FBTCON287E You must enter an integer value for the clock skew.

Explanation: The value entered for clock skew is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for the clock skew.

FBTCON288E A new password for the keystore must be entered.

Explanation: In order to change the keystore password a new password needs to be entered.

System action: No action taken.

Administrator response: Enter a non empty new password.

FBTCON289E New password mismatch. Please confirm the new password.

Explanation: In order to change the keystore password a new password needs to be entered and properly confirmed.

System action: No action taken.

Administrator response: Make sure the new password and its confirmation matches.

FBTCON290E The new password is the same as the original.

Explanation: In order to change the keystore password a new password different than the original password must be entered .

System action: No action taken.

Administrator response: Make sure the new password is different than the original.

FBTCON291E An error occurred discovering the Tivoli Directory Integrator configuration settings.

Explanation: An error occurred discovering the TDI configuration settings. Check the host name and port and make sure host is allowed to access the TDI server.

System action: No action taken.

Administrator response: Enter the correct host name and port and if using SSL, ensure the SSL settings are configured correctly.

FBTCON292E You must enter a Server Hostname and Server Port to discover the Tivoli Directory Integrator configuration settings.

Explanation: Enter a host name and port and make sure host is allowed to access the TDI server.

System action: No action taken.

Administrator response: Enter the correct host name and port and if using SSL, ensure the SSL settings are configured correctly.

FBTCON293E An error occurred retrieving the hardware cryptographic device settings.

Explanation: This error can occur if the console is unable to communicate with the kess service.

System action: No action taken.

Administrator response: Check the system stack trace for more information.

FBTCON294E An error occurred applying the hardware cryptographic device settings.

Explanation: This error can occur if the console is unable to communicate with the kess service.

System action: No action taken.

Administrator response: Check the system stack trace for more information.

FBTCON295E The event *insert* requires a valid file name for the HTML page that is displayed.

Explanation: The specified field requires a valid file name.

System action: No action taken.

Administrator response: Enter the appropriate value for the specified field.

FBTCON296E The page locale cannot be empty. Specify the page locale and page root directory.

Explanation: The page locale and page root directory values are required to continue.

System action: No action taken.

Administrator response: Enter the required values in the table.

FBTCON297E The event pages cannot be displayed because the page factory configuration is missing the default page identifier mappings.

Explanation: The event pages are retrieved from the default page identifier mappings in the sps.xml file.

System action: No action taken.

Administrator response: Ensure that the sps.xml file is configured with the appropriate page identifier mappings. Refer to the Tivoli Federated Identity Manager Configuration Guide for information on configuring these settings.

FBTCON298E An error occurred while modifying the event pages configuration. Check the system stack trace for more information.

Explanation: The specified changes to the event pages configuration were not applied.

System action: No action taken.

Administrator response: Check the system stack trace for more information.

FBTCON300W Warning: the module chain is shared with other trust chain mappings. Modifications to the chain identification or chain structure affects other trust chain mappings that use this chain.

Explanation: The chain is shared. Modifications to the chain affect other trust chain mappings that use this chain.

System action: No action taken.

Administrator response: Ensure that the effects of the specified changes on all of the trust chain mappings are desired before you enact the changes.

FBTCON301W Warning: *keystore* keys or certificates in this keystore have expired or will expire in less than 30 days.

Explanation: The validity period of a key or certificate in the specified keystore will expire or has expired already.

System action: No action taken.

Administrator response: An expired key or certificate cannot be used, and will generate a message during the validation process.

FBTCON302E The self-signed certificate could not be created.

Explanation: An error occurred while attempting to create the self-signed certificate.

System action: No action taken.

Administrator response: Check the console and Management Service logs to determine the source of the error.

FBTCON303E The certificate signature request (CSR) could not be created.

Explanation: An error occurred on the management server side while attempting to create the CSR.

System action: No action taken.

Administrator response: Check the console and Management Service logs to determine the source of the error.

FBTCON304E A valid host name is required to establish an SSL connection.

Explanation: You must specify a host name to establish an SSL connection.

System action: No action taken.

Administrator response: Specify a host name.

FBTCON305E A valid port value is required to establish an SSL connection.

Explanation: You must specify a valid port value to establish an SSL connection.

System action: No action taken.

Administrator response: Specify a port value.

FBTCON306E An alias is required to store the certificate in the keystore.

Explanation: You must specify an alias to store the certificate in the keystore.

System action: No action taken.

Administrator response: Specify an alias.

FBTCON307E An error occurred while attempting to establish an SSL connection to retrieve the certificate. Ensure that the hostname and port are correct and that the target SSL server is active.

Explanation: A connection could not be established with the specified parameters. Either the specified values for the host and port are incorrect, or the target SSL server is not actively monitoring for incoming requests.

System action: No action taken.

Administrator response: Ensure that the hostname and port are correct and that an SSL server is monitoring for requests.

FBTCON308E A common name is required to create a certificate.

Explanation: You must specify a common name to create a certificate.

System action: No action taken.

Administrator response: Specify a common name.

FBTCON309E A validity period (in days) is required to create a certificate.

Explanation: You must specify a validity period to create a certificate.

System action: No action taken.

Administrator response: Specify a validity period.

FBTCON310E An organization is required to create a certificate.

Explanation: You must specify an organization to create a certificate.

System action: No action taken.

Administrator response: Specify an organization.

FBTCON311E A value is required for Logout Request Lifetime.

Explanation: You must enter a value for Logout Request Lifetime.

System action: No action taken.

Administrator response: Enter a value for Logout Request Lifetime.

FBTCON312E The specified value for Logout Request Timeout must be a positive integer.

Explanation: The value entered for Logout Request Timeout is not an integer.

System action: No action taken.

Administrator response: Enter an integer value for Logout Request Timeout.

FBTCON313E An error occurred while invoking the ITFIM Management Service. The Management Service may be unavailable.

Explanation: An mbean registered by the ITFIM Management Service could not be contacted through the WebSphere AdminClient. This is likely due to the ITFIM Managent Service not running on specified application server.

System action: No action taken.

Administrator response: Make sure the ITFIMManagementService EAR is installed and running on the WebSphere Application Server. In a cluster deployment, the ITFIMManagementService is only installed on the deployment manager.

FBTCON314E While contacting the ITFIM Management Service, a WebSphere AdminClient connector could not be created to the Management Service's application server with the given host and port.

Explanation: An AdminClient connector can not be created to the server if the remote server is down. This may also occur if host or port are erroneous.

System action: No action taken.

Administrator response: Make sure the host is running an application server with ITFIM installed. Make sure the port is set to the SOAP port configured for the application server, and that the port is listening.

FBTCON315E While contacting the ITFIM Management Service, the WebSphere AdminClient connector was unable to authenticate to the Management Service's application server. Make sure the WebSphere administrator credentials are correct.

Explanation: An AdminClient connector failed to authenticate to the application server due to incorrect WebSphere administrator credentials. This may occur if invalid administrator username and password are specified.

System action: No action taken.

Administrator response: Make sure a valid administrative username and password are specified that can authenticate with the application server.

FBTCON316E An invalid connector type is specified for connecting to the ITFIM Management Service.

Explanation: An invalid connector type is specified when trying to create an WebSphere AdminClient to the ITFIM Management Service. The connector type of SOAP should always be used to contact the ITFIM Management Service.

System action: No action taken.

Administrator response: When configuring the AdminClient connector, set the connector type to AdminClient.CONNECTOR_TYPE_SOAP.

FBTCON318E The passwords you entered do not match. Please enter the passwords again.

Explanation: The password re-entered does not match the originally entered password. This password will not be set unless its entered twice for validation.

System action: No action taken.

Administrator response: Enter the passwords again.

FBTCON319E An error occurred while retrieving the attribute filter for the partner with ID *insert*.

Explanation: An attempt was made to retrieve the attributes for the attribute filter.

System action: No action taken.

Administrator response: Check the console and Management Service logs to determine the source of the error.

FBTCON320E You must select an SSL Endpoint Key Identifier.

Explanation: The key is required

System action: No action taken.

Administrator response: Select a key

FBTCON321E You must use the https protocol with *insert*.

Explanation: The HTTPS protocol is required.

System action: No action taken.

Administrator response: Enter your base URL in the appropriate text entry field.

FBTCON322E You cannot create a Information Card Relying Party partner for the federation *insert*. A global partner was added when you created the federation.

Explanation: The Information Card Identity Provider federation has the concept of a global partner and additional partners are not allowed.

System action: No action taken

Administrator response: Select the federation to which you want to add a partner from the table. If no federations exist, you must create one before creating a partner.

FBTCON323E The entered cache size value is invalid. It must be a postive integer ranging from 0 to 32767.

Explanation: An invalid value was entered for the cache size. It must be a postive integer ranging from 0 to 32767.

System action: No action taken

Administrator response: Enter another value for the cache size.

FBTCON325E Errors occurred while saving the web plug-in configuration changes to the management service. Check the console and Management Service logs to determine the source of the error.

Explanation: Errors occurred while saving the web plug-in configuration changes to the management service. Check the console and Management Service logs to determine the source of the error.

System action: No action taken

Administrator response: Check the console and Management Service logs to determine the source of the error.

FBTCON326W Recent configuration changes require that WebSphere be restarted. All configuration changes will not take effect until the restart completes.

Explanation: In order for the configuration changes made to take effect, you must restart WebSphere.

System action: No action taken

Administrator response: Please select whether to restart WebSphere now, or dismiss this message. If you dismiss this message, you will not be reminded again. If you have deployed FIM in a cluster, your cluster will be ripple started; single servers will be restarted individually. See the Runtime Node Management page for node status.

FBTCON327E The Identity URL Pattern must contain the string @ID@.

Explanation: The Identity URL Pattern is a regular expression and must contain the string @ID@. For example, https://webseald.example.com/@ID@

System action: No action taken

Administrator response: Enter a url with the string @ID@.

FBTCON328E The value entered for *insert* contains an improperly formatted URL.

Explanation: Enter a valid URL format.

System action: No action taken

Administrator response: None

FBTCON329E The format of the received certificate seems to be invalid for this operation. Either use a DER encoded certificate or a Base64 encoded one.

Explanation: This operation required that the certificate is encoded either using binary DER or ascii Base64. The Certificate Authority should be able to provide this format or import the certificate into WebSphere (using the security menus) and export it in the appropriate format.

System action: No action taken

Administrator response: None

FBTCON330E The CA signed certificate was not imported to the Keystore. The problem seems to be that there is no matching certificate that holds the same public key. The CA certificate would replace the temporary certificate that was created when the Certificate Signature Request was created. Please verify that the certificate is correct and that you are using the appropriate keystore.

Explanation: The public key in the certificate received from the CA and the temporary one needs to match. Check that you are using the correct certificate and the correct keystore by trying to look at the subject of the CA certificate and the subjects in the keystore

System action: No action taken

Administrator response: None

FBTCON331E The value entered for *insert* cannot contain a comma. Each value should be input on a separate line.

Explanation: The text area used for input does not allow comma separated values. Enter each value on a separate line.

System action: No action taken

Administrator response: Enter values on separate lines.

FBTCON332E You cannot create an OpenID partner for the federation *insert*. A global partner was added when you created the federation.

Explanation: OpenID federations have the concept of a global partner and additional partners are not allowed.

System action: No action taken

Administrator response: Select the federation to which you want to add a partner from the table. If no federations exist, you must create one before creating a partner.

FBTCON333E The field *insert* requires a protocol to be selected.

Explanation: The check boxes represent the set of allowed protocols for those OpenID servers that the user agent will permit connection to.

System action: No action taken

Administrator response: Select at least one of the checkboxes. It is recommended to only allow https.

FBTCON334E In order to modify the Tivoli Access Manager properties for this domain, all the nodes need to be unconfigured. Unconfigure the domain by using the Runtime Node Management panel.

Explanation: The Tivoli Access Manager properties cannot be modified when the domain is configured. After unconfiguring the domain, modify the properties and then reconfigure.

System action: No action taken

Administrator response: Unconfigure the domain, modify the Tivoli Access Manager properties and then reconfigure.

FBTCON335E You must select an Information Card Signing Key Identifier

Explanation: The key is required

System action: No action taken.

Administrator response: Select a key

FBTCON336E An error occurred retrieving the properties for the WSSM partner with ID: *insert*.

Explanation: Close the portlet page and try again. This error can occur if the console is unable to communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running.

FBTCON337E The entered keystore name contains the invalid character *insert*. Please correct the name and try again.

Explanation: Certain characters cannot be used for keystore names.

System action: No action taken

Administrator response: Enter a valid name for the keystore in the appropriate text entry field.

FBTCON339E A point of contact profile with name *insert* already exists.

Explanation: An existing point of contact profile uses the display name that you entered. Each point of contact profile must have a unique display name.

System action: No action taken.

Administrator response: Please enter a different display name for this point of contact profile.

FBTCON340E The given keystore or key could not be read. Please verify that the file exists in the filesytem, that it is not corrupted, that the correct password was supplied or that your Java Cryptography Extension setup is appropriate for the type of keystore/key you are trying to use. Detailed information about this failure can be found in the log file.

Explanation: A keystore or key could not be read. This is a problem seen when the password to the keystore is incorrect, the file is corrupted or when the Java Cryptography Extension is not properly setup for the use of strong keys.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON341E Error displaying report parameters. Check system logs for more details.

Explanation: A problem occurred while attempting to display report parameters to display in console. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON342E Error building layout for report parameters. Check system logs for more details.

Explanation: A problem occurred while attempting to build report parameters layout. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON343E Error executing report. Check system logs for more details.

Explanation: A problem occurred while attempting to execute report. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON344E Error determining report render type. Check system logs for more details.

Explanation: A problem occurred while attempting to determine report render type. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON345E Error building layout for reports. Check system logs for more details.

Explanation: A problem occurred while attempting to build reports layout. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON347E Error downloading report. Check system logs for more details.

Explanation: A problem occurred while attempting to download report. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON348E Error deleting report. Check system logs for more details.

Explanation: A problem occurred while attempting to delete report. Check system logs for more details.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON350E An error occurred importing file *insert*. The file is not a valid LTPA key file.

Explanation: Either the file is not a valid LTPA key file or an unexpected error occurred.

System action: No action taken

Administrator response: Check the exception stack trace and/or the logs.

FBTCON351E An authorization server host-port pair is repeated. Please ensure that different authorization servers are supplied.

Explanation: The same host and port has been given for an authorization server.

System action: No action taken

Administrator response: Check the pairs of host-ports given

FBTCON352W A request to deploy the Tivoli Federated Identity Manager Runtime is in progress. New deployment requests will be ignored until the previous request is complete.

Explanation: A request to deploy the Tivoli Federated Identity Manager runtime as an application into the WebSphere Application Server environment has been started. Another request to deploy the Tivoli Federated Identity Manager runtime cannot be started until the previous one is complete.

System action: The Deploy Runtime button is not active.

Administrator response: If you want to deploy the Tivoli Federated Identity Manager runtime again, wait for the current deployment to complete. This may take up to 10 minutes. If you want to check if a deployment is complete, click the Deploying Tivoli Federated Identity Manager Runtime text or refresh the page of the console. Click the Deploy Runtime button when it is activated.

FBTCON353E An error occurred while reloading the configurations. Check the server log for error details.

Explanation: An error occurred while reloading the configurations.

System action: None of the configuration updates were completed.

Administrator response: Check the server log for more information about the error, make the updates to the configuration, and try reloading the configuration again.

FBTCON356W Some of the keys within the supplied keystore could not be read. Make sure that the keystore file has keys and that those keys are not protected by a different password than the keystore itself.

Explanation: Some of the keys in the supplied keystore could not be read. This happens when the keys have a different password than the keystore itself or when the file itself is damaged.

System action: No action taken

Administrator response: No action taken

FBTCON358E You must specify the Subject DN expression for the allowable X.509 certificates.

Explanation: You have not specified the Subject DN.

System action: No action taken

Administrator response: Please use the entry field to specify the required DN expression.

FBTCON359E The artifact resolution service index entry *insert* must be 0 or a positive integer.

Explanation: The text field for the artifact resolution service index must be 0 or a positive number.

System action: No action taken.

Administrator response: Enter 0 or a positive integer for the artifact resolution service index field.

FBTCON360E The artifact resolution service indexes must be unique.

Explanation: The artifact resolution service indexes must be unique.

System action: No action taken.

Administrator response: Enter 0 or a positive integer for the artifact resolution service index field.

FBTCON361E Only one artifact resolution service endpoint is allowed to be the default endpoint.

Explanation: You have specified more than one default artifact resolution service endpoint.

System action: No action taken

Administrator response: Select only one artifact resolution service endpoint to be the default endpoint.

FBTCON362E The OP Generated Claimed Identifier Pattern must contain the string @ID@.

Explanation: The OP Generated Claimed Identifier Pattern must contain the string @ID@. For example, https://webseald.example.com/@ID@

System action: No action taken

Administrator response: Enter a URL with the string @ID@.

FBTCON363E The maximum authentication age must be 0, a positive integer, or -1 to disable.

Explanation: The maximum authentication age must be in the correct range. An age of 0 forces authentication.

System action: No action taken

Administrator response: Enter -1, 0, or a positive integer.

FBTCON364E An unknown error was encountered when processing the specified mapping rule.

Explanation: The mapping rule validator cannot determine the exact error when processing the specified mapping rule.

System action: No action taken

Administrator response: Check the log file to see if there is an exception that indicates the error encountered.

FBTCON365E An XSL syntax error was encountered when processing the specified mapping rule. The specific error in the log file is [[*loggederror*]].

Explanation: The mapping rule validator encountered an XSLT syntax error when it attempted to process the XSLT file.

System action: No action taken

Administrator response: Check the log file to see if there is an exception that indicates the error.

FBTCON366E A JavaScript syntax error was encountered when processing the specified mapping rule. The specific error in the log file is [[*loggederror*]].

Explanation: The mapping rule validator encountered a JavaScript syntax error when it attempted to process the JavaScript file.

System action: No action taken.

Administrator response: Check the log file to see if there is an exception logged that might indicate the error encountered.

FBTCON367E The mapping rule type cannot be determined. Ensure that the mapping rule file has a known file extension and that there are no syntax errors in the given rule.

Explanation: The mapping rule validator cannot determine the mapping rule type.

System action: No action taken

Administrator response: Check the log file to see if there is an exception that indicates the error.

FBTCON368E The audit client profiles could not be retrieved from the management service.

Explanation: This error can occur if the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON369E An error occurred while deleting an audit client profile: *insert***.**

Explanation: This error occurs if the audit client profile is the current active profile. It can also occur if the profile does not exist.

System action: No action taken.

Administrator response: Check that this profile is not the current active profile.

FBTCON370E An error occurred activating the audit client profile: *insert***.**

Explanation: Ensure that the profile exists and is configured correctly. This error can also occur if the console cannot communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the status of management service.

FBTCON371E The audit events list could not be retrieved from the management service.

Explanation: This error can occur if the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON372E The audit events list could not be updated.

Explanation: This error can occur if the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON373E An error occurred while creating an audit client profile.

Explanation: A single sign-on protocol service encountered a problem creating an audit client profile.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON374E An error occurred retrieving the properties of the audit client profile with ID: *insert***.**

Explanation: A single sign-on protocol service encountered a problem creating an audit client profile.

System action: No action taken.

Administrator response: See the exception stack trace.

FBTCON375E An audit client profile with name *insert* **exists.**

Explanation: An existing audit client profile uses the display name that you entered. Each audit client profile must have a unique display name.

System action: No action taken.

Administrator response: Enter a different display name for this audit client profile.

FBTCON376E The list of available audit event handlers could not be retrieved from the single sign-on protocol service.

Explanation: Close the portlet page and try again. This error can occur if the console cannot communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running. See the exception stack trace.

FBTCON377E The field names for the audit event handler could not be retrieved from the management service.

Explanation: This error can occur if the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON378E An error occurred modifying the properties for the audit client profile: ***insert*****.**

Explanation: This error can occur if the console cannot communicate with the single sign-on protocol service.

System action: No action taken.

Administrator response: Ensure that the profile exists. Close the portlet page and try again. Check the service configurations to ensure that you have the correct host name and port for the single sign-on protocol service. Check that the single sign-on protocol service is running. See the exception stack trace.

FBTCON379E The key alias ***alias*** **is already used by another key in this keystore.**

Explanation: Keys must have unique aliases in the keystore.

System action: No action taken.

Administrator response: Please enter a unique keystore alias.

FBTCON380E The field ***insert*** **contains an invalid regular expression.**

Explanation: You have entered an invalid regular expression. Modify the regular expression so that it is valid.

System action: No action taken.

Administrator response: Please enter a valid regular expression in the appropriate text entry field.

FBTCON381E The artifact resolution service index entry ***insert*** **is too large for an integer. The maximum value is** ***insert*****.**

Explanation: The text field for the artifact resolution service index must be 0 and the maximum value.

System action: No action taken.

Administrator response: Enter a number between 0 and the maximum for the artifact resolution service index field.

FBTCON382E The event handler properties could not be retrieved from the management service.

Explanation: This error can occur if the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON383E The federation display name can contain only characters from the set set 'a-z', 'A-Z' and '0-9'. Specify a different name using only the valid characters.

Explanation: The federation display name that you entered contains an invalid character.

System action: No action taken

Administrator response: Please enter a different display name for this federation.

FBTCON384E No suitable signature algorithms are found for the ***insert*** **signing key type.**

Explanation: There is no suitable signature algorithm found for the selected federation signing key type.

System action: No action taken.

Administrator response: Select a different signing key for the federation.

FBTCON385E Temporary credentials and verification code lifetime is not valid.

Explanation: The temporary credentials and verification code lifetime must be a positive integer value.

System action: No action taken.

Administrator response: Enter the valid temporary credentials and verification code lifetime.

FBTCON386E The maximum OAuth token credentials lifetime is not valid.

Explanation: The maximum OAuth token credentials lifetime must be a positive integer value.

System action: No action taken.

Administrator response: Enter the valid maximum OAuth token credentials lifetime.

FBTCON387E The skew time between OAuth server and client is not valid.

Explanation: The skew time between OAuth server and client must be a positive integer value.

System action: No action taken.

Administrator response: Enter the valid skew time between OAuth server and client.

FBTCON388E Error occurred when verifying the client identifier.

Explanation: An exception was encountered when checking the uniqueness of the client identifier you entered.

System action: No action taken.

Administrator response: Check the exception stack trace.

FBTCON389E The minimum length of client identifier is <*number*> characters.

Explanation: An exception was encountered when checking the length of the client identifier you entered.

System action: No action taken.

Administrator response: Ensure the client identifier meets the minimum length requirement.

FBTCON390E The client identifier can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Specify a different client identifier using the valid characters.

Explanation: The client identifier that you entered contains a character that is not valid.

System action: No action taken.

Administrator response: Please enter the valid client identifier.

FBTCON391E The minimum length of client shared-secret is <*number*> characters.

Explanation: An exception was encountered when checking the length of the client shared-secret you entered.

System action: No action taken.

Administrator response: Ensure the client shared-secret meets the minimum length requirement.

FBTCON393E The client callback URI is not valid. Enter 'oob' if it is not applicable.

Explanation: The client callback URI that you entered is not valid.

System action: No action taken.

Administrator response: Enter the valid client callback URI.

FBTCON394E An OAuth partner cannot be created for the federation *insert*.

Explanation: An external client provider was selected for the federation. IBM Tivoli Federated Identity Manager internal partners are not allowed when an external client provider is selected.

System action: No action taken.

Administrator response: Add clients externally based on your implementation, or change the OAuth client provider configuration to add partners to IBM Tivoli Federated Identity Manager.

FBTCON395E An error occurred when verifying the client identifier. A client with the specified client identifier already exists.

Explanation: An exception was encountered when checking the uniqueness of the client identifier you entered.

System action: No action taken.

Administrator response: Ensure the client identifier specified is unique for this federation.

FBTCON396E The minimum length of client identifier is <*number*> characters.

Explanation: An exception was encountered when checking the length of the client identifier you entered.

System action: No action taken.

Administrator response: Ensure the client identifier meets the minimum length requirement.

FBTCON397E The client identifier can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Specify a different client identifier using the valid characters.

Explanation: The client identifier that you entered contains a character that is not valid.

System action: No action taken.

Administrator response: Enter the valid client identifier.

FBTCON398E The minimum length of client shared-secret is <*number*> characters.

Explanation: An exception was encountered when checking the length of the client shared-secret you entered.

System action: No action taken.

Administrator response: Ensure the client shared-secret meets the minimum length requirement.

FBTCON400E The client redirection URI is not valid.

Explanation: The syntax of the client redirection URI that you entered is not valid.

System action: No action taken.

Administrator response: Enter a valid client redirection URI.

FBTCON401E The client provider is not valid.

Explanation: You have not selected a client provider option.

System action: No action taken.

Administrator response: Select the option that corresponds to your client provider for the federation.

FBTCON402E The external client provider implementation is not specified.

Explanation: You have not published the external client provider plugin, selected an external client provider implementation or did not specify the external client provider implementation module ID.

System action: No action taken.

Administrator response: Publish the external client provider plugin, select an external client provider implementation for the federation or specify the external client provider implementation module ID in your plugin.

FBTCON403E The configuration settings for the *module id* could not be retrieved from the management service.

Explanation: One possible reason for this error is that the console cannot communicate with the management service.

System action: No action taken.

Administrator response: Check the service configurations to ensure that you have the correct host name and port for the management service. Check that the management service is running.

FBTCON404W The external client provider implementation for *module id* cannot be loaded.

Explanation: Make sure the external client provider plugin is published.

System action: No action taken.

Administrator response: Publish the external client provider plugin.

FBTCON405E You must select at least one authorization grant type (Authorization Code, Implicit Grant, Client Credentials, or Resource Owner Password Credentials).

Explanation: See message.

System action: No action taken.

Administrator response: Ensure that you select the authorization grant you want to support in your federation.

FBTCON406E The authorization code lifetime is not valid.

Explanation: The authorization code lifetime must be a positive integer value.

System action: No action taken.

Administrator response: Enter a valid authorization code lifetime.

FBTCON407E The maximum authorization grant lifetime is not valid.

Explanation: The maximum authorization grant lifetime must be a positive integer value and greater than the authorization code and access token lifetime.

System action: No action taken.

Administrator response: Enter a valid maximum authorization grant lifetime.

FBTCON408E The access token lifetime is not valid.

Explanation: The access token lifetime must be a positive integer value.

System action: No action taken.

Administrator response: Enter a valid access token lifetime.

FBTCON413W There are no available access token types.

Explanation: The extension manager could not load any of the access token type modules.

System action: No action taken.

Administrator response: Verify that the access token type module is included in the published plug-ins.

FBTCON414W The access token type implementation for *module id* cannot be loaded.

Explanation: The extension manager could not load the specified access token type module.

System action: No action taken.

Administrator response: Verify that the extension for the specified module ID is included in the published plug-ins.

FBTCON415E You must select an access token type.

Explanation: The OAuth client requires an access token type to make protected resource requests.

System action: No action taken.

Administrator response: Ensure that you select an access token type for this federation.

FBTCON415W There are no available token cache implementations.

Explanation: The extension manager could not load any of the token cache modules.

System action: No action taken.

Administrator response: Verify that the token cache module is included in the published plug-ins.

FBTCON416E You must select a token cache implementation.

Explanation: You must specify the method used to cache OAuth tokens.

System action: No action taken.

Administrator response: Ensure that you select a token cache implementation for this federation.

FBTCON416W The token cache implementation for *module id* cannot be loaded.

Explanation: The extension manager could not load the specified token cache module.

System action: No action taken.

Administrator response: Verify that the extension for the specified module ID is included in the published plug-ins.

FBTCON417E The specified URL *value* is not a valid URL.

Explanation: The syntax of the URL that you have entered is not correct.

System action: No action taken.

Administrator response: Verify that the URL is correct and try again.

FBTCON418E A HTTPS URL is expected. The specified URL *value* is not a HTTPS URL.

Explanation: The URL that you have entered is not a HTTPS URL.

System action: No action taken.

Administrator response: Verify that the URL begins with https://.

FBTCON419E The specified URI *value* is not a valid URI.

Explanation: The syntax of the URI that you have entered is not correct.

System action: No action taken.

Administrator response: Verify that the URI is correct and try again.

FBTCON420W There are no available trusted clients manager implementations.

Explanation: The extension manager could not load any of the trusted clients manager modules.

System action: No action taken.

Administrator response: Verify that the trusted clients manager module is included in the published plug-ins.

FBTCON421W The trusted clients manager implementation for *module id* cannot be loaded.

Explanation: The extension manager could not load the specified trusted clients manager module.

System action: No action taken.

Administrator response: Verify that the extension for the specified module ID is included in the published plug-ins.

FBTCON422E You must select a trusted clients manager implementation.

Explanation: You must specify the method used to manage trusted client information.

System action: No action taken.

Administrator response: Ensure that you select a trusted clients manager for this federation.

FBTCON424E The token cache implementation module ID is not specified.

Explanation: The token cache implementation module ID is required.

System action: No action taken.

Administrator response: Specify the token cache implementation module ID in your plugin.

FBTCON425E The trusted clients manager implementation module ID is not specified.

Explanation: The trusted clients manager implementation module ID is required.

System action: No action taken.

Administrator response: Specify the trusted clients manager implementation module ID in your plugin.

FBTCON426E An OAuth 1.0 partner cannot be created for the federation *insert*.

Explanation: An external client provider was selected for the federation. IBM Tivoli Federated Identity Manager internal partners are not allowed when an external client provider is selected.

System action: No action taken.

Administrator response: Add clients externally based on your implementation, or change the OAuth client provider configuration to add partners to IBM Tivoli Federated Identity Manager.

FBTCON427E The value entered for *insert* is not in the accepted URL format. Specify the URL either in http://.../sps/... or https://.../sps/... format.

Explanation: Enter the URL either in http://.../sps/... or https://.../sps/... format

System action: No action taken

Administrator response: None

FBTFDB001E Creation of database connection failed. Check the database configuration and network connectivity to the database server.

Explanation: The database connection could not be created.

System action: Command execution is halted.

Administrator response: Ensure that the database is configured correctly. Also check that the network connectivity to the database server is available.

FBTFDB002E A database error occurred.

Explanation: An unrecoverable database error occurred.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB003E A file database error has ocurred.

Explanation: An unrecoverable file database error occurred.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB004E The database file does not exist.

Explanation: An unrecoverable database error occurred.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB005E Unable to reach Database.

Explanation: The database cannot be reached

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB006E Unable to get Data Access Object.

Explanation: An instance of the Data Access Object cannot be retrieved

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB007E Unable to retrieve transaction.

Explanation: A Transaction object cannot be retrieved from the Data Access Object

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB008E An invalid SQL statement was executed.

Explanation: The result from a SQL statement showed invalid execution.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB009E An invalid cleanup interval of *VALUE_0* was defined.

Explanation: The clean up interval is invalid, it must be a valid integer above 60000.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB010E The datasource *VALUE_0*, could not be retrieved.

Explanation: The JNDI lookup to get a datasource failed.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB011E An error occured during deserialization as part of a database operation.

Explanation: The deserialization failed for a stored data object.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFDB012E An invalid configuration parameter was specified for either the retry limit, retry delay or default TTL of the distributed map.

Explanation: One or more of the following parameters values is invalid; retryLimit, retryDelay, or defaultTTL.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTFIR001E You have entered an invalid WebSphere Application Server administrator user name or password.

Explanation: Error results from either entering a non-administrator user name, corresponding wrong password, an incorrect spelling of the administrator name or password.

System action: Command execution halted.

Administrator response: Enter the correct administrator user name and password.

FBTFIR002E Cannot connect to the WebSphere Application Server.

Explanation: An attempt to connect to the target WebSphere Application Server failed. It might be due to any of the following reasons: WebSphere Application Server is not in service, or it is not responding.

System action: Command execution halted.

Administrator response: Start or restart the WebSphere Application Server. If this error recurs, check the WebSphere Application Server log files to determine the source of the error.

FBTFIR003E The WebSphere Application Server installation directory is not valid.

Explanation: The fim.appservers.properties file in FIM install directory etc folder might not have the correct entry for WebSphere Application Server installation directory.

System action: Command execution halted.

Administrator response: Make sure the fim.appservers.properties has the correct value for was.install.location.

FBTFIR004E The federation name you specified already exists. Specify a different federation name.

Explanation: The federation name you have entered already exists in the system.

System action: Command execution halted.

Administrator response: Specify a different federation name.

FBTFIR005E The federation name can contain only characters from the set 'a-z', 'A-Z' and '0-9'. Change the federation name to match the criteria.

Explanation: The federation name does not comply with the prescribed set of characters to use.

System action: Command execution halted.

Administrator response: Make sure that the federation name you have specified complies with the prescribed set of characters that you can use.

FBTFIR006E Unable to complete the task due to a wsadmin SOAP connection timeout.

Explanation: The current process can take a long time to complete. The wsadmin SOAP connection might time out before the operation is finished.

System action: Command execution halted.

Administrator response: To avoid timeouts, modify the com.ibm.SOAP.request.Timeout property to 800. The property is in the WebSphere installation directory and the following subdirectory: /profiles/profile_name/properties/soap.client.props. Then, restart the WebSphere server. Note: The timeout might occur during runtime deployment. As a result, the process halts. You can run the same configurations again, and the tool proceeds in carrying out subsequent tasks.

FBTFIR007E You have multiple FIM domains. The tool does not support multiple Tivoli Federated Identity Management domains.

Explanation: The Federation First Steps tool currently does not support a cluster environment.

System action: Command execution halted.

Administrator response: Make sure you are not working on a cluster environment.

FBTFIR008E You have multiple WebSphere Application Server clusters. The tool does not support multiple clusters.

Explanation: The Federation First Steps tool currently does not support a multiple cluster environment.

System action: Command execution halted.

Administrator response: Make sure you are not working in a multiple cluster environment.

FBTFIR009E The Deployment Manager has no cluster members. The tool does not support a Deployment Manager without cluster members.

Explanation: The tool does not support a Deployment Manager without cluster members.

System action: Command execution halted.

Administrator response: Make sure you are not working with a Deployment Manager that has no cluster members.

FBTFIR010E The type of process connected is not handled.

Explanation: Only WebSphere Application Server process and Deployment Manager process are handled.

System action: Command execution halted.

Administrator response: Make sure you are connected to either a WebSphere Application Server process or Deployment Manager process.

FBTFIR011E A user name and password must be specified to login.

Explanation: A user name and password must be specified to login.

System action: Command execution halted.

Administrator response: Enter your credentials in the appropriate fields.

FBTFIR012E A problem occurred. Check the log for details.

Explanation: A problem occurred. Check the log for details.

System action: Command execution halted.

Administrator response: Check the Federation First Steps tool log file for details.

FBTFIR014E You must enter the appropriate value for each field.

Explanation: Fill out the fields with the appropriate value.

System action: Command execution halted.

Administrator response: Make sure that all the fields have been filled out with appropriate values.

FBTFIR015E There is an error in loading the Tivoli Federated Identity Manager command line interface. If you have just installed Tivoli Federated Identity Manager, ensure that you stop the WebSphere Application Server, and then restart it before attempting to run the Federation First Steps tool.

Explanation: The FIM command line interface might not be loaded properly.

System action: Command execution halted.

Administrator response: Ensure that the Tivoli Federated Identity Manager is installed, and the command line interface is properly initialized. See the Command reference section in the Administration Guide for details (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.1/concept/commandoverview.html).

FBTFIR016E There is an error running a native process.

Explanation: Some processes might have some problems running on certain native platforms.

System action: Command execution halted.

Administrator response: None.

FBTFIR017E You must enter a base URL for your protocol endpoints.

Explanation: A common base URL is required for all protocol endpoints.

System action: Command execution halted.

Administrator response: Enter your base URL in the appropriate text entry field.

FBTFIR018E Unable to execute tfimcfg.jar.

Explanation: The Federation First Steps tool requires the tfimcfg.jar file to be in its original location.

System action: Command execution halted.

Administrator response: Make sure that the tfimcfg.jar file is in the original location as when the Tivoli Federated Identity Manager was installed.

FBTFIR019E Unable to create a temporary working directory.

Explanation: The Federation First Steps tool requires a temporary working directory to be created.

System action: Command execution halted.

Administrator response: Make sure that the temporary directory of the system is not full, and the Federation First Steps tool has read and write permissions to it.

FBTFIR020E Unable to load the fim.appservers.properties file.

Explanation: The Federation First Steps tool requires the fim.appservers.properties file to be present and readable on this system.

System action: Command execution halted.

Administrator response: Make sure that Tivoli Federated Identity Manager has been installed correctly, and the Federation First Steps tool has the correct permissions read the installation directory.

FBTFIR021E Failed to retrieve the TCP/IP ports this server uses for connections.

Explanation: The Federation First Steps tool failed to retrieve the TCP/IP ports this server uses for connections.

System action: Command execution halted.

Administrator response: Make sure serverindex.xml is not corrupted and is readable. The file is in the WebSphere installation directory and the following subdirectory: /profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml.

FBTFIR022E Unable to connect to the Tivoli Federated Identity Manager InfoServiceXML endpoint at *EndpointURL*.

Explanation: Unable to connect to the Tivoli Federated Identity Manager InfoServiceXML endpoint.

System action: Command execution halted.

Administrator response: Make sure that the InfoServiceXML endpoint can be accessed.

FBTFIR023E The WebSEAL configuration file you specified is not valid.

Explanation: The WebSEAL configuration file you specified is not valid.

System action: Command execution halted.

Administrator response: Specify a valid path to WebSEAL configuration file.

FBTFIR045E You have a cluster environment. This template does not support a cluster environment.

Explanation: This template currently does not support a cluster environment.

System action: Command execution halted.

Administrator response: Make sure you are not working on a cluster environment.

FBTFIR050E Failed to configure WebSEAL as the Point of Contact server. Please see the log for details.

Explanation: Failed to configure WebSEAL as the Point of Contact server. Please see the log for details.

System action: Command execution halted.

Administrator response: Read the log for the cause of failure, and fix it accordingly.

FBTFIR057E The Assertion Consumer Service URL you specified is not a valid URL.

Explanation: The Assertion Consumer Service URL you specified is not a valid URL.

System action: Command execution halted.

Administrator response: Make sure the Assertion Consumer Service URL provided by the partner is a valid URL.

FBTFIR058E The ImmutableID lookup method specified is not valid.

Explanation: You did not specify a valid ImmutableID lookup method.

System action: Command execution halted.

Administrator response: Specify the correct ImmutableID lookup value: 0=TAM principal UUID, 1=FIM alias service.

FBTFIR059E The domain name is not valid.

Explanation: You did not specify a valid domain name.

System action: Command execution halted.

Administrator response: Specify the correct domain name that is associated with your account.

FBTFIR060E Specify a valid domain name.

Explanation: You did not specify a valid domain name.

System action: Command execution halted.

Administrator response: Specify a valid domain name.

FBTFIR061E Select a value from the drop-down.

Explanation: You did not select a value from the drop-down.

System action: Command execution halted.

Administrator response: Select a value from the drop-down.

FBTFIR062E Specify a valid federation name.

Explanation: You did not specify a valid federation name.

System action: Command execution halted.

Administrator response: Specify a valid federation name.

FBTFIR063E Failed to get the keys from the keystore.

Explanation: The keys were not retrieved from the keystore.

System action: Command execution halted.

Administrator response: Failed to get the keys from the keystore.

FBTFIR064E Failed to import the key into the keystore.

Explanation: The key was not imported into the keystore because you might have provided a wrong keystore password or wrong file path.

System action: Command execution halted.

Administrator response: Failed to import the key into the keystore.

FBTFIR065E One or more required fields are missing.

Explanation: You did not enter all the required input fields.

System action: Command execution halted.

Administrator response: One or more required fields are missing.

FBTFIR066E Could not connect to the Tivoli Access Manager environment.

Explanation: You cannot connect to the Tivoli Access Manager because of wrong user name password combination or the Tivoli Access Manager is not running on the specified port.

System action: Command execution halted.

Administrator response: Could not connect to the Tivoli Access Manager environment.

FBTFIR067E The mapping rule file is missing.

Explanation: You did not provide the mapping rule.

System action: Command execution halted.

Administrator response: The mapping rule file is missing.

FBTFIR073W It appears that Tivoli Federated Identity Manager has not been configured with WebSEAL as the Point of Contact. In order for risk based access to function correctly, you must configure Tivoli Federated Identity Manager with WebSEAL as Point of Contact.

Explanation: One or more pre-requisite set up may be missing, check the message and resolve the issue.

System action: None.

Administrator response: None.

FBTFIR074E *ConfigStep* **failed due to** *ConfigStepError*

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR080E Tivoli Access Manager Configuration Failed, Please check whether it is already running on this system, and padmin command can be executed on this system. Error details : *ErrorDetails*

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR081E Invalid junction name specified.

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR082E Invalid Tivoli Access Manager Resource URI specified.

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR083E Invalid Point of Contact Server URL Specified.

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR085E Risk-based Access Configuration could NOT be completed successfully.

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR086E Invalid WebSEAL instance name.

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFIR089E Failed Execution of : *command* **Exit code :** *exitCode* **Output :** *output* **Error :** *error*

Explanation: One or more internal failures may have caused configuration wizard to fail. Check the logs for more details.

System action: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

Administrator response: Check the logs for a more detailed explanation and fix inputs or environmental issues before trying again.

FBTFMS100E *argument* **is a required argument.**

Explanation: A required argument was missing.

System action: The request has been halted.

Administrator response: Examine the client code that made this call and ensure that it passes the right arguments.

FBTFMS101E *argument* **is not a legal argument. Input must be: DEBUG_MIN, DEBUG_MID, DEBUG_MAX, AUDIT_ID_AUTH, AUDIT_SECURITY, AUDIT_CREATE_MOD_DELETE, INFO, WARN, ERROR, or OFF**

Explanation: The given event level string was not a valid value.

System action: The request returned the empty string.

Administrator response: Examine the client code that made this call and ensure that it passes a legal value.

FBTFMS102E *argument* **is not a valid ID.**

Explanation: The given unique ID does not exist.

System action: An exception has been thrown.

Administrator response: Pass in a valid ID.

FBTFMS103E Expected a list of size *size1*, but received a list of size *size2*

Explanation: This method expected a list of a certain size and received a different size.

System action: An exception has been thrown.

Administrator response: Pass in a list with the right size.

FBTFMS104E Received an unexpected argument type: *msg*

Explanation: This method expected an argument of a certain type and received an argument with a different type.

System action: An error has been logged.

Administrator response: Pass in an argument with the correct type.

FBTFMS105E Received an unexpected value *msg1*. Expected one of the following: *msg2*

Explanation: This method expected a certain value from a given list of values but received something else.

System action: An error has been logged.

Administrator response: Pass in an expected value.

FBTFMS106E Encountered an error getting an instance of ModuleLoaderFactory: *msg1*.

Explanation: The module factory loader threw an exception.

System action: An error has been logged.

Administrator response: Check the trace log to determine the cause of the problem.

FBTFMS107E A configuration file or directory was not found: *msg1*.

Explanation: A required configuration file was not found.

System action: An error has been logged.

Administrator response: Ensure that the required file exists.

FBTFMS108E Could not delete the point of contact client given by ID: *id*.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration.

FBTFMS109E Could not delete the delegate protocol instance given by ID: *id*.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration.

FBTFMS110E Could not delete the protocol determination module given by ID: *id*.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration.

FBTFMS111E Could not delete the global handler given by ID: *id*.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration.

FBTFMS112E Could not delete the page selector given by ID: *id*.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration.

FBTFMS116E The management operation is missing required input values. The management operation has failed to complete.

Explanation: The management operation is missing required input values.

System action: The operation will return failure.

Administrator response: The management operation being called requires specific input values to complete the operation. Check the documentation for all the required input values.

FBTFMS117E The provided password is incorrect or the *keystore* keystore does not exist. The management operation has failed to complete.

Explanation: The provided password was not correct, or the keystore does not exist.

System action: The operation will return failure.

Administrator response: Ensure that the keystore exists and ensure the correct password was entered.

FBTFMS118E Error encountered when retrieving the encoded format of the certificate.

Explanation: An attempt was made to encode a certificate that returned errors.

System action: The operation will return failure.

Administrator response: Check the trace logs for a more specific exception error.

FBTFMS119E Error encountered while creating the keystore for export. Export operation failed.

Explanation: During the generation of the keystore to export the server encountered a error.

System action: The operation will return failure.

Administrator response: Check the logs for an exception that will give a more specific reason for the error.

FBTFMS120E Error encountered while importing the given keystore. Import operation failed.

Explanation: During the importing of the keystore the server encountered a error.

System action: The operation will return failure.

Administrator response: Check the logs for an exception that will give a more specific reason for the error.

FBTFMS121E The store *storename* **does not exist. Operation failed to complete.**

Explanation: The given store does not exist.

System action: The operation will return failure.

Administrator response: Ensure that the given store exists.

FBTFMS122E The import into store *storename* **failed. Operation failed to complete, check trace logs for more specific error.**

Explanation: An error was encountered when the key and/or certificate were being imported.

System action: The operation will return failure.

Administrator response: Check the trace logs for a more specific error message.

FBTFMS123E The password for the given keystore is incorrect. Operation failed to complete.

Explanation: An error was encountered validating the password for the given keystore.

System action: The operation will return failure.

Administrator response: Ensure that the correct password is entered for the keystore or for the key entry.

FBTFMS124E An error occurred when attempting to update the store (*storename***) with the new data. Operation failed to complete.**

Explanation: An error occurred while updating the specified store.

System action: The operation will return failure.

Administrator response: Check the trace logs for a more specific error message.

FBTFMS125E The key alias *alias name* **returned no data for the keystore provided. Confirm that the key alias given exists. Operation failed to complete.**

Explanation: There are no keys or certificates located at the key alias given.

System action: The operation will return failure.

Administrator response: Confirm that the given key alias exists in the provided keystore.

FBTFMS126E The key alias *alias name* **already exists in the store** *store name***. Operation failed to complete.**

Explanation: The import operation was asked to not overwrite existing key aliases and the alias provided already existed in the store.

System action: The operation will return failure.

Administrator response: Confirm that the given key alias does not exists in the provided store.

FBTFMS127E The encountered file '*file name***' could not be read.**

Explanation: An error occurred while attempting to read the specified file.

System action: The operation will return failure.

Administrator response: Confirm that the file has the correct permissions and is a valid JKS file.

FBTFMS128E The configured directory '*directory name***' could not be read or does not exist.**

Explanation: An error occurred while attempting to read the configured directory.

System action: The operation will return failure.

Administrator response: Confirm that the directory exists and has the correct permissions.

FBTFMS129E The specified label '*label*' could not be deleted from the specified keystore '*key store*'.

Explanation: An error occurred while attempting to modify the specified keystore.

System action: The operation will return failure.

Administrator response: Confirm that the input values to the management operation are correct.

FBTFMS135E Obtaining a new context requires the ITFIM_CONTEXT_DOMAIN parameter.

Explanation: The management service operation requires the domain name to be set using the ITFIM_CONTEXT_DOMAIN parameter.

System action: The processing has been halted.

Administrator response: Set the ITFIM_CONTEXT_DOMAIN parameter as input to the management operation.

FBTFMS136E The specified keystore name '*keystore name*' is already in use, and cannot be re-used again to create a new keystore.

Explanation: An error occurred while attempting to create a keystore.

System action: The operation will return failure.

Administrator response: Confirm that the inputs to the management operation are correct.

FBTFMS137E An error occurred creating keystore '*keystore name*'.

Explanation: An error occurred while attempting to create a keystore.

System action: The operation will return failure.

Administrator response: Confirm that the inputs to the management operation are correct and check trace logs for details.

FBTFMS138E STS module instance cannot be deleted because it is in use.

Explanation: An error occurred while attempting to delete an STS module instance.

System action: The operation will return failure.

Administrator response: Confirm the STS module instance is not in use before attempting to delete it.

FBTFMS139E An error occurred while reading the license file *path*. The default license will be used instead. The root cause of the error was '*exception text*'.

Explanation: Federated Identity Manager attempted to verify the license file, but the verification failed.

System action: The system will use the default license.

Administrator response: Verify that the license file exists and has not been modified from the version included with your product installation media. If necessary, copy the original license file from the Federated Identity Manager installation media into place.

FBTFMS140E Could not delete the point of contact profile given by ID: *id*. Ensure that the profile exists, is not read-only, and is not the currently active profile.

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration, is not read-only, and is not the current profile.

FBTFMS141E Could not modify the point of contact profile given by ID: *id*. Make sure the profile exists and is not read-only.

Explanation: The modify operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration and it is not read-only.

FBTFMS142E The plug-in directory was null.

Explanation: The plug-in directory could not be determined by the Management Service.

System action: An error has been logged.

Administrator response: Ensure that the moduledirs.properties file exists inside the ITFIMManagementService.ear application.

FBTFMS143E Could not make the point of contact profile given by ID: *id* the current profile. The profile must contain a Sign In callback and Local ID callback to make it an active profile. The current profile configuration is incomplete.

Explanation: The make profile current operation has failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity has a valid configuration.

FBTFMS144E An error occurred while communicating with the TDI Server.

Explanation: The list of configuration files for the TDI Server could not be retrieved.

System action: An error has been logged.

Administrator response: Ensure that the TDI Server daemon is running.

FBTFMS145E Could not delete the audit client profile given by ID: ***id*****. Ensure that the profile exists and is not the currently active profile.**

Explanation: The delete operation failed.

System action: An error has been logged.

Administrator response: Ensure that the ID of the given entity exists in the configuration and is not the current profile.

FBTFMS146E STS module chain ***argument*** **cannot be deleted because it is in use.**

Explanation: An error occurred while attempting to delete an STS module chain.

System action: The operation returns failure.

Administrator response: Confirm that the STS module chain is not in use before attempting to delete it.

FBTIDS001W The alias service configuration file (etc/idservice.xml) was not found.

Explanation: The alias service configuration file was not found.

System action: The alias service will start with default clients.

Administrator response: Ensure that the request has all the required data.

FBTIDS002E The module reference id ['*referenceId*'], is invalid. The module reference does not exist.

Explanation: The referenced identifier does not exist.

System action: The plug-in module will not be available at runtime.

Administrator response: Validate the Identity Service configuration.

FBTIDS003E The class '*className*' with module reference id '*referenceId*' could not be initialized. The init method did not successfully complete.

Explanation: The module implementation did not successfully initialize.

System action: The plug-in module will not be available at runtime.

Administrator response: Validate the Identity Service configuration and installed Identity Service plugins.

FBTIDS004E The class '*className*' does not implement the interfaces of class '*referenceClass*'.

Explanation: The module does not implement the required interface.

System action: The plug-in module will not be available at runtime.

Administrator response: Validate the Identity Service configuration and installed Identity Service plugins.

FBTISJ001E Unable to locate the local interface ***name*****.**

Explanation: No EJB instance was found.

System action: The request will be halted.

Administrator response: Validate the configuration of the EJB, then try the operation again.

FBTISJ002E The identity service was unable to read the user's alias.

Explanation: The LDAP alias-read operation failed.

System action: The service will not return a value.

Administrator response: Validate the configuration of the ID service, and check logs for an EJB error message.

FBTISJ003E The identity service was unable to write the user's alias.

Explanation: The LDAP alias-write operation failed.

System action: The service will not return a value.

Administrator response: Validate the configuration of the ID service, and check the logs for an EJB error message.

FBTISL001E The local interface ***name*** **could not be located.**

Explanation: No EJB instance can be found.

System action: The request will be halted.

Administrator response: Validate the configuration of the EJB.

FBTISL002E The remote interface *name* could not be located.

Explanation: No EJB instance can be found.

System action: The request will be halted.

Administrator response: Validate the configuration of the EJB.

FBTISL003E The Naming name of the EJB was not provided.

Explanation: No EJB instance can be found.

System action: The request will be halted.

Administrator response: Validate the configuration of the EJB.

FBTISL004E A manager could not be created on this node. This result might not be an error if the system is running in a clustered environment. Confirm the configuration and startup on the appropriate node.

Explanation: See message.

System action: The request will be halted.

Administrator response: No response required.

FBTISL006E Configuration was not provided for the enterprise bean.

Explanation: No EJB configuration can be found.

System action: The request will be halted.

Administrator response: Validate the configuration of the EJB.

FBTISL007E The provided SSL configuration is not valid.

Explanation: The SSL configuration contains missing parameters or parameters that are not valid.

System action: The request will be halted.

Administrator response: Validate the configuration of the ID service.

FBTISL008E The configuration key *key* is not valid.

Explanation: The configuration contains a parameter key that is not valid.

System action: The configuration key will be ignored.

Administrator response: Validate the configuration of the ID service.

FBTISL012E The bootstrap failed

Explanation: The configuration contains a parameter key.

System action: The configuration key will be ignored.

Administrator response: Validate the configuration of the ID service

FBTISL014E The identity service was unable to read the user's alias.

Explanation: The alias read LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL015E The identity service was unable to write the user's alias.

Explanation: The alias write LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL016E The identity service was unable to read the user's attributes.

Explanation: The attribute read LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL017E The identity service was unable to write the user's attributes.

Explanation: The attribute write LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL018E The provided DN, *dn*, does not exist.

Explanation: The attribute read LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL019E The attribute *attribute* with value *value* could not be written.

Explanation: The attribute write LDAP operation failed.

System action: The service will return no value.

Administrator response: Validate the configuration of the ID service, and check logs for an LDAP error message.

FBTISL020E No trusted keystore was returned by the key service.

Explanation: The call to the key service did not return a trusted keystore.

System action: The service SSL functionality will not operate.

Administrator response: Validate that the configuration has the correct trusted key store name.

FBTISL021E No trusted keystore type was returned by the key service.

Explanation: The call to the key service did not return a trusted keystore type.

System action: The default key store type will be used.

Administrator response: Validate that the configuration has the correct trusted key store name.

FBTISL022E The input provided to the management operation is not valid.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted

Administrator response: Check the trace for the input to the management operation.

FBTISL023E The input provided to the management operation is not valid, the parameter *parameter* is missing.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted

Administrator response: Check the trace for the input to the management operation.

FBTISL024E The input provided to the management operation is not valid and the type *type* for parameter *parameter* is not valid. The expected input is *expectedType*.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted.

Administrator response: Check the trace for the input to the management operation.

FBTISL025E The input provided to the management operation are not valid. The server *server* is undefined.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted.

Administrator response: Check the trace for the input to the management operation.

FBTISL026E The provided service configuration is not valid. The required parameter *parameter* is not specified.

Explanation: The specified parameter is required for ID service LDAP function.

System action: The current operation will be halted.

Administrator response: Check the product documentation for the correct parameters.

FBTISL027E The provided server configuration is not valid. The required parameter *parameter* is not specified.

Explanation: The specified parameter is required for ID service LDAP function.

System action: The current operation will be halted.

Administrator response: Check the product documentation for the correct parameters for server configuration.

FBTISL028E The ID service LDAP management bean could not be registered.

Explanation: An error has occurred while registering the management bean for the ID service LDAP provider.

System action: The server will start with no management interface.

Administrator response: Enable trace and check for errors leading up to this failure.

FBTISL029E The configuration update failed.

Explanation: An error has occurred while updating the server configuration.

System action: The server will continue running with the existing configuration.

Administrator response: Enable trace and check for errors leading up to this failure.

FBTIVT003E The distributed map to run the test cannot be located.

Explanation: The current test cannot be run because the distributed map could not be located.

System action: The test has failed.

Administrator response: Validate the setup of the WebSphere Application Server environment, cluster, and replication domain.

FBTIVT004E The key "*key*" cannot be located in the distributed map.

Explanation: The current test has failed because the specified key could not be found.

System action: The test has failed.

Administrator response: Validate the setup of the WebSphere Application Server environment, cluster, and replication domain.

FBTKES001E The global configuration properties file is not in the classpath of the server.

Explanation: The global configuration properties file could not be found in the server's classpath. The file is typically created at installation time for the installer and is required for the server to successfully start.

System action: The request is halted.

Administrator response: Ensure that the system was installed correctly, locate the global configuration properties file, and ensure that the file is located in the server's classpath.

FBTKES002E No keystore or keystore password was provided.

Explanation: A keystore or keystore password or both must be provided for the server to start.

System action: The request is halted.

Administrator response: Ensure that the keystore has the correct file permissions for the server to read and write.

FBTKES003E The password could not be unobfuscated.

Explanation: The obfuscated password could not successfully be unobfuscated.

System action: The request is halted.

Administrator response: Check that the Java that supports the A.E.S. 128-cipher algorithm is being used.

FBTKES005E A problem was encountered while creating the keystore at location: *filename*.

Explanation: Because the keystore at the given location did not exist, the server attempted to create a new keystore but failed.

System action: The keystore was not created.

Administrator response: Ensure that the directory path up to the given file exists and that the correct read and write file permissions are set. Check the cause exception to get more specific details about what caused the problem.

FBTKES006E The key type for the given alias *alias* is an unknown key.

Explanation: An attempt was made to use a key that has an unknown type.

System action: No action taken.

Administrator response: Ensure that the key for the given alias is a supported key type.

FBTKES007E A key was not found with the given alias (*alias*).

Explanation: The server could not find a key with the provided alias.

System action: No action taken.

Administrator response: Ensure that you have the correct keystore configured.

FBTKES008E The required input was not given.

Explanation: The required input was not given to process the request.

System action: The request is halted.

Administrator response: Ensure that the correct input is given.

FBTKES009E The document owner was not given. The signature template could not be generated.

Explanation: For the signature template to generate correctly, the document owner must be provided.

System action: The request is halted.

Administrator response: Ensure that the caller provides the correct document owner.

FBTKES010E A reference list of elements to be signed was not given. The signature template cannot be generated without a reference list.

Explanation: For a signature template to be generated, a reference list must be provided.

System action: The request is halted.

Administrator response: Ensure that the caller provides the correct reference list of elements to be referenced in the generated signature template.

FBTKES011E A context was not provided by caller.

Explanation: The caller did not provide a context.

System action: The request is halted.

Administrator response: Ensure that a context is provided.

FBTKES012E A key alias was not provided by the caller.

Explanation: The caller did not provide a key alias.

System action: The request is halted.

Administrator response: Ensure that a key alias is provided.

FBTKES013E No data was provided to be signed.

Explanation: The caller did not provide any data to be signed.

System action: The request is halted.

Administrator response: Ensure that there is data provided.

FBTKES014E A certificate was not found with the given alias (*alias*).

Explanation: The server could not find a certificate with the provided alias.

System action: The request is halted.

Administrator response: Ensure that you have the correct keystore configured.

FBTKES015E The signature validation failed.

Explanation: The server encountered an error while attempting to validate a signature.

System action: The request is halted.

Administrator response: Check the cause exception to find more details about why the validation failed.

FBTKES016E No document was given.

Explanation: An XML document is required to perform the operation.

System action: The request is halted.

Administrator response: Ensure that a document is provided.

FBTKES017E The signature creation operation failed.

Explanation: The server encountered an error while attempting to sign the given data.

System action: The request is halted.

Administrator response: Check the cause exception to find more details about why the signing failed.

FBTKES020E The signature was not valid.

Explanation: The signature was determined to be invalid while attempting to validate the byte array of the signature.

System action: The request is halted.

Administrator response: No response required.

FBTKES021E No keystore directory was provided.

Explanation: A keystore directory must be provided for the server to start.

System action: The request is halted.

Administrator response: Ensure that the keystore directory is provided.

FBTKES022E The keystore directory provided (*alias*) does not exist or is not a directory.

Explanation: The keystore directory provided in the configuration does not exist or is not a directory.

System action: The request is halted.

Administrator response: Ensure that the given directory exists.

FBTKES023E The required path element was not provided.

Explanation: For the given request, a path that points to the specific XML element is required.

System action: The request is halted.

Administrator response: Ensure that the caller is passing all required parameters.

FBTKES024E The given element path did not point to an XML element.

Explanation: For the given request, a path that points to the specific XML element is required.

System action: The request is halted.

Administrator response: Ensure that the caller is passing all required parameters.

FBTKES025E The key encryption and signature service client factory could not locate the key encryption and signature service module.

Explanation: The modules or module directory could not be located in the current environment configuration.

System action: The request is halted.

Administrator response: Ensure that the caller is passing all required parameters and that the configuration is correct.

FBTKES026E An alias was not given.

Explanation: The caller did not pass an alias.

System action: The request is halted.

Administrator response: Ensure that the key configuration has all the correct key alias names configured.

FBTKES027E The given key profile does not have a cipher assigned or an error occurred when getting an instance of the cipher.

Explanation: The key profile given did not return a cipher.

System action: The request is halted.

Administrator response: Ensure that the key profile configuration has the cipher configured correctly.

FBTKES028E The raw key bytes for key *id* were not specified.

Explanation: The key bytes were not specified in the configuration file for the given key ID.

System action: The key given was not generated, process continued to the next key in the configuration file.

Administrator response: Ensure that the key configuration has the required configuration item.

FBTKES029E The type for key *id* was not specified.

Explanation: The type was not specified in the configuration file for the given key ID.

System action: The key given was not generated, process continued to the next key in the configuration file.

Administrator response: Ensure that the key configuration has the required configuration item.

FBTKES030E An unknown error occurred, the cipher returned no data but data was expected.

Explanation: Data was given to the cipher engine but it did not return any data.

System action: The request is halted.

Administrator response: Ensure that key profile, the cipher and the key are configured correctly.

FBTKES031E During the decryption an error was encountered. It appears the given cipher text is corrupt.

Explanation: The given cipher text could not be decrypted and parsed into a valid XML document.

System action: The operation will return a failure.

Administrator response: Confirm that the message is not being altered.

FBTKES032W The certificate with the subject's distinguished name of [*dn*] and serial of [*number*] has expired, therefore it was not used for runtime operations.

Explanation: The given certificate has expired and will not be used for runtime operations.

System action: The system will not use the certificate.

Administrator response: Only use certificates that are still valid.

FBTKES033E The block cipher algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation: The block cipher algorithm URI provided from configuration is not supported by the XML security API.

System action: The system will not complete the request.

Administrator response: Change the configuration to a supported block cipher algorithm URI.

FBTKES034E The key transport algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation: The key transport algorithm URI provided from configuration is not supported by the XML security API.

System action: The system will not complete the request.

Administrator response: Change the configuration to a supported key transport algorithm URI.

FBTKES035E The provided message contained too many EncryptedKey elements, the process is unable to determine the correct key to use.

Explanation: The provided message did not have a KeyInfo element as a child of the EncryptedData element. Because there was no KeyInfo element, the service has to look for EncryptedKey elements under the parent node of the EncryptedData. If there is more than one EncryptedKey element under the parent, this error is returned.

System action: The system will not complete the request.

Administrator response: Ensure the given message contains a KeyInfo element as a child of the EncryptedData element, which includes either the EncryptedKey or references the EncryptedKey if there is more then one EncryptedKey in the message.

FBTKES036E No EncryptedKey element found, the process cannot decrypt the given message.

Explanation: The given message did not contain a EncryptedKey element, the EncryptedKey element contains the key material to decrypt the EncryptedData element.

System action: The system will not complete the request.

Administrator response: Ensure that messages contain at least one EncryptedKey element for every EncryptedData element.

FBTKES037E The key encryption and signature service client factory could not locate a certificate path validator module.

Explanation: The modules or module directory could not be located in the current environment configuration.

System action: The request is halted.

Administrator response: Ensure that the required certificate path validator module is properly configured and installed.

FBTKES038W Certificate path validation is disabled because no keystores of type CA Certificates are configured.

Explanation: There are no keystores of type CA Certificates configured.

System action: The request is halted.

Administrator response: Ensure that at least one keystore containing CA certificates is configured with a type of CA Certificates.

FBTKES039E The configuration file *file* could not be read.

Explanation: The configured file might not exist, might not be readable by this user, or might not be a valid file.

System action: The server cannot perform initialization of the hardware device.

Administrator response: Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES040E A <HardwareProviderType> element could not be found with reference ID *idref* in etc/kessjks.xml.

Explanation: The configuration file contains a reference to an element that does not exit.

System action: The server cannot perform initialization of the hardware device.

Administrator response: Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES041E A <ModuleReference> element could not be found with reference ID *idref* in etc/kessjks.xml.

Explanation: The configuration file contains a reference to an element that does not exit.

System action: The server will skip initialization of the module referenced by the ID.

Administrator response: Correct the configuration for the hardware provider in etc/kessjks.xml and restart the server.

FBTKES042E The hardware cryptographic device could not be initialized.

Explanation: The hardware cryptographic device failed to initialize. See previous messages.

System action: The server will not be able to perform signing and cryptography services.

Administrator response: Verify that the hardware device is installed correctly and is operating properly.

FBTKES043E There is no provider available to perform the requested operation.

Explanation: The signature and cryptographic provider failed to initialize. See previous messages.

System action: The server cannot perform the requested operation.

Administrator response: Check the message log for related errors and take corrective action accordingly.

FBTKES044E The key encryption and signature service configuration is missing the required parameter *parameter*.

Explanation: An error has occurred while validating the server configuration. This error is due to the absence of a required parameter.

System action: The server will not function with a missing configuration.

Administrator response: Ensure that the missing configuration entry is specified.

FBTKES045E The hardware cryptography feature is not supported by Tivoli Federated Identity Manager on this version of WebSphere Application Server.

Explanation: The installed version of WebSphere Application Server does not provide the proper support for the hardware cryptography feature.

System action: The server will not function with a missing configuration.

Administrator response: Either upgrade to WebSphere Application Server version 6.1 or greater, or disable the hardware cryptography feature.

FBTKES046E The key profile with alias *alias* requires an initialization vector.

Explanation: The mode of the cipher in the key profile requires an initialization vector to be configured.

System action: The key profile is discarded.

Administrator response: Correct the configuration and restart the server.

FBTKES047E The key profile with alias *alias* has an incomplete initialization vector.

Explanation: The initialization vector must include a size or initialization data to be configured.

System action: The key profile is discarded.

Administrator response: Correct the configuration and restart the server.

FBTKES048E An exception occurred while processing the keystore on the hardware device. The exception message text is: *message*.

Explanation: An exception was encountered while processing the keystore provided by the hardware device.

System action: The keys and certificates not already processed will be unavailable.

Administrator response: Correct the configuration and restart the server.

FBTKES049E The message signature did not include the required KeyInfo data to find a validation certificate.

Explanation: The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but the signature does not have the required data.

System action: The request is rejected.

Administrator response: Ensure that the sender includes either a Public Key, X509 Certificate data, X509 Subject Key Identifier or X509 Subject Name in the KeyInfo element of the signature.

FBTKES050E The message signature did not include any KeyInfo data that matches the configured DN expression [*alias*].

Explanation: The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but the DN of the certificate does not match the allowable names in the configuration.

System action: The request is rejected.

Administrator response: Ensure that the configured DN expression is correct and retry the operation.

FBTKES051E There are no certificates available that match the KeyInfo data in the message signature for the DN [*alias*].

Explanation: The server is configured to use the KeyInfo data in the message signature to locate a key for signature validation but a certificate could not be found in any keystore.

System action: The request is rejected.

Administrator response: Ensure that the public key certificate is imported into the Tivoli Federated Identity Manager keystore.

FBTKES052E The signature algorithm URI provided [*URI*] is not supported.

Explanation: The system does not support the signature algorithm URI provided from the configuration.

System action: The system will not complete the request.

Administrator response: Change the configuration to the supported signature algorithm URI.

FBTKES053E The digest algorithm URI provided [*URI*] is not supported.

Explanation: The system does not support the digest algorithm URI provided from the configuration.

System action: The system will not complete the request.

Administrator response: Change the configuration to the supported digest algorithm URI.

FBTKES054E The signing key type [*KeyType*] does not match the signature algorithm [*URI*].

Explanation: The signing key type does not match the signature algorithm provided from the configuration.

System action: The system will not complete the request.

Administrator response: Change the configuration to match the key type and signature algorithm.

FBTKES055E The key type [*KeyType*] does not support encryption.

Explanation: The key type provided from configuration does not support encryption.

System action: The system cannot complete the request.

Administrator response: Change the configuration to a supported encryption key type.

FBTKJK001E A manager could not be created on this node. This result might not be an error if the system is running in a clustered environment. Confirm configuration and startup on the appropriate node.

FBTKJK002E The global configuration properties file is not in the classpath of the server.

Explanation: The global configuration properties file could not be found in the server's classpath. The file is typically created at installation time for the installer and is required for the server to successfully start.

System action: The global configuration properties file could not be found.

Administrator response: Ensure that the system was installed correctly, locate the global configuration properties file, and ensure that the file is located in the server's classpath.

FBTKJK006E The Key Encryption and Signature Service Java Keystore management bean cannot be registered.

Explanation: An error has occurred registering the management bean for the Key Encryption and Signature Service Java Keystore provider.

System action: The server will start with no management interface.

Administrator response: Enable a trace and check for errors leading up to this failure.

FBTKJK007E The configuration file for the Key Encryption and Signature Service Java Keystore, *filename*, cannot be read.

Explanation: An error has occurred reading the configuration for the Key Encryption and Signature Service Java Keystore provider.

System action: The server will not be able to start unless the configuration file is located on another node.

Administrator response: Enable a trace and check for errors leading up to this failure.

FBTKJK008E The bootstrap of the Key Encryption and Signature Service Java Keystore provider has failed.

Explanation: The bootstrap process of the Key Encryption and Signature Service Java Keystore did not complete successfully.

System action: Check earlier error and trace messages for problems leading up to this failure.

Administrator response: Validate the configuration of the Key Encryption and Signature Service Java Keystore provider.

FBTKJK009E The input provided to the management operation is not valid.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted.

Administrator response: Check the trace for the input to the management operation.

FBTKJK010E The input provided to the management operation is not valid. The parameter *parameter* is missing.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted.

Administrator response: Check the trace for the input to the management operation.

FBTKJK011E The input provided to the management operation is not valid. The type *type* for parameter *parameter* is not valid. A value of *expectedType* was expected.

Explanation: This error is typically due to null input values, missing input values, or input values of the wrong type.

System action: The management operation will be halted.

Administrator response: Check the trace for the input to the management operation.

FBTKJK012E The configuration update failed.

Explanation: An error has occurred while updating the server configuration.

System action: The server will continue running with the existing configuration.

Administrator response: Enable a trace and check for errors leading up to this failure.

FBTKJK015E The key encryption and signature service configuration could not be discovered because no configuration store was found.

Explanation: An error has occurred discovering the server configuration. This error occurred because the distributed map instance could not be located.

System action: The server will not function without configuration information.

Administrator response: Ensure that the configuration store is running on the application server and enable the trace to check for errors leading up to this failure.

FBTKJK016E The key encryption and signature service configuration is missing the required parameter *parameter*.

Explanation: An error has occurred while validating the server configuration. This error is due to the absence of a required parameter.

System action: The server will not function with a missing configuration.

Administrator response: Ensure that the missing configuration entry is specified.

FBTKJK017E The configured Java key store configuration directory *directory* could not be read.

Explanation: The configured directory might not exist, might not be readable by this user, or might not be a directory.

System action: The server will not function with a missing configuration.

Administrator response: Ensure that the configured entry is valid.

FBTKJK018E The configured Java key store configuration directory contains a file *file* that could not be read.

Explanation: The configured file might not exist, might not be readable by this user, or might not be a valid.

System action: The server will attempt to read the remaining files in the directory.

Administrator response: Ensure that the file is valid.

FBTKJK021E The required input was not given.

Explanation: The required input was not given to process the request.

System action: The request could not be processed because the required input is missing.

Administrator response: Ensure that the correct input is given.

FBTKJK022E The document owner was not given and the signature template could not be generated.

Explanation: For the signature template to generate correctly, the document owner must be provided.

System action: The signature template was not generated.

Administrator response: Ensure that the caller provides the correct document owner.

FBTKJK023E A reference list of elements to be signed was not given. The signature template cannot be generated without a reference list.

Explanation: For a signature template to be generated, a reference list must be provided.

System action: Ensure that the caller provides the correct list of elements to be referenced in the generated signature template.

Administrator response: Ensure that the caller provides the correct list of elements to be referenced in the generated signature template.

FBTKJK024E A context was not provided by the caller.

Explanation: The caller did not provide a context.

System action: The request is halted.

Administrator response: Ensure that a context is provided.

FBTKJK025E A key alias was not provided by caller.

Explanation: The caller did not provide a key alias.

System action: The request is halted.

Administrator response: Ensure that a key alias is provided.

FBTKJK026E There was no data provided to be signed.

Explanation: The caller did not provide any data to be signed.

System action: The request is halted.

Administrator response: Ensure that data is provided.

FBTKJK027E A certificate with given alias (*alias*) was not found.

Explanation: The server could not find a certificate with the provided alias.

System action: Ensure that you have the correct keystore configured.

Administrator response: Ensure that you have the correct keystore configured.

FBTKJK028E Signature validation failed.

Explanation: The server encountered an error while attempting to validate a signature.

System action:

Administrator response: Check the cause exception to determine why the validation failed.

FBTKJK029E No document was given.

Explanation: An XML document is required to perform the operation.

System action: The request is halted.

Administrator response: Ensure that a document is provided.

FBTKJK030E The signature creation operation failed.

Explanation: The server encountered an error while attempting to sign the given data.

System action: The request is halted.

Administrator response: Check the cause exception to determine why the signing failed.

FBTKJK031E The signature is not valid.

Explanation: See message.

System action: The request is halted.

Administrator response: Check the logs for exceptions to determine why signature validation failed.

FBTKJK032E A key was not found with the given alias (*alias*).

Explanation: The server could not find a key with the provided alias.

System action: Ensure that you have the correct keystore configured.

Administrator response: Ensure that you have the correct keystore configured.

FBTKJK033E The required path element was not provided.

Explanation: For the given request, a path that points to the specific XML element is required.

System action: The request is halted.

Administrator response: Ensure that the caller is passing all required parameters.

FBTKJK034E The given element path did not point to an XML element.

Explanation: For the given request, a path that points to the specific XML element is required.

System action: The request is halted.

Administrator response: Ensure that the caller is passing all required parameters.

FBTKJK035E The key type for a given alias *alias* is an unknown key.

Explanation: An attempt was made to use a key that has an unknown type.

System action: An attempt was made to use a key that has an unknown type.

Administrator response: Ensure that the key for given alias is a supported key type.

FBTKJK036E The key encryption and signature service Java keystore was unable to find a worker to complete the task. This error is likely due to an incorrect configuration.

Explanation: No configuration worker instance could be found.

System action: The operation returned failure.

Administrator response: Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK037E The key encryption and signature service Java keystore EJB client could not create the remote interface, *remote*

Explanation: No remote EJB instance could be created.

System action: The operation will return a failure.

Administrator response: Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK038E The key encryption and signature service Java keystore EJB client encountered an error with the EJB invocation.

Explanation: An exception was thrown while communicating with the remote EJB.

System action: The operation will return a failure.

Administrator response: Enable a trace and check the logs for errors that might have lead up to this action.

FBTKJK039E The SignedInfo signature value does not match the calculated value.

Explanation: The SignedInfo portion of the signature did not match the calculated value. This error is usually caused by the SignedInfo digest not matching or the public key used to validate does not match the private key used to sign.

System action: The operation will return a failure.

Administrator response: Ensure that the correct certificate is used to validate the message.

FBTKJK040E The Reference with the identifier *identifier* **calculated a different digest value.**

Explanation: The given Reference digest did not match the calculated digest. This error is usually caused by the message changing after being signed.

System action: The operation will return a failure.

Administrator response: Ensure that the message does not change after being signed.

FBTKJK041E While writing out the updated file *filename***, an error was encountered. The update to the file did not occur.**

Explanation: An error was encountered when making an update to the given file.

System action: The operation will return a failure.

Administrator response: Ensure that the given file exists and has the correct file permissions to allow updates to occur. See the corresponding exception in the trace file for more details.

FBTKJK042E The directory *directory* **cannot be read.**

Explanation: An error was encountered when attempting to read the directory given.

System action: The operation will return a failure.

Administrator response: Ensure that the given directory exists and that the correct file permissions are enabled.

FBTKJK043E The backup operation failed. The backup JAR file *filename* **for directory** *directory* **cannot be created.**

Explanation: An error was encountered when attempting to create a backup.

System action: The operation will return a failure.

Administrator response: Ensure that the given directory exists and that the correct file permissions are enabled.

FBTKJK045E The management operation is missing required input values. The management operation has failed to complete.

Explanation: The management operation is missing required input.

System action: The operation will return a failure.

Administrator response: The management operation being called requires specific input to complete the operation. Check the documentation for all the required input.

FBTKJK046E The provided password is incorrect or the *keystore* **keystore does not exist. The management operation has failed to complete.**

Explanation: The provided password was not correct, or the keystore does not exist.

System action: The operation will return a failure.

Administrator response: Ensure that the keystore exists and ensure that the correct password was entered.

FBTKJK047E An error was encountered when retrieving the encoded format of the certificate.

Explanation: An attempt was made to encode a certificate that returned errors.

System action: The operation will return a failure.

Administrator response: Check the trace logs to find out a more specific exception error.

FBTKJK048E An error was encountered while creating the keystore for export. The export operation failed.

Explanation: During the generation of the keystore to export, the server encountered a error.

System action: The operation will return a failure.

Administrator response: Check the logs for an exception that will give a more specific reason for the error.

FBTKJK049E An error was encountered while importing the given keystore. The import operation failed.

Explanation: During the importing of the keystore, the server encountered a error.

System action: The operation will return a failure.

Administrator response: Check the logs for an exception that will give a more specific reason for the error.

FBTKJK050E The store *storename* **does not exist. The operation failed to complete.**

Explanation: The given store does not exist.

System action: The operation will return a failure.

Administrator response: Ensure that the given store exists.

FBTKJK051E The import into store *storename* **failed. The operation failed to complete. Check the trace logs for more specific errors.**

Explanation: An error was encountered when the key or certificate or both were being imported.

System action: The operation will return a failure.

Administrator response: Check the trace logs for a more specific error message.

FBTKJK052E The password for the given keystore is incorrect. The operation failed to complete.

Explanation: An error was encountered while validating the password for the given keystore.

System action: The operation will return a failure.

Administrator response: Ensure that the correct password is entered for the keystore or for the key entry.

FBTKJK053E An error occurred when attempting to update the store (*storename***) with the new data. The operation failed to complete.**

Explanation: An error occurred when updating the store listed.

System action: The operation will return a failure.

Administrator response: Check the trace logs for a more specific error message.

FBTKJK054E The key alias *alias name* **returned no data for the keystore provided. Confirm that the key alias given exists. The operation failed to complete.**

Explanation: There are no keys or certificates located at the key alias given.

System action: The operation will return a failure.

Administrator response: Confirm that the given key alias exists in the provided keystore.

FBTKJK055E The key alias *alias name* **already exists in the store** *store name***. The operation failed to complete.**

Explanation: The import operation was asked to not overwrite existing key aliases and the alias provided already existed in the store.

System action: The operation will return a failure.

Administrator response: Confirm that the given key alias does not exist in the provided store.

FBTKJK056W The certificate with the subject's distinguished name of [*dn***] and serial of [***number***] has expired therefore it was not used for runtime operations.**

Explanation: The given certificate has expired and will not be used for runtime operations.

System action: The system will not use the certificate.

Administrator response: Only use certificates that are still valid.

FBTKJK057E The block cipher algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation: The block cipher algorithm URI provided from configuration is not supported by the XML security API.

System action: The system will not complete the request.

Administrator response: Change the configuration to a supported block cipher algorithm URI.

FBTKJK058E The key transport algorithm URI provided [*URI*] is not supported by the XML security API.

Explanation: The key transport algorithm URI provided from configuration is not supported by the XML security API.

System action: The system will not complete the request.

Administrator response: Change the configuration to a supported key transport algorithm URI.

FBTKJK059E The provided message contained too many EncryptedKey elements, we are unable to determine the correct key to use.

Explanation: The provided message did not have a KeyInfo element as a child of the EncryptedData element. Since there was no KeyInfo element the service has to look for EncryptedKey elements under the parent node of the EncryptedData. If there is more then one EncryptedKey element under the parent, this error is returned.

System action: The system will not complete the request.

Administrator response: Ensure the given message contains a KeyInfo element as a child of the EncryptedData element which includes either the EncryptedKey, or which references the EncryptedKey if there is more then one EncryptedKey in the message.

FBTKJK060E No EncryptedKey element found, we are unable to decrypt the given message.

Explanation: The given message did not contain a EncryptedKey element, the EncryptedKey element contains the key material to decrypt the EncryptedData element.

System action: The system will not complete the request.

Administrator response: Ensure that messages contain at least one EncryptedKey element for every EncryptedData element.

FBTLIB001E A configuration error has occurred.

Explanation: A configuration error has occurred due to invalid configuration.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB002E Internal Error: The delegate protocol was unable to retrieve the Liberty Request Context.

Explanation: Internal Error: The delegate protocol was unable to retrieve the Liberty Request Context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB003E The Liberty plug-in is not able to route the incoming request correctly.

Explanation: The Liberty plug-in is not able to determine the protocol that must be used for the incoming request.

System action: The request has been halted.

Administrator response: Make sure that the endpoint that is configured is correct. Enable a trace for detailed messages about the error.

FBTLIB004E Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP GET.

Explanation: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP GET.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB005E Internal Error: The delegate protocol cannot retrieve the AuthnResponse from incoming HTTP POST.

Explanation: The delegate protocol cannot retrieve the AuthnResponse from incoming HTTP POST.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB006E Internal Error: The delegate protocol cannot decode the incoming AuthnResponse from BASE64.

Explanation: The delegate protocol cannot decode the incoming AuthnResponse from BASE64.

System action: The request has been halted.

Administrator response: Make sure that the AuthnResponse was encoded correctly by the partner. Enable a trace for detailed messages about the error.

FBTLIB007E Internal Error: The delegate protocol cannot retrieve the value in the LARES field in the incoming AuthnReponse POST.

Explanation: The delegate protocol cannot retrieve the value in the LARES field in the incoming AuthnReponse POST.

System action: The request has been halted.

Administrator response: Make sure that the AuthnResponse was sent by the partner adhering to Liberty specifications. Enable a trace for detailed messages about the error.

FBTLIB008E Internal Error: An error was encountered in the execution of protocol chain.

Explanation: An error was encountered in the execution of protocol chain.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB009E Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

Explanation: The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB010E Internal Error: The Delegate protocol is unable to obtain the SingleSignOnUrl from the context.

Explanation: The Delegate protocol is unable to obtain the SingleSignOnUrl from the context.

System action: The request has been halted.

Administrator response: Make sure all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB011E Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnResponse from LibertyContext.

Explanation: The Delegate protocol is unable to process the response because it could not retrieve the AuthnResponse from LibertyContext.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB012E Internal Error: The Delegate protocol is unable to process the response because it could not convert the AuthnResponse to an XML string.

Explanation: The Delegate protocol is unable to process the response because it could not convert the AuthnResponse to an XML string.

System action: The request has been halted.

Administrator response: The AuthnResponse message might not be formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB013E Internal Error: The Delegate protocol is unable to convert the response from an XML string to BASE64 encoded data.

Explanation: The Delegate protocol is unable to convert the response from an XML string to BASE64 encoded data.

System action: Contact your IBM support representative.

Administrator response: The AuthnResponse message might not be formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB014E Internal Error: The Delegate protocol is unable to obtain the AssertionConsumerUrl from the context.

Explanation: The Delegate protocol is unable to obtain the AssertionConsumerUrl from the context.

System action: The request has been halted.

Administrator response: Make sure that all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB015E Internal Error: The Delegate protocol is unable to obtain the RelayState from the AuthnResponse.

Explanation: The Delegate protocol is unable to obtain the RelayState from the AuthnResponse.

System action: The request has been halted.

Administrator response: RelayState might not be set correctly in the AuthnResponse. Enable a trace for detailed messages about the error.

FBTLIB016E Internal Error: The Delegate protocol is unable to find the template page *PageTemplate*.

Explanation: The delegate protocol is unable to find the specified page template.

System action: Contact your IBM support representative.

Administrator response: Make sure that the product is installed and configured correctly. Enable a trace for detailed messages about the error.

FBTLIB017E Internal Error: The delegate protocol cannot retrieve the LogoutRequest from incoming HTTP GET.

Explanation: The delegate protocol cannot retrieve the LogoutRequest from incoming HTTP GET.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB018E The delegate protocol cannot retrieve the *EndPointType* from the defined federations.

Explanation: The specified endpoint is not configured.

System action: The request has been halted.

Administrator response: Make sure that all the endpoints are configured correctly. Enable a trace for detailed messages about the error.

FBTLIB019E The delegate protocol cannot convert the logout response to a URL encoded string.

Explanation: The delegate protocol cannot convert the logout response to a URL encoded string.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB020E Internal Error: The delegate protocol could not find the session ID *SessionId* in the global session.

Explanation: The specified session ID was not found in the global session.

System action: Contact your IBM support representative.

Administrator response: The session ID might not have been stored or it might have expired. Enable a trace for detailed messages about the error.

FBTLIB021E The delegate protocol configuration determined that no federations are defined.

Explanation: The delegate protocol configuration determined that no federations are defined.

System action: Contact your IBM support representative.

Administrator response: Make sure that the federations are defined. Enable a trace for detailed messages about the error.

FBTLIB022E The required attribute *VariableName* was not found in the defined self-federation entity.

Explanation: The specified attribute is not defined in the self-federation entity.

System action: Contact your IBM support representative.

Administrator response: Make sure that the specified required attribute is defined in the self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB023E The Delegate protocol configuration could not find the Provider ID in the defined self-federation entity.

Explanation: The Delegate protocol configuration could not find the Provider ID in the defined self-federation entity.

System action: Contact your IBM support representative.

Administrator response: Make sure that the Provider ID is defined in the self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB024E The Delegate protocol configuration could not find the Key identifier in the defined self-federation entity.

Explanation: The Delegate protocol configuration could not find the Key identifier in the defined self-federation entity.

System action: The request has been halted.

Administrator response: Make sure the Key identifier is defined in the defined self-federation entity. Enable a trace for detailed messages about the error.

FBTLIB025E The SOAPEndpoint URL is malformed. SoapEndpoint = *SoapEndpoint*

Explanation: The specified SOAPEndpoint URL is not valid.

System action: The request has been halted.

Administrator response: Make sure that the correct SOAPEndpoint is configured. Enable a trace for detailed messages about the error.

FBTLIB026E The Liberty plug-in cannot connect to SOAPEndpoint *SoapEndpoint*

Explanation: The Liberty plug-in cannot connect to the specified SOAPEndpoint.

System action: The request has been halted.

Administrator response: Make sure that the SOAPEndpoint accepts connections. Enable a trace for detailed messages about the error.

FBTLIB027E The Liberty plug-in caught an unexpected exception when sending the SOAP message.

Explanation: The Liberty plug-in caught an unexpected exception when sending the SOAP message.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB028E The Liberty plug-in received a SOAP request that is not valid.

Explanation: The Liberty plug-in received a SOAP request that is not valid.

System action: The request is halted.

Administrator response: Make sure that the received SOAP request is formatted correctly. Enable a trace for detailed messages about the error.

FBTLIB029E The keystore is not initialized for SSL communication for the SOAP client.

Explanation: The keystore is not initialized for SSL communication for the SOAP client.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB030E The Liberty plug-in caught an exception during SSL initialization.

Explanation: The Liberty plug-in caught an exception during SSL initialization.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB031E The Liberty plug-in configuration failed to find the key *Key* **in the SPS configuration.**

Explanation: The Liberty plug-in configuration failed to find the specified key in the SPS configuration.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB032E The Liberty SOAP client failed to initialize due to an unexpected exception.

Explanation: The Liberty SOAP client failed to initialize due to an unexpected exception.

System action: The request has been halted.

Administrator response: Make sure that the SOAP back channel configuration is correct. Enable a trace for detailed messages about the error.

FBTLIB033E The Liberty plug-in is unable to get an artifact from the context.

Explanation: The Liberty plug-in is unable to get an artifact from the context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB034E The Liberty plug-in is unable to get an artifact from the incoming HTTP GET query parameters.

Explanation: The Liberty plug-in is unable to get an artifact from the incoming HTTP GET query parameters.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB035E The Liberty plug-in is unable to get a SAML response from the context.

Explanation: The Liberty plug-in is unable to get a SAML response from the context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB036E Internal Error: The Delegate protocol is unable to get the logout response from the received HTTP GET.

Explanation: The Delegate protocol is unable to get the logout response from the received HTTP GET.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB037E Internal Error: The delegate protocol cannot retrieve the Logout response from the context.

Explanation: The delegate protocol cannot retrieve the Logout response from the context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB038E The delegate protocol cannot convert a logout request to a URL-encoded string.

Explanation: The delegate protocol cannot convert a logout request to a URL-encoded string.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB039E Internal Error: The Delegate protocol is unable to process the request because it could not retrieve a LogoutRequest from LibertyContext.

Explanation: The Delegate protocol is unable to process the request because it could not retrieve a LogoutRequest from LibertyContext.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB040E An incorrect LECP header was received in the incoming request.

Explanation: An incorrect LECP header was received in the incoming request.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB041E The Delegate protocol is unable to get the AuthnRequest from the incoming SOAP message.

Explanation: The Delegate protocol is unable to get the AuthnRequest from the incoming SOAP message.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB042E The Delegate protocol is unable to get the AuthnResponse from the received HTTP POST.

Explanation: The Delegate protocol is unable to get the AuthnResponse from the received HTTP POST.

System action: The request has been halted.

Administrator response: Make sure that the partner is configured to send the AuthnResponse. Enable a trace for detailed messages about the error.

FBTLIB043E The Delegate protocol is unable to find an AuthnRequest in the received SOAP message.

Explanation: The Delegate protocol is unable to find an AuthnRequest in the received SOAP message.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB044E Internal Error: The Delegate protocol is unable to get the AuthnRequestEnvelope from the Context.

Explanation: The Delegate protocol is unable to get the AuthnRequestEnvelope from the Context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB045E Internal Error: The Delegate protocol is unable to get the AuthnResponseEnvelope from the Context.

Explanation: The Delegate protocol is unable to get the AuthnResponseEnvelope from the Context.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB046E A common domain name has not been configured.

Explanation: An attempt was made to perform an Identity Provider introduction but a common domain name was not configured.

System action: The operation was not performed.

Administrator response: Configure a common domain name and restart the server.

FBTLIB047E An MSISDN header was not found in the incoming LECP request.

Explanation: The incoming LECP request does not contain an MSISDN header.

System action: The request was rejected.

Administrator response: Configure the LECP provider ID correctly and restart the server.

FBTLIB048E An error was encountered while unobfuscating the password *ObfuscatedPassword* for key *Key* from the configuration.

Explanation: Liberty plug-in tried to unobfuscate the specified password set in the configuration, but failed to do so.

System action: The Liberty plug-in failed to initialize SSL for the SOAP backchannel.

Administrator response: Configure SSL for the SOAP backchannel correctly and restart the server.

FBTLIB049E Partner provider ID cannot be determined for checking signature configuration options.

Explanation: Liberty plug-in tried to find the partner this message was sent to or received from, but failed to do so.

System action: The Liberty plug-in failed to determine the partner from the configuration.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB050E Request to create an unsolicited AuthnResponse was received but the request does not contain all the required parameters.

Explanation: The required parameters are missing in the request.

System action: The request was rejected.

Administrator response: The request must have the TargetURL and ProviderID parameters set.

FBTLIB100E The value *value* received for *AttributeName* in the *ElementName* element is not valid.

Explanation: The data received from the peer node does not conform to Liberty protocol version 1.0.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB101E A value for the attribute *AttributeName* must be provided for the <*ElementName*> element.

Explanation: The application is in error. Required data was not set in the Liberty protocol object.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB102E The *VariableName* message that was received specifies an unsupported version [*MajorMinor*]. Only version *MajorMinor* is supported.

Explanation: The data from the peer node specifies a version that is not supported by this application.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB103E The received message failed signature verification: *error_message*.

Explanation: The received message was signed but signature verification failed.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB104E The received message was not signed.

Explanation: This application is configured to require that all received messages must be signed, but the message received was not signed.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB105E The attempt to sign a message was unsuccessful.

Explanation: The protocol message could not be signed. This error could be caused by a keystore configuration error or expired certificates.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB106E An unexpected exception was caught while initializing the keystore.

Explanation: An unexpected exception was caught from the key service.

System action: The request will not be signed.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB107E An unexpected exception was caught decoding a BASE64 encoded string.

Explanation: A string that should be BASE64 encoded could not be decoded.

System action: The string is ignored.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB108E The member element *MemberElementName* **must be provided for the <***ElementName***> element.**

Explanation: The application is in error. Required data was not set in the Liberty protocol object.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB109E The received <*ElementName***> element does not contain the required member element** *MemberElementName***.**

Explanation: The sending application is in error. Required data was not included in the incoming request message.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB110E The received element <*ElementName***> does not contain the required attribute** *MemberElementName***.**

Explanation: The sending application is in error. Required data was not included in the incoming request message.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB111E The received element <*ElementName***> does not match the expected element <***ExpectedElementName***>.**

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB112E The elements <*ElementName***> and <***ElementName***> are mutually exclusive members of the <***ElementName***> element.**

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB113E The artifact string length is not valid. The length is <*length***> bytes instead of 42 bytes.**

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB114E The artifact type is unsupported.

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB115E The signature algorithm <*length*> is missing or unsupported.

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB116E The received namespace URI [*Namespace*] does not match the expected namespace URI [*ExpectedNamespace*] for element <*ExpectedNamespace*>.

Explanation: The sending application is in error. The request or response does not conform to the Liberty message protocol.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB117E The received URL-encoded <*Request*> is not valid: [*Input string*].

Explanation: The URL-encoded string that was received is not valid. The most likely cause is that the data was sent to the wrong URL endpoint by the sender.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB118E A key alias was not provided by the caller.

Explanation: The caller did not provide a key alias.

System action: The request is halted.

Administrator response: Ensure that a key alias is provided.

FBTLIB119E The attempt to encrypt or decrypt a message was unsuccessful: *Error message*.

Explanation: The protocol message could not be signed. This error could be caused by a keystore configuration error or expired certificates.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTLIB200E The protocol action caught an unexpected exception while building a Liberty assertion.

Explanation: The protocol action caught an unexpected exception from outside of Liberty while building a Liberty assertion.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB201E The protocol action cannot retrieve the SAML status from the Liberty context.

Explanation: No SAML_STATUS attribute was found in the Liberty context. This attribute is typically set by a previous protocol action.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB202E The protocol action cannot find a request ID in the request object.

Explanation: No RequestID attribute was found in the request message being processed. This attribute is required.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB203E The protocol action cannot determine the current provider identifier.

Explanation: The configuration did not return an identifier for the current provider.

Administrator response: Verify that configuration files are present and have not been corrupted. If the files appear good, enable a trace for detailed messages about the error.

FBTLIB204E No federation exists for this principal.

Explanation: Single sign-on is not possible for this principal because the account cannot be federated. The following conditions can prevent account federation: the user does not consent to federation when queried, the authentication request Federate element is set to false, the authentication request IsPassive element is set to true and the user cannot be queried for consent.

Administrator response: Verify that the authentication request provides proper values for the Federate and IsPassive elements, and that the user answers affirmatively if queried for consent to federate. In addition, enable a trace for detailed messages about the error.

FBTLIB205E The protocol action caught an unexpected exception while determining consent to federate.

Explanation: The protocol action caught an unexpected exception outside of Liberty while determining if the user consents to account federation.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB206E The protocol action cannot determine the identity of a locally authenticated user.

Explanation: No local user information was available in the Liberty context. This information is typically set by a previous protocol action by querying the local execution environment for user identity and credentials.

User response: Verify that the user has logged on successfully.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB207E The protocol action cannot determine the value of the name identifier provided by the identity provider.

Explanation: No IDP_NAME_ID attribute was found in the Liberty context. This value is typically set by a previous protocol action.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB208E The protocol action caught an unexpected exception while federating the principal.

Explanation: The protocol action caught an unexpected exception outside of Liberty while attempting to federate the principal.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB209E The protocol action caught an unexpected exception while executing ForceAuthn logic.

Explanation: The protocol action caught an unexpected exception outside of Liberty while executing ForceAuthn logic.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB210E The protocol action cannot obtain a local token from the Liberty context.

Explanation: Local authentication is not possible because the protocol action requires a LOCAL_TOKEN attribute in the Liberty context. This attribute is typically set by a previous protocol action.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB211E The protocol action caught an unexpected exception while attempting to set the user's local credentials.

Explanation: The protocol action caught an unexpected exception outside of Liberty while attempting to set the user's local credentials.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB212E SAML error in response: *SamlStatus***.**

Explanation: The response message contains a SAML error indicating that the request was not successful.

Administrator response: Enable a trace on the message provider for information about why the error was returned.

FBTLIB213E No Liberty assertion was returned in the authentication response message.

Explanation: The identity provider did not return any Liberty assertions in the authentication response. Single sign-on failed.

Administrator response: Enable a trace on the identity provider for information about why no Liberty assertions were included in the authentication response.

FBTLIB214E No RelayState element was found in the authentication response.

Explanation: The authentication response message did not contain a RelayState element, which is required for single sign-on. The RelayState should have been provided in the original authentication request.

Administrator response: Enable a trace on both the service provider and identity provider for more information. On the service provider, verify that the original authentication request contains the appropriate RelayState element.

FBTLIB215E No request with identifier *InResponseTo* **was found. The response is ignored.**

Explanation: The response message contained an InResponseTo attribute whose value did not correspond to any request identifiers in the current session.

Administrator response: Enable a trace on both the service provider and identity provider for more information. On the service provider, verify that the original request contains a RequestID attribute. On the identity provider, verify that the response references that same value in the InResponseTo attribute.

FBTLIB216E The protocol action caught an unexpected exception while processing the Liberty message.

Explanation: The protocol action caught an unexpected exception outside of Liberty while processing the Liberty message.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB217E The Liberty assertion could not be exchanged for a local credential.

Explanation: The protocol action caught an unexpected exception from the token exchange service while exchanging a Liberty assertion for a local credential.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB218E The protocol action caught an unexpected exception while querying the user who wants to federate his identity.

Explanation: The protocol action caught an unexpected exception outside of Liberty while querying the user who wants to federate his identity.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB219E The protocol action caught an unexpected exception while querying the execution environment for the user's current federation state.

Explanation: The protocol action caught an unexpected exception outside of Liberty while querying the execution environment for the user's current federation state.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB220E The protocol action caught an unexpected exception while querying the execution environment for the user's current login state.

Explanation: The protocol action caught an unexpected, non-Liberty exception while querying the execution environment for the user's current login state.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB221E A Liberty version mismatch occurred: runtime = *LibertyRuntimeMajorVersion*.*LibertyRuntimeMinorVersion*; **message =** *MessageMajorVersion*.*MessageMinorVersion*.

Explanation: The Liberty version of the message is not supported by the Liberty runtime.

Administrator response: Verify that the providers in this provider's circle of trust operate at a compatible level of the Liberty protocol.

FBTLIB222E The protocol action caught an unexpected exception while validating a Liberty message.

Explanation: The protocol action caught an unexpected exception outside of Liberty while validating a Liberty message.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB223E The identity provider (*IdentityProvider***) does not have a configured federation with the requesting service provider (***ServiceProvider***).**

Explanation: There are no configured federations that include the service provider who issued the request.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, establish a partnership with the service provider in question.

FBTLIB224E The user has no local credentials.

Explanation: The protocol being executed by this action requires that the user is locally authenticated. No local credentials could be found; therefore, the protocol cannot be completed.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB225E The protocol action caught an unexpected exception while verifying that the user has local credentials.

Explanation: The protocol action caught an unexpected exception outside of Liberty while verifying that the user has local credentials.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB226E The protocol action caught an unexpected exception while building a Liberty request or response message.

Explanation: The protocol action caught an unexpected exception outside of Liberty while building a Liberty request or response message.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB227E No destination URL was found in the Liberty context.

Explanation: The protocol action cannot find the APPLIES_TO_URL attribute in the Liberty context. This attribute is typically set by a previous action that sets it to the value of a service provider's AssertionConsumerServiceURL.

Administrator response: Verify that configuration files are present and have not been corrupted. Enable a trace for detailed messages about the error.

FBTLIB228E The local credential could not be exchanged for a Liberty assertion.

Explanation: The protocol action caught an unexpected exception from the token exchange service while exchanging a local credential for a Liberty assertion.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB229E The identity provider is passive and cannot authenticate the user.

Explanation: The identity provider must interact with the user for local authentication, but it cannot because the authentication request's IsPassive element is set to 'true'.

Administrator response: Retry the authentication request with the IsPassive element set to 'false'.

FBTLIB230E The ForceAuthn element is not supported.

Explanation: Forced authentication is not supported in this release, and the authentication request's ForceAuthn element is set to 'true'.

Administrator response: Retry the authentication request with the ForceAuthn element set to 'false'.

FBTLIB231E The ReauthenticateOnOrAfter attribute is not supported.

Explanation: Reauthentication requirements specified in the Liberty assertion is not supported in this release. Therefore, the assertion cannot be used for single sign-on.

Administrator response: Retry the authentication request, sending it to an identity provider that does not specify a reauthentication time.

FBTLIB232E The provider identifier cannot be retrieved from configuration.

Explanation: Configuration did not return a value for the provider identifier.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, add the needed configuration data.

FBTLIB233E The protocol profile could not be retrieved from the Liberty context.

Explanation: The Liberty context did not contain a LIB_PROTOCOL_PROFILE attribute. This attribute is typically set by the delegate protocol.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB234E The protocol action caught an unexpected exception while generating claims for the token exchange between a local credential and a Liberty assertion.

Explanation: The protocol action caught an unexpected exception outside of Liberty while generating a LibertyClaims object for the token exchange.

Administrator response: Enable trace for detailed messages about the error.

FBTLIB235E No provider identifier was found in the Liberty message.

Explanation: The protocol action could not find a provider identifier in the message being processed.

Administrator response: Enable a trace for detailed messages about the error, including format of the message in question.

FBTLIB236E No identity service was found.

Explanation: No identity service was found.

Administrator response: Check the identity service configuration. Enable a trace for detailed messages about the error.

FBTLIB237E No token request information was found.

Explanation: Token exchange requires Issuer information, AppliesTo information, or both. Neither Issuer information nor AppliesTo information could be found.

Administrator response: If the error is seen on an identity provider, check the configuration and make sure that the self-provider is configured properly; this configuration is needed to determine the Issuer information. Enable a trace for detailed messages about the error, including the contents of the message, which should contain the ProviderID. The ProviderID is needed to determine the AppliesTo information. If the error is seen on a service provider, enable a trace for detailed messages about the error; Issuer information is determined from information in the Liberty assertion, and AppliesTo information is determined from the RelayState in the original authentication request.

FBTLIB238E No alias was found for user *User* and provider *PartnerProvider*.

Explanation: There was no alias found for the currently authenticated user for the specified partner provider.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB239E The timestamp (IssueInstant attribute) in a received Liberty request or response was out of range.

Explanation: Validation failed for a received Liberty message because the timestamp in the message did not fall within a configured range from the current system's time.

Administrator response: Synchronize the clocks of the sending and receiving machines, if possible. Also check that the configured time skew tolerance is acceptable.

FBTLIB240E The protocol action caught an unexpected exception while executing a local logout.

Explanation: The protocol action caught an unexpected exception outside of Liberty while executing a local logout.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB241E The local logout operation failed.

Explanation: The local logout operation failed.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB242E The protocol action could not build a list of service providers that were sent Liberty assertions on this session.

Explanation: The protocol action could not build a list of service providers that were sent Liberty assertions on this session.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB243E The response does not correlate to the current request.

Explanation: Validation failed for a Liberty or SAML response because the InResponseTo attribute in a received Liberty response did not match the current request identifier.

Administrator response: Enable a trace on both the responding and requesting machines for detailed messages about the error.

FBTLIB244E The service provider (*ServiceProvider*) does not have a configured federation with the responding identity provider (*IdentityProvider*).

Explanation: No configured federations include the identity provider that issued the response.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, establish a partnership with the identity provider in question.

FBTLIB245E The service provider (*ServiceProvider*) making the logout request was not issued an assertion by this session in the identity provider.

Explanation: The identity provider session information does not indicate that this service provider has been issued an assertion. Therefore, the service provider cannot initiate a logout request.

Administrator response: This error might mean that the identity provider has received an inappropriate logout message. Examine the configuration and enable a trace to investigate which service providers can request authentication and which actually have requested authentication.

FBTLIB246E The provider (*ServiceOrIdentityProvider*) does not have a required endpoint URL configured (*EndpointURL*).

Explanation: A required endpoint URL was not found in the configuration for the specified provider.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, define the required endpoint URL for the provider in question.

FBTLIB247E Bad SAML status.

Explanation: A previous protocol action set the SAML_STATUS Liberty attribute to a value other than

Success, indicating that subsequent actions should not execute.

Administrator response: Enable a trace to determine which action set the SAML_STATUS value, and why the value is not samlp:Success.

FBTLIB248E No LogoutRequest was found for the responding service provider (*ServiceProvider*).

Explanation: A LogoutResponse was received from a service provider and no corresponding LogoutRequest could be found. The LogoutResponse is ignored.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB249E No audience entry was found for self-service provider (*ServiceProvider*).

Explanation: The Liberty assertion did not contain an audience entry for the current self-provider. The assertion is ignored.

Administrator response: Enable trace for detailed messages on the issuing identity provider to determine why the self-provider was not included in the assertion audience.

FBTLIB250E The protocol action caught an unexpected exception while validating a Liberty assertion.

Explanation: The protocol action caught an unexpected exception outside of Liberty while validating a Liberty assertion.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB251E The Liberty assertion failed validation.

Explanation: The Liberty assertion did not pass validation checks of the ReauthenticationOnOrAfter attribute, the InResponseTo attribute, or the AudienceRestrictionCondition element.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB252E Required data could not be found from configuration.

Explanation: A required data item was not found in the provider's configuration, so the operation cannot be performed.

Administrator response: Enable a trace for detailed messages about the error, including which data item could not be found. Then verify that the provider's configuration files are not incorrect or unreadable and that they contain the proper data.

FBTLIB253E Required data could not be found in a Liberty request or response message.

Explanation: A required data item was not found in a Liberty request or response message, so the operation cannot be performed.

Administrator response: Enable a trace for detailed messages about the error, including which data item could not be found. Note that trace might need to be enabled on the provider of the Liberty message as well to determine why the message lacks the required data.

FBTLIB254E Required data could not be found in the Liberty context.

Explanation: A required data item was not found in the Liberty context, so the operation cannot be performed.

Administrator response: Enable a trace for detailed messages about the error, including which data item could not be found.

FBTLIB255E The issuer of the Liberty assertion (*AssertionIsuer*) did not match the issuer of the Liberty artifact (*ArtifactIssuer*).

Explanation: The Liberty assertion's issuer did not match the Liberty artifact's issuer. The assertion is ignored.

Administrator response: Enable a trace for detailed messages about the error. Verify that the configuration maps the succinct ID in the artifact to the correct provider.

FBTLIB256E The Liberty Service implementation class (*ClassName*) is not valid.

Explanation: The Liberty Service implementation parameter is not valid.

Administrator response: Update the configuration. Ensure that the implementation class is a fully qualified Java class.

FBTLIB257E The Liberty Service failed to validate the configuration.

Explanation: The Liberty Service failed to validate the configuration information.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB258E The Liberty Service Factory failed to instantiate the service with the implementation class (*ClassName*).

Explanation: The Liberty Service Factory failed to instantiate the service implementation class.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB259E No assertion or status information was found for artifact (*LibertyArtifact*).

Explanation: No information related to the specified artifact could be found.

Administrator response: Verify that the artifact is specified properly and that it has been used within the allowed assertion store timeout.

FBTLIB260E The Liberty module failed to retrieve the service factory for the specified service key (*Service Key*).

Explanation: The Liberty module failed to retrieve the service factory.

Administrator response: Enable trace for detailed messages about the error. Verify that the configuration has the correct entry for the service factory and retry the operation.

FBTLIB261E The Liberty module failed to retrieve a service instance using the service factory. (*ServiceFactory*).

Explanation: The Liberty module failed to retrieve a service instance.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB262E The succinct ID in the artifact does not correspond to a configured provider.

Explanation: No provider was mapped to the succinct ID in the artifact. The artifact is ignored.

Administrator response: Enable a trace for detailed messages about the error, including which succinct ID is in the artifact. Verify that configuration has correct mappings for providers and their succinct IDs.

FBTLIB263E The provider referenced by the succinct ID in the Liberty artifact (*ArtifactSuucinctIDProvider*) did not match the current provider (*SelfProvider*).

Explanation: The provider mapped to the succinct ID in the Liberty artifact did not match the current identity provider. The assertion request is ignored.

Administrator response: Enable a trace for detailed messages about the error. Verify that the configuration has the correct mappings for providers and their succinct IDs.

FBTLIB264E The protocol action caught an unexpected exception while validating a Liberty artifact.

Explanation: The protocol action caught an unexpected exception outside of Liberty while validating a Liberty artifact.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB265E The protocol action caught an unexpected exception while building a Liberty artifact.

Explanation: The protocol action caught an unexpected exception outside of Liberty while building a Liberty artifact.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB266E The Liberty module caught an unexpected exception while serializing an object.

Explanation: The Liberty module caught an unexpected exception while serializing an object.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB267E The Liberty module caught an unexpected exception while deserializing an object.

Explanation: The Liberty module caught an unexpected exception while deserializing an object.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB268E The Liberty LogoutRequest could not be found.

Explanation: The Liberty LogoutRequest object, which is required to complete the operation, could not be found. If the operation was being performed on a service provider, the LogoutRequest should be in the Liberty context. If the operation was being performed on an identity provider, the LogoutRequest should be in the Liberty session.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB269E The Protected Resource URL value could not be found in the Liberty Context object.

Explanation: The Protected Resource URL value, which is required to complete the operation, could not be found in the Liberty Context object.

Administrator response: Verify that the point of contact at the service provider is configured properly.

FBTLIB270E The requested provider *provider* **does not exist.**

Explanation: The provider ID, which is required to initiate federation termination, could not be found.

Administrator response: Verify that the provider ID is correct and that the configuration specifies that provider ID.

FBTLIB271E The profile specified for termination *profile* **is not valid.**

Explanation: The profile specified is not present or supported.

Administrator response: Verify that the profile URI is correct and that the configuration specifies that provider URI.

FBTLIB272E The federation termination service URL specified for termination *url* **is not valid.**

Explanation: The URL specified is not present or supported.

Administrator response: Verify that the URL is correct and that the configuration specifies that provider URL.

FBTLIB273E The federation termination service SOAP endpoint specified for termination *endpoint* **is not valid.**

Explanation: The URL specified is not present or supported.

Administrator response: Verify that the URL is correct and that the configuration specifies that provider URL.

FBTLIB274E The federation termination service is missing a notification message.

Explanation: The notification message specified is not present or supported.

Administrator response: Verify that the message is correct and that the configuration specifies the provider URL and correct notification profile.

FBTLIB275E The federation partner's service return URL, *endpoint* **is missing or not valid.**

Explanation: The termination service return URL specified is not present or supported.

Administrator response: Verify that the message is correct and that the configuration specifies the provider URL and service return URL.

FBTLIB276E A response to an unsolicited federation termination was received.

Explanation: A request was received as a response to an unsolicited federation termination. This request will be ignored but could be due to the requestor not having cookies enabled. The configuration can override this default behavior.

Administrator response: Verify that the message is correct and that the configuration specifies the provider URL and service return URL.

FBTLIB277E The ID service request to remove an alias for *userId* **and provider** *providerId* **failed.**

Explanation: The ID service operation was not successful.

Administrator response: Validate that the identity and provider are valid and check the log for messages returned from the ID service.

FBTLIB279E The user's response to the consent to federate was not found in the browser query string.

Explanation: Internal Error: The Delegate protocol is unable to process the response because it could not retrieve the AuthnRequest from LibertyContext.

System action: The operation will be halted.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB280E The register name identifier could not be performed. The user *user* **does not have a required name identifier configured for provider** *provider***.**

Explanation: For a register name identifier request to be created, it is a requirement that the user has a name identifier for the partner.

Administrator response: Validate that the given user has a name identifier configured.

FBTLIB281E The register name identifier request failed. The provider *provider* **did not provide a name identifier in the register name identifier request.**

Explanation: A name identifier is required in a register name identifier request.

Administrator response: Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB282E The register name identifier could not be performed. The provider *provider* did not provide an old name identifier in the register name identifier request.

Explanation: A old name identifier is required in a register name identifier request.

Administrator response: Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB283E Register name identifier request failed. The provider *provider* provided the old name identifier *old identifier* but the expected one was *expected old identifier*.

Explanation: The provided old name identifier did not match the current name identifier. The register name identifier request failed.

Administrator response: Validate that the given provider is correctly formatting its register name identifier requests.

FBTLIB284E The register name identifier could not be performed. The provider *provider* does not have the required register name identifier endpoint configured.

Explanation: The given provider does not have the required register name identifier endpoint configured.

Administrator response: Validate that the given provider has a register name identifier endpoint configured.

FBTLIB285E The register name identifier request for *userid* could not complete because the identity service was unavailable.

Explanation: The identity service was not available to complete the register name identifier request.

Administrator response: Validate that the identity service is configured into the environment and is functioning correctly.

FBTLIB286E The register name identifier request for *userid* could not complete because an error was encountered during the modification of the alias in the registry.

Explanation: The identity service was not able to make the alias modification in the registry.

Administrator response: Check a trace log for a more specific error that will indicate what caused the problem.

FBTLIB287E No register name identifier response message was given.

Explanation: The partner did not respond with a register name identifier message.

Administrator response: Ensure that the partner responds with correctly formatted messages.

FBTLIB288E No provider identifier was given in the register name identifier response.

Explanation: The provider did not respond with a provider identifier.

Administrator response: Ensure that the provider responds with correctly formatted messages.

FBTLIB289E The provider *provider* did not include a status in the register name identifier response.

Explanation: The provider given did not include a status or a correctly formatted status in its response.

Administrator response: Ensure that the provider responds with correctly formatted messages.

FBTLIB290E No register name identifier request found in the session.

Explanation: When the provider returns a response, the original request is needed to complete the transaction.

Administrator response: Ensure that the browser has cookies enabled.

FBTLIB291E The protocol action caught an unexpected exception while executing a local login.

Explanation: The protocol action caught an unexpected exception outside of Liberty while executing a local login.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB292E The name identifier provided for federation termination, *identifier*, is not valid.

Explanation: The requestor sent a name identifier that was not valid for the principal.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB293E A federation termination notification that was not valid was received.

Explanation: An attempt to decode the federation termination notification failed either because of schema violation or a signature failure.

Administrator response: Check a trace log for the message and ensure that it is correctly formatted, and validate the configured keys for the partner sending the notification.

FBTLIB294E The federation termination notification could not be created because '*schemaMessage*'. The federation termination has not been performed.

Explanation: An attempt to encode the federation termination notification failed either because of schema violation or a signature failure.

Administrator response: Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB295E The register name identifier provided is not valid or could not be understood, because [*reason*]. The register name identifier has not been performed.

Explanation: An attempt to encode the register name identifier failed either because of a schema violation or a signature failure.

Administrator response: Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB296E There was no register name identifier request provided. The register name identifier has not been performed.

Explanation: There was no register name identifier request provided.

Administrator response: Ensure that the provider making the register name identifier request provides a request message.

FBTLIB297E The register name identifier message could not be created because [*schemaMessage*]. The federation termination has not been performed.

Explanation: No register name identifier request was created because an error occurred.

Administrator response: Check a trace log for the message and ensure that it is correctly formatted, and validate the configured private key aliases.

FBTLIB300E The identity service could not set the self or partner alias for user *user* and partner provider *provider*.

Explanation: The identity service encountered an error while storing alias data for the current local user.

Administrator response: Validate that the identity service is configured into the environment and is functioning correctly.

FBTLIB301E A Liberty message was not included in the request to the SOAP endpoint.

Explanation: The message that was received by the SOAP endpoint did not include a Liberty message as a child of the SOAP body.

Administrator response: Validate that the partner that is sending messages to the SOAP endpoint is sending correctly formatted Liberty requests.

FBTLIB304E The Delegate protocol is unable to obtain the AuthenticationURL endpoint.

Explanation: A required endpoint URL was not found in the configuration for the specified provider.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, define the required endpoint URL for the provider in question.

FBTLIB305E The name identifier to be used to determine the local user cannot be obtained from Liberty context.

Explanation: The name identifier that comes in the request is needed to determine the local identity of user. It might not have come in the request.

Administrator response: Turn on the provider tracing to check if the incoming request had name identifiers set.

FBTLIB306E The protocol action caught an unexpected exception while attempting to get the user's local credentials.

Explanation: The protocol action caught an unexpected exception outside of Liberty while attempting to get the user's local credentials.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB307E The protocol action caught an unexpected exception while executing.

Explanation: The protocol action caught an unexpected exception outside Liberty while executing.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB308E The Liberty plug-in caught an unexpected exception when building the SOAP message.

Explanation: The Liberty plug-in caught an unexpected exception when building the SOAP message.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB309E The received message failed signature verification. The message was not signed by a trusted signer or was modified after signing.

Explanation: The received message was signed but signature verification failed.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate configuration.

FBTLIB310E The configured Liberty version is valid for the federation *federationId* with display name *federationName*.

Explanation: The Liberty version of the message is not supported by the Liberty runtime.

Administrator response: Verify that the providers in this provider's circle of trust operate at a compatible level of the Liberty protocol.

FBTLIB311E The provider *provider* does not have an AssertionConsumerServiceURL endpoint configured with an ID of *id*.

Explanation: The configuration does not contain an AssertionConsumerServiceURL endpoint with the given identifier for the given provider.

System action: The request has been halted.

Administrator response: Ensure that the configuration is correct.

FBTLIB312E The user *user* has authenticated with a one-time name identifier and cannot execute a register name identifier action.

Explanation: The user was issued a one-time name identifier during authentication. Register name identifier actions can be executed only when a user has been issued federated name identifiers.

System action: The request has been halted.

Administrator response: No action is required.

FBTLIB313E The user *user* has authenticated with a one-time name identifier and cannot execute a defederation action.

Explanation: The user was issued a one-time name identifier during authentication. Federation termination actions can be executed only when a user has been issued federated name identifiers.

System action: The request has been halted.

Administrator response: No action is required.

FBTLIB314E The user was not authenticated because a pre-existing logout request was found.

Explanation: The user was not authenticated because a pre-existing logout request was detected. This can happen if a user logs in but logs out of another federated site, and the logout message arrives before the authentication credentials.

System action: The request has been halted.

Administrator response: The user should log in again.

FBTLIB315E No authentication request was found in the session.

Explanation: When a user authenticates, the authentication request message is stored and used to validate the corresponding response message. A response message was received, but there was not a request message, and so the unsolicited response is rejected.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages.

FBTLIB316E The calculated proxy count value, *count*, is invalid.

Explanation: The calculated proxy count value must be at least one less than the original proxy count value. A pluggable proxy service has returned an invalid value. This limitation is specified by the Liberty Architecture.

System action: The request has been halted.

Administrator response: Install and configure a proxy service that will return a valid proxy count value, such as the default proxy service plug-in that is delivered with the product.

FBTLIB317E The user cannot be authenticated directly or by proxy.

Explanation: The incoming authentication request forbids proxying of the request, and the identity provider cannot authenticate the user directly.

System action: The request has been halted.

Administrator response: The request should be retried permitting proxying, if possible. Otherwise, the request should be directed to another identity provider that is configured to authenticate users directly.

FBTLIB318E No identity provider was found in configuration.

Explanation: No identity provider was configured as a partner to this provider.

System action: The request has been halted.

Administrator response: Verify that configuration files are present and have not been corrupted. If necessary, define one or more identity provider partners for this provider.

FBTLIB319E The liberty version specified in the federation group configuration '*groupId*', self entity '*entity*' is invalid. Specify the correct values in the '*majorVersionProperty*' and '*minorVersionProperty*' properties. Current values MajorVersion: '*minorVersion*' MinorVersion: '*minorVersion*'

Explanation: An invalid liberty version is specified in the configuration.

System action: The liberty module could not be initialized.

Administrator response: Specify a valid liberty version in the configuration.

FBTLIB320E The federation group type specified in the configuration is not supported. Group id: '*id*', Group display name: '*id*', federation group type '*type*'.

Explanation: The federation group defined is not a supported type.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a supported group type in the configuration.

FBTLIB321E The *partnerEndpointType* endpoint for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. Endpoint value '*displayName*'.

Explanation: The specified partner endpoint is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTLIB322E The *partnerEndpointType* endpoint for self '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. Endpoint value '*displayName*'.

Explanation: The specified self endpoint is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTLIB323E The *partnerEndpointType* endpoint is missing from the provider '*id*' and display name '*displayName*' configuration for federation group with ID '*id*' and display name '*displayName*'.

Explanation: A required endpoint is missing from the provider's configuration.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify the required endpoint in the provider's configuration.

FBTLIB324E The *propertyName* property is missing from the provider '*id*' and display name '*displayName*' configuration for federation group with ID '*id*' and display name '*displayName*'.

Explanation: A required property is missing from the provider's configuration.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify the required property in the provider's configuration.

FBTLIB325E The protocol profile value '*protocolProfileValue*' for protocol type '*protocolProfile*' specified for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid.

Explanation: The specified protocol profile value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid protocol profile value in the configuration.

FBTLIB326E The property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid.

Explanation: The specified property value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid property value in the configuration.

FBTLIB327E The boolean property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. For boolean properties the permitted values are 'true' or 'false'.

Explanation: The specified boolean property value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid boolean property value in the configuration.

FBTLIB328E The numeric property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. The minimum value for this property is '*displayName*'.

Explanation: The specified numeric property value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid numeric property value in the configuration.

FBTLIB329E The Identity provider succinct id value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. The identity provider succinct ID is a required property.

Explanation: The specified numeric property value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTLIB330E The common domain service host value '*commonDomainServiceHost*' specified using property '*propertyName*' for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is invalid. The common domain service host must start with http:// or https:// and end with the common domain value '*displayName*'.

Explanation: The specified common domain service host is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid common domain service host in the configuration.

FBTLIB331E The Identity provider succinct ID value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' does not match the message digest of the provider ID.

Explanation: The specified identity provider succinct ID value is invalid.

System action: The Liberty Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTLIB332E The proxy list is invalid.

Explanation: The proxy list used in a proxy authentication request must adhere to the Liberty specifications. A pluggable proxy service has returned an invalid proxy list.

System action: The request has been halted.

Administrator response: Install and configure a proxy service that will return a valid proxy list, such as the default proxy service plug-in that is delivered with the product.

FBTLIB333E The '*propertyValue*' property is missing from the partner with provider ID '*providerId*' configuration.

Explanation: The specified property is missing from the partner configuration.

System action: The SOAP client could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Include the missing property in the partner configuration.

FBTLIB334E The authentication request contained a RequestAuthnContext element which is not supported by this identity provider.

Explanation: This version of the product does not support RequestAuthnContext elements in authentication requests. Any request containing a RequestAuthnContext cannot be processed.

System action: The request has been halted.

Administrator response: No action is necessary on the identity provider. If possible, configure the service provider to issue authentication requests that do not include a RequestAuthnContext element.

FBTLIB335E Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP POST.

Explanation: Internal Error: The delegate protocol cannot retrieve the AuthnRequest from incoming HTTP POST.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB336E Internal Error: The Delegate protocol is unable to process the request because it could not convert the liberty request to an XML string.

Explanation: Internal Error: The Delegate protocol is unable to process the request because it could not convert the liberty request to an XML string.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB337E Internal Error: The Delegate protocol is unable to convert the request from an XML string to BASE64 encoded data.

Explanation: Internal Error: The Delegate protocol is unable to convert the request from an XML string to BASE64 encoded data.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB338E Internal Error: The Delegate protocol is unable to convert the request from BASE64 encoded data to an XML string.

Explanation: Internal Error: The Delegate protocol is unable to convert the request from BASE64 encoded data to an XML string.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB339E Internal Error: The Delegate protocol is unable to process the request because it couldn't parse the liberty request XML string.

Explanation: Internal Error: The Delegate protocol is unable to process the request because it couldn't parse the liberty request XML string.

System action: Contact your IBM support representative.

Administrator response: Enable a trace for detailed messages about the error.

FBTLIB340E The maximum amount of authentication attempts *authenticationAttempts* has been reached. Please verify that the Access Control Lists are specified correctly. The *authenticationURL* URL needs to be a protected endpoint.

Explanation: The user has exhausted the amount of attempts to authenticate.

System action: Verify the point of contact configuration.

Administrator response: Verify that the Access Control Lists are specified correctly.

FBTLOG001E The logging configuration file was not found.

Explanation: The system could not find the file containing the logging configuration data.

System action: The system will revert to default settings.

Administrator response: Ensure that the configuration file exists and is in the classpath of the application.

FBTLOG002W An integer was expected.

Explanation: The system expected an argument of integer type.

System action: The system will revert to a hardcoded value (5000).

Administrator response: Ensure that the argument is the correct type.

FBTLOG003W An EventLevel was expected.

Explanation: The system expected one of the following: DEBUG_MIN, DEBUG_MID, DEBUG_MAX.

System action: The system will revert to DEBUG_MIN.

Administrator response: Ensure that the argument is valid.

FBTLOG004W An EventType was expected.

Explanation: The system expected one of the following: INFO_TYPE, WARN_TYPE, ERROR_TYPE, ALL_MSG_TYPE, TRACE_TYPE, AUDIT_TYPE.

System action: The system will revert to ALL_MSG_TYPE.

Administrator response: Ensure that the argument is valid.

FBTLOG005E An error occurred while saving the configuration.

Explanation: The system could not write the configuration file.

System action: The configuration will not be saved.

Administrator response: Ensure that the configuration file is in the correct location and is writable.

FBTLOG006E An error occurred during the loading of the logging configuration.

Explanation: The system could not read from the file containing the logging configuration data.

System action: The system will revert to default settings.

Administrator response: Ensure that the configuration file exists and is in the classpath of the application.

FBTLOG007E The management context was not valid. The changes could not be committed during this session.

Explanation: The management context was invalidated probably because a commit occurred elsewhere.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG008E An exception was received during the commit process. The changes could not be committed during this session.

Explanation: The management component caught an exception thrown while trying to commit the changes.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG009E An exception was received during a getMaxMsgFileSize operation.

Explanation: An exception was received during the retrieveMaxMsgFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG010E An exception was received during a retrieveMaxTraceFileSize operation.

Explanation: An exception was received during the retrieveMaxMsgFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG011E An exception was received during a retrieveMsgType operation.

Explanation: An exception was received during the retrieveMsgType operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG012E An exception was received during a retrieveTraceLevel operation.

Explanation: An exception was received during the retrieveTraceLevel operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG013E Required parameters were missing.

Explanation: A required parameter was missing from the argument map.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG014E An exception was received during a retrieveTracing operation.

Explanation: An exception was received during a retrieveTracing operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG015E An exception was received during a retrieveAuditLevel operation.

Explanation: An exception was received during a retrieveAuditLevel operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG016E An exception was received during a retrieveMaxAuditFileSize operation.

Explanation: An exception was received during the retrieveMaxAuditFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG017E An exception was received during a retrieveLogHomeDir operation.

Explanation: An exception was received during the retrieveLogHomeDir operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG018E An exception was retrieved during a retrieveProductName operation.

Explanation: An exception was received during the retrieveProductName operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG019E An exception was received during a retrieveTivoliCommonDir operation.

Explanation: An exception was received during the retrieveTivoliCommonDir operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG020E An exception was received during a modifyMaxMsgFileSize operation.

Explanation: An exception was received during the modifyMaxMsgFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG021E An exception was received during a modifyMaxTraceFileSize operation.

Explanation: An exception was received during the modifyMaxTraceFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG022E An exception was received during a modifyMsgType operation.

Explanation: An exception was received during the modifyMsgType operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG023E An exception was received during a modifyTraceLevel operation.

Explanation: An exception was received during the modifyTraceLevel operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG024E An exception was received during a modifyTracing operation.

Explanation: An exception was received during the modifyTracing operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG025E An exception was received during a modifyAuditLevel operation.

Explanation: An exception was received during the modifyAuditLevel operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG026E An exception was received during a modifyMaxAuditFileSize operation.

Explanation: An exception was received during the modifyMaxAuditFileSize operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG027E An exception was received during a modifyLogHomeDir operation.

Explanation: An exception was received during the modifyLogHomeDir operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG028E An exception was received during a modifyProductName operation.

Explanation: An exception was received during the modifyProductName operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG029E An exception was received during a modifyTivoliCommonDir operation.

Explanation: An exception was received during the modifyTivoliCommonDir operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG030E An exception was received during a retrieveComponentList operation.

Explanation: An exception was received during the retrieveComponentList operation.

System action: The system will revert back to the previous settings.

Administrator response: Create a new session and attempt the operation again.

FBTLOG037E The component identifier is null.

Explanation: The component identifier specified in a request to initialize logging is null.

System action: The logging initialization request is ignored.

Administrator response: This is an internal programming error. Report this problem and the invocation stack dump found in SystemErr.log to your IBM service representative.

FBTLOG038E Invalid class name provided for constructing a logger: *parameter*

Explanation: The class name provided for constructing a logger should be a full package-qualified class name beginning with com.tivoli.am.fim.

System action: The logger has not been created.

Administrator response: This is an internal programming error. Report this problem and the invocation stack dump found in SystemErr.log to your IBM service representative.

FBTMET001E The desired metadata element of type *descriptor* **was not found in the metadata file.**

Explanation: The metadata import operation failed because a proper descriptor was not found.

System action: The request has been halted.

Administrator response: Verify that the metadata file contains valid metadata and retry the operation.

FBTMOD001E The received request is missing the required parameter: *parameter*

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTMOD002E The element *localName* **is missing the required attribute** *attributeName*

Explanation: The current element is not valid because it does not contain required attributes.

System action: The parse operation will be halted.

Administrator response: Validate the module XML file.

FBTMOD003E Encountered unexpected element with URI *uri* **and local name** *elementName* **while parsing modules metadata file.**

Explanation: The current element is not valid in that location either because it is in the wrong place or is an unknown element.

System action: The parse operation will be halted.

Administrator response: Validate the module XML file.

FBTMOD004E The specified version string *version* **is in a format that could not be recognized.**

Explanation: The value for the version attribute is in an unrecognized format.

System action: The parse operation will be halted.

Administrator response: Validate the module XML file.

FBTMOD005E The plug-in and module initializer was unable to locate a directory where plug-ins are stored.

Explanation: The Federated Identity Manager application does not contain the directory containing modules and plug-ins.

System action: No plug-ins or modules can be used.

Administrator response: Validate the Federated Identity Manager configuration.

FBTOAU0010E The signature base string cannot be created from the request.

Explanation: The OAuth server is unable to create a base string from the HTTP request because the request message syntax is not valid.

System action: The request is rejected.

Administrator response: Verify that the syntax of the request message is a valid OAuth request message.

FBTOAU0011E The received signature does not match the calculated signature: Calculated signature: '*signature***' Signature received: '***signature***' Signature base string: '***string***'.**

Explanation: The signature on the received message does not match the signature calculated at the OAuth server.

System action: The request is rejected.

Administrator response: Compare the base string build in the OAuth server with the one used for signing in the request message. If the base strings are the same, check the client shared-secret that was used to sign the base string at the OAuth client and server.

FBTOAU0012E The client with identifier: '*client identifier***' sends the token: '***token***' to the OAuth server. However, the token is assigned to a different client with identifier: '***client identifier***'.**

Explanation: The token in the request is not mapped to the client identifier in the request.

System action: The authentication fails.

Administrator response: Validate the client identifier in the request message and compare it with the client identifier stored in the server. Ensure that the token is mapped to the correct OAuth client.

FBTOAU0013E OAuth token exchange between the SPS and STS failed in the '*type*' delegate.

Explanation: The SPS delegate is unable to receive an OAuth token from STS. Either the request sent to STS is not valid, or there is no STS chain to process the request.

System action: The token exchange stops.

Administrator response: Ensure that the request sent to STS is valid, and there is an STS chain to process the request.

FBTOAU0014E A duplicate OAuth parameter with the name: '*param*' has been found.

Explanation: There is a duplicate parameter in the request.

System action: The request is rejected.

Administrator response: Ensure that there are no duplicate parameters in the request message.

FBTOAU0015E The authenticated user name cannot be found in the OAuth request.

Explanation: The authenticated user name cannot be found because there is no proper Authentication service to handle the request.

System action: The authentication is rejected.

Administrator response: Ensure that the access control for the resource owner authorization endpoint is configured correctly.

FBTOAU0016E An STSUU token build failed due to an IOException.

Explanation: Unable to build an STSUU token from the request message because the request syntax is not a valid OAuth request.

System action: The STSUU build stops.

Administrator response: Verify that the content of the request sent from the browser is a valid OAuth request.

FBTOAU0017E The OAuth protocol parameter: '*param*' is found in the authorization header and in the HTTP entity-body or query parameter.

Explanation: OAuth parameter is found in two locations.

System action: The request is rejected.

Administrator response: Verify that the request sent from browser has a parameter that only exists in one location.

FBTOAU0018E The callback provided '*callback*' is not valid.

Explanation: The value callback URI in the request is not valid because it is not an absolute URI or 'oob'.

System action: The request is rejected.

Administrator response: Ensure that the callback is either specified to an absolute URI or 'oob'.

FBTOAU0019E The realm received in the request: '*realm*' does not match the realm that the token was created for: '*realm*'.

Explanation: The realm in the request does not match the one stored with the token in the request.

System action: The request is rejected.

Administrator response: Ensure that the realm is mapped to the token in the request message.

FBTOAU001E The OAuth client with identifier: '*client identifier*' cannot be found.

Explanation: The client identifier in the request does not match any registered client, or the client is disabled at the OAuth server.

System action: The request is rejected.

Administrator response: Ensure that the client is valid and is registered correctly.

FBTOAU0020E The authorize delegate received a consent-to-authorize page with a consent form verifier that is not valid.

Explanation: The consent form verifier sent to the Authorize delegate is not valid.

System action: The browser displays an error page and the operation stops.

Administrator response: Ensure that the consent form verifier in the request message and the one sent to the authorize delegate are valid.

FBTOAU0021E The parameter value for the parameter: '*param*' is not valid. The value found was: '*value*'.

Explanation: The value of the parameter is not valid.

System action: The operation stops.

Administrator response: Ensure that the parameter values in the request message has the correct type and format.

FBTOAU0022E The configuration value for the parameter: '*param*' is not valid. The value found was: '*value*'.

Explanation: The value of the configuration parameter is not valid.

System action: The operation stops.

Administrator response: Ensure the configuration parameter type is correct and the value is valid.

FBTOAU0023E An OAuth client with identifier: '*client identifier*' attempted to reuse the token: '*token*'.

Explanation: The client sent a token that has been used for a token exchange.

System action: The request is rejected.

Administrator response: Validate that the token in the request message has never been used before.

FBTOAU0024E An OAuth client with identifier: '*client identifier*' attempted to verify a token with the incorrect verification code: '*verification code*'.

Explanation: The verification code is not mapped to the client identifier in the OAuth server.

System action: The request is rejected.

Administrator response: Ensure that the verification code in the request message is valid and mapped to the client identifier in the OAuth server.

FBTOAU0025W The runtime cannot load the OAuth token cache with module ID: '*moduleID*'. The default module with ID: '*defaultModuleID*' loads instead.

Explanation: The runtime plug-in manager cannot load the module ID specified during configuration.

System action: A default token cache module loads instead.

Administrator response: Validate that the module ID configured for the OAuth token cache and plug-in which contains the specified module are deployed to the runtime.

FBTOAU0026E The configuration parameter: '*param*' for action: '*action*' is missing or contains an invalid value: '*value*'.

Explanation: The current request cannot be completed because the configuration is not valid.

System action: The request is halted.

Administrator response: Validate that the system is configured correctly.

FBTOAU0027E The runtime cannot load the OAuth trusted clients manager module with ID: '*moduleID*'. The default module with ID: '*defaultModuleID*' loads instead.

Explanation: The runtime plug-in manager cannot load the module ID specified during configuration.

System action: A default trusted clients manager module loads instead.

Administrator response: Validate that the module ID configured for the OAuth trusted clients manager and plug-in which contains the specified module are deployed to the runtime.

FBTOAU0029E The authorize delegate received consent form data that contained OAuth 1.0 parameters.

Explanation: The consent page form returned one or more OAuth 1.0 parameters such as oauth_callback or oauth_token.

System action: The browser displays an error page and the operation stops.

Administrator response: Ensure that the consent page form does not contain OAuth 1.0 parameters such as oauth_callback or oauth_token.

FBTOAU002E The OAuth token with lookup: '*token string*' and type: '*type*' cannot be found.

Explanation: The token for the given token type does not exist in the cache.

System action: The request is rejected.

Administrator response: Ensure that the token is valid and is mapped to the token type.

FBTOAU0030E The authorize delegate received a request that did not contain an oauth_token or a consent_form_verifier.

Explanation: The request to the authorize delegate did not contain an oauth_token parameter or a consent_form_verifier parameter.

System action: The browser displays an error page and the operation stops.

Administrator response: Ensure that requests to the authorize delegate contain either an oauth_token or a consent_form_verifier.

FBTOAU003E The OAuth token with lookup: '*token*' cannot be found.

Explanation: The token does not exist in the cache.

System action: The request is rejected.

Administrator response: Ensure that the token in the incoming message is valid.

FBTOAU004E Validation of the OAuth required parameters for token type: '*type*' failed. The following parameter was missing: '*param*'.

Explanation: The token validation failed because there is a missing parameter in the request message for the given token type.

System action: The request is rejected.

Administrator response: Verify that the request message has all the required parameters for the given token type.

FBTOAU005E Validation of the OAuth version parameter failed. The required version number is: '*version*', the supplied version number was: '*version*'.

Explanation: The validation failed because the version number in the request is not supported.

System action: The request is rejected.

Administrator response: Verify that the OAuth server supports the version number in the request message.

FBTOAU006E Timestamp validation failed because the timestamp is set in advance. Current timestamp: '*timestamp*' Supplied timestamp: '*timestamp*' Allowed clock skew: '*skew*' Allowed request lifetime: '*lifetime*'

Explanation: The timestamp validation failed because the timestamp in the request is set in advance.

System action: The request is rejected.

Administrator response: There are several reasons that an OAuth message timestamp might be set in the advance: the clocks on the client and the OAuth server are skewed beyond the acceptable tolerance or the acceptable tolerance for message timestamp is set too low. The administrator must check these points and make any necessary adjustments.

FBTOAU007E Timestamp validation failed due to an expired request. Current timestamp: '*timestamp*' Supplied timestamp: '*timestamp*' Allowed clock skew: '*skew*' Allowed request lifetime: '*lifetime*'

Explanation: The timestamp in the request has expired and is not valid.

System action: The request is rejected.

Administrator response: There are several reasons that a OAuth message timestamp might be expired: the clocks on the client and OAuth server are skewed beyond the acceptable tolerance, network delays are hampering message flow, or the acceptable tolerance for message timestamp is set too low. The administrator must check these points and make any necessary adjustments.

FBTOAU008E A nonce replay attack was detected with the nonce: '*nonce*'.

Explanation: A nonce replay attack happens when the same nonce exists in the cache.

System action: The request is rejected.

Administrator response: Ensure that signed messages sent to the OAuth server are only presented once.

FBTOAU009E The OAuth signature method '*method*' is not supported.

Explanation: The OAuth server does not support the signature method in the request.

System action: The request is rejected.

Administrator response: Ensure that the OAuth server supports the signature method in the request message.

FBTOAU028E The preferred client provider class: '*preferred_provider*' could not be loaded, falling back on the default client provider class: '*default_provider*'.

Explanation: The preferred client provider class could not be found.

System action: The default client provider class is used.

Administrator response: Check that the preferred client provider class is present.

FBTOAU201E The response type: [*response_type*] is not supported.

Explanation: The response_type parameter received in the request has an unsupported value.

System action: The request is rejected.

Administrator response: Ensure that the response_type parameter is one of the following: - code - token - a valid extension response type

FBTOAU202E The required parameter: [*name*] was not found in the request.

Explanation: A required parameter for this request type was not found in the received request

System action: The request is rejected.

Administrator response: Ensure that the request contains all of the required parameters.

FBTOAU203E The client with identifier: [*client_id*] could not be found.

Explanation: The client identifier in the request does not match any registered client.

System action: The request is rejected.

Administrator response: Ensure that the client is valid and is registered correctly.

FBTOAU204E An invalid secret was provided for the client with identifier: [*client_id*].

Explanation: The client secret in the request does not match the secret registered for this client.

System action: The request is rejected.

Administrator response: Ensure that the client secret is valid for this client.

FBTOAU205E The preferred client provider class: [*preferred_provider*] could not be loaded, falling back on the default client provider class: [*default_provider*].

Explanation: The preferred client provider class could not be found.

System action: The default client provider class is used.

Administrator response: Check that the preferred client provider class is present.

FBTOAU207E The browser request could not be converted into an STSUU because: [*message*].

Explanation: The process of converting an HTTP request to an STSUU failed.

System action: The request is rejected.

Administrator response: Ensure that the request has been properly constructed.

FBTOAU209E The token request with applies to: [*applies_to*] and issuer: [*issuer*] failed.

Explanation: The token exchange failed.

System action: The request is rejected.

Administrator response: Ensure that your OAuth 2.0 trust chains have been correctly configured.

FBTOAU210E The redirection URI provided in the request: [*redirect_uri*] is either invalid, or does not meet matching criteria against the registered redirection URI.

Explanation: An invalid redirection URI was provided.

System action: The request is rejected.

Administrator response: Ensure that you have provided the correct redirection URI.

FBTOAU211E The [*type*] received of type [*sub_type*] does not exist.

Explanation: An invalid grant/token was provided.

System action: The request is rejected.

Administrator response: Check that the grant/token being provided is valid.

FBTOAU214E The [*type*] received of type [*sub_type*] does not belong to the client attempting to use it.

Explanation: An invalid grant/token was provided.

System action: The request is rejected.

Administrator response: Check that the grant/token being provided is valid.

FBTOAU215E The grant type: [*grant_type*] is not supported.

Explanation: The grant_type parameter received in the request has an unsupported value.

System action: The request is rejected.

Administrator response: Ensure that the grant_type parameter is one of the following: - authorization_code - refresh_token - a valid extension grant type

FBTOAU216E The runtime could not load the OAuth 2.0 extension module with ID: [*moduleID*] for the extension point: [*extension*] . Instead the default module will be loaded with ID: [*defaultID*].

Explanation: The configuration specifies a module ID which could not be loaded by the runtime plugin manager.

System action: A default module will be loaded instead.

Administrator response: Validate that the plugin containing the specified module is deployed to the runtime.

FBTOAU217E You are not authorized to access this protected resource.

Explanation: This resource can only be access by an authorized user.

System action: The request is rejected.

Administrator response: Ensure that the authorization endpoint has been properly configured and secured.

FBTOAU218E The user denied consent to the protected resource.

Explanation: The user denied authorization to the OAuth 2.0 client.

System action: Inform the client of the decision.

Administrator response: None.

FBTOAU219E The scope requested in the access token request exceeds the scope granted by the resource owner.

Explanation: The client has requested an access token with greater scope then that granted.

System action: The request is rejected.

Administrator response: Ensure the client is not requesting too great a scope in it's token request.

FBTOAU220E The authenticated client id: [*username***] does not match the client id in the request body: [***client_id***].**

Explanation: The client's authenticated username does not match the client id it provided in the request body.

System action: The request is rejected.

Administrator response: Ensure that the authenticated username matches the client id.

FBTOAU222E The client's registered redirection URI is not a valid absolute URI.

Explanation: The client's configured redirection URI is invalid.

System action: The request is rejected.

Administrator response: Ensure that your client is configured correctly.

FBTOAU223E The received redirection URI: [*redirect_uri***] does not match the redirection URI that this grant was issued to.**

Explanation: The redirection URI in the request is no the same as the redirection URI used in the request for the authorization grant.

System action: The request is rejected.

Administrator response: Ensure the same redirection URI is used when requesting an authorization grant and using an authorization grant.

FBTOAU224E The runtime cannot load the OAuth 2.0 trusted clients manager module with ID: [*moduleID***]. The default module with ID: [***defaultModuleID***] loads instead.**

Explanation: The runtime plug-in manager cannot load the module ID specified during configuration.

System action: A default trusted clients manager module loads instead.

Administrator response: Validate that the module ID configured for the OAuth trusted clients manager and plug-in which contains the specified module are deployed to the runtime.

FBTOAU225E The authorization delegate received a consent page form verifier that was not valid compared to the verifier in the user's session.

Explanation: The consent page form verifier sent to the authorization delegate was not valid compared to the verifier contained in the user's session.

System action: The browser displays an error page and the operation stops.

Administrator response: Ensure that the consent page form verifier parameter submitted matches that set by the intial authorization delegate request.

FBTOAU226E The authorization delegate received consent form data that contained OAuth 2.0 parameters.

Explanation: The consent page form returned one or more OAuth 2.0 parameters such as client_id, redirect_uri, response_type or state.

System action: The browser displays an error page and the operation stops.

Administrator response: Ensure that the consent page form does not contain OAuth 2.0 parameters such as client_id, redirect_uri, response_type or state.

FBTOAU227E Multiple values of the OAuth 2.0 protocol parameter: [*request_parameter***] were found in the request.**

Explanation: OAuth 2.0 protocol parameters may not occur more then once in the request.

System action: The request is rejected.

Administrator response: Make sure that OAuth 2.0 request parameters do not occur more then once in the request.

FBTOAU228E The request included multiple client credentials.

Explanation: OAuth 2.0 protocol requests may not include multiple client credentials, for example client credentials in both the BA header and the request body.

System action: The request is rejected.

Administrator response: Make sure that OAuth 2.0 request did not include client credentials in more then one place, for example, in the BA header and the request body.

FBTOAU229E Confidential clients accessing the token endpoint must authenticate using their registered credentials.

Explanation: A confidential client attempted to access the token endpoint without authenticating.

System action: The request is rejected.

Administrator response: Ensure any confidential clients accessing the token endpoint present their client credentials.

FBTOAU230E The client credentials flow is restricted to confidential clients.

Explanation: A public client attempted to use the client credentials grant type, this grant type is restricted to confidential clients.

System action: The request is rejected.

Administrator response: Ensure public clients are not attempting to use the client credentials grant type.

FBTOAU231E The token endpoint is not configured to allow public client access.

Explanation: A public client attempted to access a token endpoint that has been configured to only allow confidential clients.

System action: The request is rejected.

Administrator response: If you wish to allow public clients to access the token endpoint, it must be configured on the federation page in the TFIM management console.

FBTOAU232E The client MUST use the HTTP POST method when making access token requests.

Explanation: A client attempted to make an access token request without using the HTTP POST method.

System action: The request is rejected.

Administrator response: Ensure that all requests to the OAuth 2.0 token endpoint use the HTTP POST method.

FBTOAU233E Maximum number of access token per user per client was reached

Explanation: There is limit on the number of access token distributed per user per client. You can set the limit in the API Protection definition.

System action: The request is rejected.

Administrator response: Increase the access token per user per client limit in the API Protection definition of the client.

FBTOAU234E Submitted PIN is wrong.

Explanation: PIN policy is enabled for the refresh token. PIN received in the request does not match.

System action: The request is rejected.

Administrator response: Prompt the user to enter the correct password.

FBTOAU235E The provided PIN does not match the PIN length setting in API Protection definition.

Explanation: The PIN length is different from the PIN length setting in API Protection definition.

System action: The request is rejected.

Administrator response: Submit a PIN with the correct length.

FBTOAU236E A PIN must be provided to protect the refresh token.

Explanation: PIN policy is enabled in the API Protection definition, but a PIN was not provided.

System action: The request is rejected.

Administrator response: Submit a PIN in the request.

FBTOAU237E The provided PIN contains invalid characters.

Explanation: A PIN should only contain numbers.

System action: The request is rejected.

Administrator response: Submit a PIN containing only numbers.

FBTOAU238E The API Protection definition is not attached to the requested resource.

Explanation: The API Protection definition should be attached to the resource.

System action: The request is rejected.

Administrator response: Attach the API Protection definition to the resource.

FBTOID0010E The openid.identity URL received from the identity provider: '*url1*' did not match the openid.identity URL sent to it: '*url2*'.

Explanation: The consumer sent a nonce to the identity provider during login, and this was not sent back to the consumer. This could indicate a replay attack.

System action: The request will be halted.

Administrator response: Please validate that the Identity Provider is not replaying messages and that it is using the correct return_to URL.

FBTOID0011E The required set of fields were not signed. The set of fields required to be signed is '*signatureRequired*'. The set of fields that were indicated as signed are '*signed*'.

Explanation: The consumer recieved a login response which did not contain a signature over the minimum set of required fields.

System action: The request will be rejected.

Administrator response: Please validate that the Identity Provider is sending a signature over at least the openid.identity and openid.return_to all the registry extension parameters.

FBTOID0012E The received message contained an invalid signature.

Explanation: The signature on the received message did not match the expected signature value.

System action: The request will be rejected.

Administrator response: Please validate that the sender of the message is generating the signature correctly.

FBTOID0013E The token exchange failed.

Explanation: The OpenID consumer was unable to exchange the login details for an authentication token at the trust service.

System action: The authentication will be rejected.

Administrator response: Please validate that the trust service is available and running, and all requirements of the trust chain have been met in the single-signon message from the identity provider.

FBTOID0014E The message was missing a required signed parameter: '*param*'

Explanation: The message has been rejected because a parameter which was required to be signed was not included in the response.

System action: The authentication will be rejected.

Administrator response: Please validate that the message contains all the required signed parameters.

FBTOID0015E The message contained an association handle: '*association*' which was not recognized.

Explanation: The message has been rejected because the association handle parameter was not known to the Identity Provider.

System action: The check_authentication will be rejected.

Administrator response: Please validate that the consumer is sending the correct association handle.

FBTOID0016E The message contained an association handle: '*association*' which was exposed to a consumer.

Explanation: The message has been rejected because the association handle parameter was previously exposed to a consumer during an associate operation.

System action: The check_authentication will be rejected.

Administrator response: Please validate that the consumer is sending the correct association handle.

FBTOID0017E The message for mode '*mode*' was sent with an invalid HTTP request method: '*method*'.

Explanation: The message has been rejected because the HTTP request method was not valid for the message being sent.

System action: The request will be rejected.

Administrator response: Please validate that the consumer is sending the message using the correct HTTP method.

FBTOID0018E The consumer requested an identity URL we could not validate: '*url*'.

Explanation: The message has been rejected because the claimed identity URL could not be validated by the identity provider.

System action: The request will be rejected.

Administrator response: Please validate that the consumer is sending the correct format of identity URL.

FBTOID0019E The user attempted to login at the Identity Provider however an OpenID has not yet been established.

Explanation: The authentication has been rejected because the OpenID identity provider is configured in alias mode, and no alias has yet been established for the user.

System action: The authentication will be rejected.

Administrator response: Please ensure the end user has established an OpenID alias before attempting login.

FBTOID001E While processing action: '*action*' the configuration parameter: '*param*' was determined to be missing or contain an invalid value: '*value*'.

Explanation: The current request could not be completed because the configuration is not valid.

System action: The request is halted.

Administrator response: Validate that the system is configured correctly.

FBTOID0020W The OpenID server has canceled the signon attempt.

Explanation: The authentication has been canceled by the OpenID Server.

System action: The authentication will be rejected.

Administrator response: Please ensure the end user has instructed the OpenID server to trust the consumer site.

FBTOID0021E The user session has been determined to be invalid while trying to retrieve the session variable: '*variable*'. This may have occured due to an incorrect transaction sequence, a session timeout, or a session replication or state management problem in a load-balanced environment.

Explanation: The user has either attempted a transaction in the wrong sequence, or the session has either timed out (e.g. user too slow to post a form) or in a clustered environment the user session may not have been replicated to all nodes in the cluster and failover (or incorrect stateful sessions) has occured.

System action: The operation will be halted.

Administrator response: Please ensure the end user has posted their form data in a timely fashion, and that in a clustered environment statefulness is maintained where possible between a browser and the TFIM server instance.

FBTOID0022E The token exchange failed.

Explanation: The OpenID identity provider was unable to exchange the current user credential for sign-in details at the trust service.

System action: The authentication will be rejected.

Administrator response: Please validate that the trust service is available and running, and all requirements of the trust chain have been met.

FBTOID0023E The OpenID server: '*server*' returned an error during the attempt to establish an association: '*errtext*'.

Explanation: The OpenID identity provider returned error text while attempting to establish an association.

System action: The authentication attempt will be halted.

Administrator response: Please validate that the OpenID server is available and able to process OpenID associate messages.

FBTOID0024E The OpenID server: '*server*' returned an error during the attempt to check the signature on a message: '*errtext*'.

Explanation: The OpenID identity provider was unable to check whether or not the message contained a valid signature, and returned error text.

System action: The authentication will be rejected.

Administrator response: Please validate that the consumer is sending correct parameters to the OpenID server, and that the OpenID server is functioning.

FBTOID0025E The OpenID consumer HTTP user agent was configured to deny access to a URL which the request attempted to access: '*url*'.

Explanation: The OpenID consumer received a request which caused it to attempt to contact an OpenID server or Identity URL at an address which the consumer has been configured to deny access to.

System action: The request will be rejected.

Administrator response: Please validate that the consumer user agent is configured correct, and that the client is not attempting malicious URL attacks at your consumer.

FBTOID0026E The provided network mask in the network declaration: '*url*' is invalid.

Explanation: The network mask it outside the permitted range for this type of network declaration.

System action: The operation will be halted.

Administrator response: Please validate that the configuration of permitted and denied network addresses for the user agent is correct.

FBTOID0027E The OpenID server: '*url*' cannot be contacted because the protocol it uses is not permitted in this federation's configuration.

Explanation: Use of this OpenID server has been denied because the protocol it uses is not permitted by the configuration of the federation.

System action: The operation will be halted.

Administrator response: Please validate that the configuration of the federation is correct, and that the OpenID server is using a matching protocol.

FBTOID0028W The runtime could not load the Trusted Sites Manager with module ID: '*moduleID*'. Instead the default module will be loaded with ID: '*defaultModuleID*'.

Explanation: The configuration specifies a module ID which could not be loaded by the runtime plugin manager.

System action: A default trusted sites manager module will loaded instead.

Administrator response: Please validate that module ID configured for the trusted sites manager and that the plugin containing the specified module is deployed to the runtime.

FBTOID0029E The relying party supplied a return_to URL: '*return_to*' that did not match the supplied realm URL: '*realm*'.

Explanation: If the relying party supplies both an openid.return_to and openid.realm, the return_to URL is requried to match the realm.

System action: The operation will be halted.

Administrator response: Please validate that the request parameters from the relying party are correct.

FBTOID002E While processing action: '*action*' the runtime parameter: '*param*' was determined to be missing or contain an invalid value: '*value*'.

Explanation: The current request could not be completed because the call to the delegate is not valid.

System action: The request will be halted.

Administrator response: Validate that the system has been called with the correct parameter value.

FBTOID0030W An association could not be established with OpenID Server '*moduleID*'. The transaction will continue with check_authentication signature validation. The error details are: *error*

Explanation: An associate request failed with the OpenID server.

System action: The signon will contine and check_authentication will be used for signature validation.

Administrator response: Please validate that OpenID server is functioning correctly as associations should be used for performance reasons.

FBTOID0031E While processing action: '*action*' the time skew with the server at endpoint: '*endpoint*' was not within the defined time skew: '*timeSkewSeconds*'.

Explanation: The current request could not be completed because the times did not match.

System action: The request will be halted.

Administrator response: Synchronize your server clock or increase the SPResponseNonceSkewTimeSeconds parameter for this federation. You can also set the parameter to -1 to disable skew checking.

FBTOID0032E While processing action: '*action*' the relying party detected a request containing an openid.response_nonce that has already been used: '*responseNonce*'.

Explanation: The current request could not be completed because of the replay.

System action: The request will be halted.

Administrator response: No administrator action is required. This could be a replay attack (which has been denied), however if no attack is suspected validate that the partner OP is not sending duplicate assertion responses.

FBTOID0033W An unexpected checkAuthentication was received. This could be due to a replay of the check_authentication request or the responseNonce '*responseNonce*' was not generated by this OpenID provider.

Explanation: The current request will return false because of the unexpected response_nonce in the check_authentication request.

System action: The check_authentication will return false.

Administrator response: No administrator resposne is required. If desired, the log file can be consulted to determine whether this was a replay or an invalid openid.response_nonce.

FBTOID0034E The identity provider '*identity_provider*' is not authorized to make claims about the identifier: '*claimed_identifier*'.

Explanation: The message has been rejected because during an OP identifier login the identity provider was not authorized to make claims about the returned claimed identifier.

System action: The request will be rejected.

Administrator response: Please verify that the identity provider is sending correct claimed identifiers or OP endpoints during OP identifier login.

FBTOID0035W The identity provider is skipping processing of unrecognized extension '*extension_uri*'.

Explanation: The message contains an OpenID extension that has not been implemented by this OpenID provider.

System action: The extension is skipped.

Administrator response: Please verify that OpenID relying-parties use extensions that this OP supports. Check that the XRDS advertised by this OP only includes supported extensions.

FBTOID0036E The identity provider is unable to process extension '*extension_uri*'.

Explanation: The message contains an OpenID extension that cannot be processed.

System action: The extension is skipped.

Administrator response: Check the extension parameters passed in the message.

FBTOID0037E An illegal extension alias has been detected: '*extension_alias*'.

Explanation: The message contains an OpenID extension that is not permitted by the specification.

System action: The message is rejected.

Administrator response: Ensure that the partner is sending valid extension parameters in the OpenID message.

FBTOID0038E An exception has occurred when trying to parse attribute information from the login form for AttributeExchange attribute: '*ax_attribute*'.

Explanation: The login form is not correctly formatted.

System action: The login attempt is terminated.

Administrator response: Ensure that the login form contains a correctly formatted URI for the attribute. If a count is specified, ensure that the value is either a positive integer or the string 'unlimited'.

FBTOID0039E An invalid value was received for the Attribute Exchange parameter: '*ax_param*' The received value was: '*received_value*'. The expected value was: '*expected_value*'.

Explanation: The received message contained an invalid value for an attribute exchange parameter.

System action: The request is halted.

Administrator response: Ensure that the OpenID partner is sending a valid value for the indicated attribute exchange parameter.

FBTOID003E Alias management is not supported for this federation.

Explanation: The OpenID federation has not been configured in Alias mode, therefore the alias management endpoint is not supported.

System action: The request will be ignored.

Administrator response: Do not use the alias management endpoint for this federation.

FBTOID0040W An attribute exchange message was sent with an unsupported mode: '*ax_mode*'

Explanation: The received message contained an unsupported attribute exchange mode.

System action: The attribute-exchange extension is ignored for this request.

Administrator response: Ensure that the OpenID partner sends supported attribute-exchange messages.

FBTOID0041E An attribute exchange alias was not in a valid format: '*ax_alias*'

Explanation: The received message contained an attribute exchange alias that did not meet the format requirements defined in the specification.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner is sending correctly formatted attribute-exchange messages.

FBTOID0042E The OpenID identity provider does not advertise support for one or more authentication policies.

Explanation: An authentication policy has been specified, but the identity provider does not support this policy.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner supports the authentication policy.

FBTOID0043E The OpenID identity provider does not support one or more assurance level policies.

Explanation: An assurance level namespace has been specified, but the identity provider does not advertise support for it.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner supports the authentication policy.

FBTOID0044E The OpenID identity provider did not authenticate the user as requested.

Explanation: An authentication policy has been specified, but the identity provider did not authenticate the user.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner supports the authentication policy.

FBTOID0045E The OpenID identity provider did not authenticate the user within the time limit that is required.

Explanation: The identity provider reported that the user was authenticated outside the specified maximum time limit.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner authenticates the user in a timely manner.

FBTOID0046E The OpenID identity provider did not specify the time at which the user was authenticated.

Explanation: A maximum authentication time limit was specified, but the identity provider did not report an authentication time.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner authenticates the user in a timely manner.

FBTOID0047E The OpenID identity provider does not support the PAPE extension.

Explanation: The selected identity provider does not support the PAPE OpenID extension.

System action: The request is rejected.

Administrator response: Ensure that the OpenID partner supports PAPE or has enabled the sendalways configuration for PAPE.

FBTOID0048E The trust chain configured by this OpenID identity provider did not provide the time that the user was authenticated.

Explanation: PAPE support requires user authentication time. Ensure that the configured mapping rule for this federation returns this value.

System action: The request is rejected.

Administrator response: Update the mapping rule to return this value.

FBTOID0049E The assurance level alias '*pape_alias*' does not have a mapped namespace.

Explanation: The OpenID message contained an assurance level alias that has not been declared with a namespace mapping.

System action: The request is rejected.

Administrator response: Ensure that only known namespace mappings are returned.

FBTOID004E The current user making the request is not authenticated.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTOID0050W Relying Party discovery of the trust root '*trustroot*' resulted in an exception: *extext*.

Explanation: Relying-party discovery cannot be successfully performed on the trust root received in the OpenID request.

System action: The request might be rejected, depending on your configuration.

Administrator response: Ensure that the relying-party advertises XRDS at the provided trust root URL that contains a service for http://specs.openid.net/auth/2.0/return_to with a matching URI.

FBTOID0051E Relying Party discovery of the trust root '*trustroot*' failed to find a match for return_to URL '*returnto*'.

Explanation: Relying-party discovery cannot be successfully performed on the trust root received in the OpenID request to validate the return_to URL.

System action: The request is rejected.

Administrator response: Ensure that the relying-party advertises XRDS at the provided trust root URL that contains a service for http://specs.openid.net/auth/2.0/return_to with a matching URI.

FBTOID0052W The runtime could not load the IDGenerator with module ID: '*moduleID*'. Instead the default module is loaded with ID: '*defaultModuleID*'.

Explanation: The configuration specifies a module ID that the runtime plug-in manager cannot load.

System action: A default IDGenerator module is loaded instead.

Administrator response: Ensure that the module ID is configured for the IDGenerator and that the plug-in containing the specified module is deployed to the runtime.

FBTOID0053E The maximum authentication age requested by the Relying Party '*authAge*' cannot be parsed.

Explanation: The Relying Party attempted to pass a parameter indicating the time in which a user must have been authenticated. However, this parameter cannot be parsed as an integer.

System action: The request is rejected.

Administrator response: Ensure that the Relying Party is sending valid data.

FBTOID0054E The PAPE assurance level alias '*alias*' has been used multiple times in the response from the OpenID OP.

Explanation: The Relying Party returned an assurance level alias that is used multiple times. Each alias must be mapped to exactly one namespace.

System action: The request is rejected.

Administrator response: Ensure that the Relying Party is sending valid data.

FBTOID0055E The PAPE assurance level namespace '*ns*' has been used multiple times in the response from the OpenID OP.

Explanation: The Relying Party returned an assurance level namespace that is used multiple times. Each namespace must be mapped to exactly one alias.

System action: The request is rejected.

Administrator response: Ensure that the Relying Party is sending valid data.

FBTOID0056E The reported PAPE authentication time string '*time*' is not a valid value.

Explanation: The authentication time is not valid.

System action: The request is rejected.

Administrator response: Ensure that the sender is sending valid data. The sender can be the Relying Party, a mapping rule, or both.

FBTOID0057E The reported PAPE authentication time string '*time*' is in the future.

Explanation: The authentication time is in the future. This situation usually occurs when the clock skew exceeds the configured skew amount.

System action: The request is rejected.

Administrator response: Ensure that the sender is sending valid data. The sender can be the Relying Party or a mapping rule, or both.

FBTOID005E The alias: *alias* has already been used by another user.

Explanation: The alias has been used by another user for this federation.

System action: The alias will not be stored for this user - they will have to select another alias.

Administrator response: The user will need to choose another alias.

FBTOID006E The alias: '*alias*' contains invalid characters. Only non-whitespace letters and digits should be used.

Explanation: The alias should contain only letters or digits.

System action: The alias will not be stored for this user - they will have to select another alias.

Administrator response: The user will need to choose another alias.

FBTOID007E An unexpected internal error has occurred: '*errtext*'.

Explanation: An unexpected internal error has occured.

System action: The request will be halted.

Administrator response: Please contact support.

FBTOID008E The supplied identity URL: '*idurl*' could not be resolved to an OpenID provider.

Explanation: The URL endpoint could not be fetched, or the fetched page did not contain OpenID server and/or delegate information.

System action: The request will be halted.

Administrator response: Please validate that the OpenID Identity URL is correct, and that it returns a page containing OpenID identity headers.

FBTOID009E The received openid.return_to URL from the identity provider: '*url1*' did not match the openid.return_to URL sent to it: '*url2*'.

Explanation: The consumer sent an openid.return_to URL to the identity provider during login, and this was not sent back to the consumer. This could indicate a replay attack.

System action: The request will be halted.

Administrator response: Please validate that the Identity Provider is not replaying messages and that it is using the correct return_to URL.

FBTOTP000E Internal Error. Contact the System Administrator.

Explanation: An internal error occurred.

System action: The one-time password manager encountered an error, process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP100E The plugin *pluginName* is missing the required parameter *parameter*

Explanation: A required plugin is missing from the plugin configuration.

System action: The one-time password plugin initialization encountered an error, process has been halted.

Administrator response: Provide the required parameter in the plugin configuration.

FBTOTP101E The value [*value*] of the plugin parameter *parameter* is not valid.

Explanation: Some of the values in the plugin configuration are not valid.

System action: The one-time password plugin initialization encountered an error, process has been halted.

Administrator response: Fix the parameter value in the plugin configuration.

FBTOTP200E The one-time password provider for type *type* is not found.

Explanation: The one-time password provider for the specified type is not found.

System action: Process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP201E The one-time password delivery for delivery type *type* is not found.

Explanation: The one-time password delivery for the specified delivery type is not found.

System action: Process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP202E One-time password manager not initialized.

Explanation: An internal error occurred.

System action: The one-time password manager encountered an error, process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP300E The required input parameter *param* is not found in the STSUU.

Explanation: A required input is missing from the input parameter.

System action: Process has been halted.

Administrator response: Provide the required parameter in the incoming STSUU.

FBTOTP301E Cannot obtain one-time password delivery option.

Explanation: There was an error in obtaining the one-time password delivery option.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP302E The one-time password cannot be generated.

Explanation: There was an error in generating the one-time password.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP303E The one-time password cannot be delivered to *deliveryAttribute*.

Explanation: There was an error in delivering the one-time password.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP304E The submitted one-time password is not valid.

Explanation: The entered one-time password is not valid.

System action: The request has been halted.

Administrator response: Correct the one-time password and resubmit the form.

FBTOTP305E The required service handle *handleName* was not provided to the STS module.

Explanation: The required service handle was not available.

System action: The STS request processing has been halted.

Administrator response: This error is a significant internal error. Check the logs for error messages indicating why the required service was not properly created.

FBTOTP306E An error occurred during the construction of the contents of a message.

Explanation: The messaging component failed to build a message to send to the user.

System action: The one-time password operation could not be completed.

Administrator response: The one-time password application could not send a message due to a problem constructing the message contents. If details are required, enable trace logging and examine the nested exception.

FBTOTP307E An internal error occurred. Contact the System Administrator.

Explanation: An internal error occurred.

System action: The one-time password application encountered an error, process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP308E The page contents might be missing the required information such as [*requiredInfo*] that is used to process an e-mail message request.

Explanation: The one-time password email delivery module requires certain information to process the request. The required information is missing.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTOTP309E The page contents might be missing the required information such as [*requiredInfo*] that is used to process an SMS message request.

Explanation: The one-time password SMS delivery module requires certain information to process the request. The required information is missing.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTOTP310E The one-time password that you submitted is not valid. Please submit a valid one-time password.

Explanation: You must use a valid one-time password.

System action: The one-time password is rejected.

Administrator response: None.

FBTOTP311E The one-time password is submitted after the one-time password has expired. Please generate another one-time password, and submit it before it expires.

Explanation: One-time passwords are only valid for a certain amount of time. Ensure that you submit the one-time password before it expires.

System action: The one-time password is rejected.

Administrator response: None.

FBTOTP312E The one-time password cannot be delivered to the email address: *toEmail*. Verify that the phone number is correct.

Explanation: There was an error in delivering the one-time password to the specified email address.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP313E The one-time password authenticate callback could not invoke the trust service to perform token exchange for operation id [*operation id*] .

Explanation: The one-time password authenticate callback could not invoke the trust service to perform the one-time password operation.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTOTP314E The one-time password authenticate callback could not retrieve the one-time password delivery options.

Explanation: The one-time password authenticate callback could not to retrieve the one-time password delivery options.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTOTP315E The one-time password cannot be generated or delivered.

Explanation: There was an error in generating and delivering the one-time password.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP316E The request received by the one-time password authentication callback was sent using a transport that is not valid.

Explanation: The request received by the one-time password authentication callback was sent using a transport that is not valid. The request was sent using the SOAP binding.

System action: The one-time password request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem. Ensure that the request is being sent using the appropriate binding.

FBTOTP317E The submitted one-time password could not be validated.

Explanation: The one-time password module could not validate the submitted one-time password value.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTOTP318E Unable to send the message to [*phoneNumber*] with username [*username*] because the SMS gateway provider returned a response HTTP status code [*statusCode*] which does not match the value that is configured in the response file for the parameter SuccessHTTPReturnCode: [*successCode*].

Explanation: The response HTTP status code returned by the SMS gateway provider does not match the value that is configured in the response file for the parameter SuccessHTTPReturnCode.

System action: The request has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP319E Unable to send the message to [*phoneNumber*] with username [*username*] because the SMS gateway provider returned an HTTP response body: [*responseBody*] which does not match the Java regular-expression pattern that is configured in the response file for the parameter SuccessHTTPResponse BodyRegexPattern: *regexPattern*

Explanation: The HTTP response body returned by the SMS gateway provider does not match the Java regular-expression pattern that is configured in the response file for the parameter SuccessHTTPResponseBodyRegexPattern.

System action: The request has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP320E The list of methods for generating, delivering, and verifying one-time password returned from OTPGetDeliveryMethods mapping rule is invalid.

Explanation: OTPGetDeliveryMethods mapping rule must return at least one method for generating, delivering, and verifying one-time password.

System action: The request has been halted.

Administrator response: Ensure that OTPGetDeliveryMethods mapping rule returns a valid list of methods for generating, delivering, and verifying one-time password.

FBTOTP321E The submitted ID of the method for generating, delivering, and verifying one-time password is invalid.

Explanation: The submitted ID must refer to one of the methods for generating, delivering, and verifying one-time password returned by

OTPGetDeliveryMethods mapping rule.

System action: The request has been halted.

Administrator response: None.

FBTOTP322E The one-time password based authentication failed. The user is not authenticated or the authentication level in the credential is not equal or higher to the supported authentication level [*authentication level*].

Explanation: The authentication process failed to generate a credential that supports the configured authentication level.

System action: The one-time password application encountered an error, process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTOTP323E The value [*action*] received on the one-time password action query string parameter is not valid.

Explanation: The value submitted using the action query string parameter is not valid.

System action: The one-time password application encountered an error, process has been halted.

Administrator response: None.

FBTOTP324E The value [*action*] received on the one-time password action query string parameter is not allowed when the previous step was [*previousPhase*].

Explanation: The authentication process failed because an invalid action value was specified.

System action: The one-time password application encountered an error, process has been halted.

Administrator response: None.

FBTOTP325E The method for generating, delivering, and verifying one-time password was not found in the session.

Explanation: The method for generating, delivering, and verifying one-time password needs to be available in the session.

System action: The request has been halted.

Administrator response: None.

FBTOTP326E The submitted CSRF token is invalid.

Explanation: The submitted CSRF token must match the last generated CSRF token.

System action: The request has been halted.

Administrator response: None.

FBTOTP328E The configured parameter [*parameterName*] with value [*value*] is outside of the range [*lowRange* - *highRange*]

Explanation: The parameter is outside of the expected range.

System action: The configuration is invalid. The one-time passwords cannot be verified.

Administrator response: Update the configuration so that the configuration parameter is in a valid range.

FBTOTP329E The configured parameter [*parameterName*] with value [*value*] is below the minimum value of [*lowRange*]

Explanation: The parameter is below the minimum accepted value.

System action: The configuration is invalid. The one-time passwords cannot be verified.

Administrator response: Update the configuration so that the configuration parameter is at least the minimum value.

FBTOTP330E Unable to locate the HMAC secret key

Explanation: The user's secret key for one-time password generation cannot be located.

System action: Unable to verify

Administrator response: Ensure that the secret key is being provided to the user through the STSUU

FBTOTP331E The specified algorithm [*parameterName*] is not supported on this system

Explanation: The algorithm chosen to generate the OTPs is not supported on this system. It is possible that the algorithm was not named correctly, or a newer version of Java is required.

System action: The algorithm specified is not supported, so OTPs cannot be verified.

Administrator response: Check the configuration to make sure the algorithm is specified correctly. It is possible that the algorithm is supported in a later version of Java than the one currently installed.

FBTOTP332E The one time use enforcement store [*parameterName*] could not be loaded or was not found.

Explanation: The one time use enforcement store implementing the OTPReplayStore interface was not found.

System action: Due to the configuration error, OTPs will not be generated or verified.

Administrator response: Check that the one time use enforcement store is available to be loaded. Also check that it implements the OTPReplayStore interface.

FBTOTP333E The one time use enforcement store [*parameterName*] implemented OTPStore, but not OTPReplayStore.

Explanation: The one time use enforcement store must implement the OTPReplayStore interface.

System action: Due to the configuration error, OTPs will not be generated or verified.

Administrator response: Specify a store that implements the OTPReplayStore interface.

FBTOTP334E The one time password provider failed to store the counter that corresponds to the user [*username*].

Explanation: The one time password provider failed to store the counter value that corresponds to the user.

System action: The request to authenticate the user using the one time password will fail.

Administrator response: Validate the one time password provider configuration .

FBTOTP335E The submitted PIN did not satisfy all requirements.

Explanation: The submitted PIN did not meet all of the requirements of the RSA Manager.

System action: The request to authenticate the user using the one time password and attempt to change the PIN will fail.

Administrator response: None.

FBTOTP336E The ID obtained from the obligation URI for the method for generating, delivering, and verifying one-time password is invalid.

Explanation: The ID obtained from the obligation URI must refer to one of the methods for generating, delivering, and verifying one-time password returned by OTPGetDeliveryMethods mapping rule.

System action: The request has been halted.

Administrator response: None.

FBTPWD001E The class *classname* is not the expected interface. The class will not be used for obfuscation.

Explanation: The class given to do obfuscation does not implement the correct interface.

System action: The class will not be used to perform obfuscation.

Administrator response: Ensure that the given class implements the documented interface to perform password obfuscation.

FBTPWD002E The password obfuscator utility is unable to locate the password obfuscator plug-in.

Explanation: A problem was encountered while attempting to load the plug-in.

System action: The plug-in was not loaded.

Administrator response: Check the logs for an exception that provides more details about the cause of the problem.

FBTPWD003E Could not determine the module directory to load the password obfuscator plug-in.

Explanation: A problem was encountered while attempting to locate the plug-in directory.

System action: The plug-in was not loaded.

Administrator response: Check the logs for an exception that provides more details about the cause of the problem.

FBTPWD004W The password obfuscator plug-in given could not be loaded. Ensure you have the module package in your classpath.

Explanation: For a plug-in to be loaded it requires some prerequisite module libraries to load the plug-in; the prerequisite module libraries are missing.

System action: The plug-in was not loaded.

Administrator response: Ensure that you have the required module libraries in the classpath to load the custom plugin.

FBTRPT001E Check that all required report parameters are set correctly.

Explanation: This error occurs when a required report parameter is missing or has been set incorrectly in a report design file.

System action: System cannot execute reporting functionality.

Administrator response: Check report parameter settings in report design file.

FBTRPT002E The Report engine cannot be started.

Explanation: This error occurs due to problems in the reports configuration.

System action: System cannot execute reporting functionality.

Administrator response: Check that the reports configuration has been defined properly.

FBTRPT003E Detected invalid or nonexistent directory for report designs.

Explanation: This error occurs when the report designs directory for the reports configuration is invalid or does not exist.

System action: System cannot execute reporting functionality.

Administrator response: Check that the report designs directory has been specified correctly in the reports configuration.

FBTRPT004E Detected invalid or nonexistent directory for report designs.

Explanation: This error occurs when the report archives directory for the reports configuration is invalid or does not exist.

System action: System cannot execute reporting functionality.

Administrator response: Check that the report archives directory has been specified correctly in the reports configuration.

FBTRPT005E Could not find report design.

Explanation: This error occurs when a report design cannot be found in the report designs directory.

System action: System cannot execute reporting functionality.

Administrator response: Check that the appropriate report design is located in the report designs directory as defined in the reports configuration.

FBTRPT006E Could not find archived report.

Explanation: This error occurs when an archived report cannot be found in the report archives directory.

System action: System cannot execute reporting functionality.

Administrator response: Check that the appropriate archived report is located in the report archives directory as defined in the reports configuration.

FBTRPT007E Could not create archive report directory for render type.

Explanation: This error occurs when a invalid or unsupported render type has been specified.

System action: System cannot execute reporting functionality.

Administrator response: Specify pdf or html as a render type.

FBTRPT008E An error has occurred while running report.

Explanation: This error occurs when an unexpected error has occurred while running a report.

System action: System cannot execute reporting functionality.

Administrator response: Check the system logs for error details.

FBTRPT009E Detected invalid report file name.

Explanation: This error occurs when the required naming convention for report design files is not followed.

System action: System cannot execute reporting functionality.

Administrator response: Check that report design file is named properly.

FBTRPT010E Detected invalid parameter with no selection choices.

Explanation: There was a problem retrieving selection choices for a list box, check box, or radio button parameter.

System action: System cannot execute reporting functionality.

Administrator response: Check that the list box, check box, or radio button parameter has been defined correctly in the report design.

FBTRPT011E Detected unsupported or invalid parameter. Parameter must be a scalar type.

Explanation: This error occurs when a parameter is not a scalar parameter.

System action: System cannot execute reporting functionality.

Administrator response: Check that the parameter has been defined as a scalar type in the report design. Only scalar parameters are supported in this release. Check the Review TFIM documentation for details on defining report parameters.

FBTRTE001E The runtime configuration properties file was not found.

Explanation: The runtime could not find its configuration file in the classpath.

System action: The action will be halted.

Administrator response: Validate the runtime configuration file is located in the runtimes classpath.

FBTRTE002E The runtime configuration domain property was not found.

Explanation: The runtime could not determine the domain from its property configuration file.

System action: The action will be halted.

Administrator response: Validate the runtime configuration file is located in the runtimes classpath and the domain is set correctly.

FBTRTE003E The runtime configuration could not get a repository handle from the managed container.

Explanation: The runtime requires a handle to the repository which it receives from the managed container.

System action: The action will be halted.

Administrator response: Validate the runtime is being used by a managed application and the container is operating correctly.

FBTRTE004E A required list of properties was not given.

Explanation: This action requires a properties list to be given.

System action: The action will be halted.

Administrator response: Validate that the required properties are being passed.

FBTRTE005E The required property (*property*) was not given.

Explanation: This action requires the specified property to complete.

System action: The action will be halted.

Administrator response: Validate that the required property is being given.

FBTRTE006E The given directory (*directory*) does not exist.

Explanation: The given directory must already exist to complete the action.

System action: The action will be halted.

Administrator response: Validate that the given directory exists.

FBTRTE007E The given directory path (*directory*) could not be created.

Explanation: This action requires that the given directory path has the access to be created.

System action: The action will be halted.

Administrator response: Validate that the given directory path can be created.

FBTRTE008E The given properties file (*properties file*) could not be found.

Explanation: This action requires that a properties file be given.

System action: The action will be halted.

Administrator response: Validate that the given properties file exists and has the correct access set.

FBTRTE012E The Access Manager server SSL configuration command returned with errors. See the log file for more details.

Explanation: The Access Manager SvrSslCfg command returned with errors.

System action: The action will be halted.

Administrator response: Check the log file for more details.

FBTRTE013E The Access Manager runtime configuration command returned with errors. See the log file for more details.

Explanation: The Access Manager PDJrteCfg command returned with errors.

System action: The action will be halted.

Administrator response: Check the log file for more details.

FBTRTE014E The server type given is not a supported type.

Explanation: The listen mode is currently not supported.

System action: The action will be halted.

Administrator response: Ensure that a supported listen mode is entered.

FBTRTE015E An error occurred when updating the server's state. Check server logs for more details.

Explanation: An error occurred when attempting to store the new server's state. See the logs for more details.

System action: The action will be halted.

Administrator response: Check the server logs for more details.

FBTRTE016E Unable to determine domain that the node is a member of. The operation did not complete.

Explanation: For any runtime operation to complete, the runtime must know what domain it is a member of.

System action: The action will be halted.

Administrator response: Ensure that Federated Identity Manager was started correctly.

FBTRTE017E An error occurred when updating the configuration in the repository. Check server logs for more details.

Explanation: The configuration repository returned an error.

System action: The action will be halted.

Administrator response: Check the server logs for more details.

FBTRTE018E The provided JAR file is not in the expected format. Import did not complete successfully.

Explanation: Only JAR files that are created by the export function can be used to import. The JAR file provided was missing required data.

System action: The action will be halted.

Administrator response: Ensure that only JAR files that are exported are used.

FBTRTE019E Did not find a software.properties file. Runtime deployment canceled.

Explanation: A software.properties file is required to give information about the runtime being deployed and it was not present.

System action: The action will be halted.

Administrator response: Ensure that the runtime was properly installed.

FBTRTE020E Did not find a serialId in the software.properties file. Runtime deployment canceled.

Explanation: The software.properties file should contain a serial identifier.

System action: The action will be halted.

Administrator response: Ensure that the runtime was properly installed.

FBTRTE021E Could not find the EAR properties file given in the software.properties file. Runtime deployment canceled.

Explanation: The EAR properties file given in the software.properties file could not be found. This properties file is required to deploy the EAR.

System action: The action will be halted.

Administrator response: Ensure that the runtime was properly installed.

FBTRTE022E An error occurred when attempting to deploy the runtime. Runtime was not deployed.

Explanation: An error occurred during the deployment of the runtime.

System action: The action will be halted.

Administrator response: Ensure that the runtime was properly installed and check the logs for further details.

FBTRTE025E An error occurred when attempting to remove the runtime. Runtime was not removed.

Explanation: An error occurred during the removal of the runtime.

System action: The action will be halted.

Administrator response: Check the logs for further details.

FBTRTE026E The node could not be unconfigured due to an error.

Explanation: An error occurred while attempting to unconfigure the runtime.

System action: The action will be halted.

Administrator response: Check the logs for further details.

FBTRTE029E The node could not be configured due to an error.

Explanation: An error occurred during the configuring of the runtime.

System action: The action will be halted.

Administrator response: Check the logs for further details.

FBTRTE030E The domain *domain name* could not be removed due to an error.

Explanation: An error occurred during the removal of the given domain.

System action: The action will be halted.

Administrator response: Check the logs for further details.

FBTRTE034E The domain *domain name* could not be created due to an error.

Explanation: An error occurred during the creation of the given domain.

System action: The action will be halted.

Administrator response: Check the logs for further details.

FBTRTE037E Unable to modify the application parameter *task or role name*.

Explanation: An attempt to locate and modify a particular set of application parameters failed.

System action: The parameters will not be modified.

Administrator response: No action is necessary unless other problems occur.

FBTRTE038E software.properties is unavailable, cannot publish any directories to domain.

Explanation: A software.properties file is required to give information about the directories to publish.

System action: The publish action is halted.

Administrator response: Ensure the runtime was properly installed.

FBTRTE039E The software.properties key *key* is missing or contains no directories to publish.

Explanation: A software.properties file is required to give information about the directories to publish.

System action: The publish action is halted.

Administrator response: Check the software.properties file and ensure there is a key with a value that is a directory or list of directories.

FBTSML001E The received request is missing the required parameter: *parameter*

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTSML002E The value *value* for attribute *attr* is not valid.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTSML003E The requested target, *target* is unknown or disabled.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message, and that the identity provider has configured and enabled service provider partners for this target.

FBTSML004E The request received an artifact with succinct ID: *succinctId*, which did not match a known partner identity provider.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message and the configuration of the partner identity providers.

FBTSML005E The current user making the request is not authenticated.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTSML006E The token cannot be exchanged for the service provider.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration.

FBTSML007E No configured post page is available to use to return the token to the service provider.

Explanation: The current request could not be completed because the token exchange succeeded but no configured post page was available.

System action: The request will be halted.

Administrator response: This is a configuration error. Ensure that the post page exists in the template directory.

FBTSML008E No token was available to return to the service provider.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration.

FBTSML009E The SAML response object received is not valid.

Explanation: The current request could not be completed because the SAML response object is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration.

FBTSML010E The sign-on message at the service provider contained parameters that are not valid.

Explanation: The current request could not be completed because the sign-on request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message from the identity provider.

FBTSML011E The response from the identity provider could not be understood or did not contain an assertion: *samlresponse***.**

Explanation: The current request could not be completed because the identity provider response was not understandable or did not contain a SAML assertion for sign on.

System action: The request will be halted.

Administrator response: Ensure that the identity provider is configured to send the correct XML element response and that the request to the identity provider was valid.

FBTSML012E The identity provider token cannot be exchanged for one that is valid for the resource.

Explanation: The current request could not be completed because the identity provider response was not understandable.

System action: The request will be halted.

Administrator response: Validate that the identity provider is configured to send the correct XML element response.

FBTSML013E The SAML artifact: *artifact* **is not valid.**

Explanation: The current request could not be completed as the provided SAML artifact is not valid.

System action: The request will be halted.

Administrator response: Validate that the service provider is configured correctly.

FBTSML014E The SAML assertion cannot be retrieved.

Explanation: The current request could not be completed because a SAML assertion could not be retrieved.

System action: The request will be halted.

Administrator response: Validate that the service provider is configured correctly and that the identity provider is configured to store the assertions for a sufficient time.

FBTSML015E While processing action: *action* **the internal context was missing attribute:** *action***.**

Explanation: The current request could not be completed because of an internal processing error.

System action: The request will be halted.

Administrator response: Contact IBM software support with this log file.

FBTSML016E While processing action: *action* **the following configuration parameter was determined to be missing or incorrect:** *action***.**

Explanation: The current request could not be completed because the configuration is not valid.

System action: The request will be halted.

Administrator response: Validate that the system is configured correctly.

FBTSML017E The assertion could not be retrieved from the identity provider at: *ip* **using artifact:** *artifact***.**

Explanation: The service provider could not retrieve the assertion from the identity provider.

System action: The request will be halted.

Administrator response: Ensure that the identity provider is available.

FBTSML018E The user cannot be authenticated.

Explanation: The current request could not be completed because the trust service response could not authenticate the user.

System action: The request will be halted.

Administrator response: Validate that the trust service and Point of Contact are properly configured.

FBTSML019E The SAML request is not valid.

Explanation: The current request could not be completed because the request received is not valid.

System action: The request will be halted.

Administrator response: Validate that the request is valid.

FBTSML020E The where-are-you-from process received a request for the identity provider: *ipURL*, **which did not match a known partner identity provider.**

Explanation: The current request received a where-are-you-from cookie which did not match an enabled partner identity provider.

System action: The request will be halted.

Administrator response: Validate that the incoming message contains a WAYF cookie that matches one of the provider IDs for an enabled partner identity provider. One workaround is to delete all persistent cookies on the browser and have the user perform the WAYF process again.

FBTSML021E The sign-on request at the service provider did not contain valid sign-on parameters. Either a SAML Response or a SAML Artifact should be included in the initial sign-on request.

Explanation: The current request could not be completed because the sign-on request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message from the browser to ensure that the identity provider has sent either a valid browser-artifact sign-on (redirect containing a SAMLart parameter), or a valid browser-post sign-on (POST containing a SAMLResponse parameter).

FBTSML200E Unexpected exception: *exception*

Explanation: The SAML 2.0 plug-in caught an unexpected exception.

System action: The operation will be halted.

Administrator response: Examine the trace logs for more information.

FBTSML201E Cannot determine the message issuer.

Explanation: The Issuer attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Verify that configuration is correct. The message issuer is the self provider ID.

FBTSML202W The provider is passive and cannot display the following page on the browser: *page*

Explanation: The provider is passive cannot take control of the user interface, including displaying pages.

System action: The page will not be displayed on the browser.

Administrator response: This might or might not be a problem. If it is a problem, determine why the provider is passive by examining trace logs and configuration. A provider can be directed to be passive by the IsPassive attribute in an authentication request.

FBTSML203E The provider cannot find the page to display.

Explanation: The provider cannot find a page to display in the browser.

System action: The page will not be displayed on the browser.

Administrator response: Examine the trace logs to determine which page was supposed to have been displayed. It might have been an error status page or a success status page. Check the system installation to determine if the pages have been properly installed.

FBTSML205E The provider is passive and cannot force a user authentication.

Explanation: The provider is passive and cannot take control of the user interface, including authenticating the user.

System action: The operation will halt.

Administrator response: Reconfigure the requesting provider to send authentication requests that do not require forced authentication, or that do not require the identity provider to be passive, or both.

FBTSML206E The provider is passive and cannot query the user for consent to federate.

Explanation: The provider is passive and cannot take control of the user interface, including querying the user for consent-to-federate accounts.

System action: The operation will halt.

Administrator response: Reconfigure the requesting provider to send authentication requests that do not require the identity provider to be passive.

FBTSML207E Cannot determine the SAML status.

Explanation: The SAML status attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Examine the trace logs to see why the SAML status was not set.

FBTSML208E Cannot create account linkage between the providers.

Explanation: The accounts are not linked and the SAML request forbids creating account information required for linkage.

System action: The operation will be halted.

Administrator response: Reconfigure the requesting provider to send authentication requests that allow the identity provider to create account linkage. This is done by setting the AllowCreate attribute in the NameIDPolicy element to true.

FBTSML209E Cannot create account linkage between the providers because the user denied consent to federate.

Explanation: The accounts are not linked (federated) and the user denied permission to link them.

System action: The operation will be halted.

Administrator response: Instruct end users to consent to account linkage (federation).

FBTSML210E The timestamp in the SAML message is out of range. The message timestamp, *msgTime***, is not within** *tolerance* **seconds of** *compareTime***.**

Explanation: The SAML message has a timestamp that is not valid.

System action: The message will be ignored.

Administrator response: There are several reasons that a SAML message timestamp might be out of range: The clocks on the service and identity providers systems are skewed beyond the acceptable tolerance, network delays are hampering message flow, or the acceptable tolerance for message timestamp is set too low. The administrator should check these points and make any necessary adjustments.

FBTSML211E The destination URL in the SAML message (*msgDest***) does not match the current provider location (***here***).**

Explanation: The SAML message has a destination URL that is not valid.

System action: The message will be ignored.

Administrator response: The most likely problem is that the SAML message is being created with an incorrect destination. Verify that configuration on the sending provider specifies the correct URL for the receiving provider.

FBTSML212E No authentication assertions were found.

Explanation: No assertions could be found at the identity provider.

System action: No assertions will be included in the authentication response message.

Administrator response: Examine the trace logs to see why no authentication assertion was set.

FBTSML213E Cannot determine the message destination.

Explanation: The Destination attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Verify that configuration is correct. The message destination is the URI to which the message is sent.

FBTSML214E Cannot determine the *endpoint* **endpoint for provider** *provider***.**

Explanation: The required target endpoint for the SAML message cannot be determined.

System action: The operation will be halted.

Administrator response: Verify that configuration is correct.

FBTSML215E The name identifier policy in the authentication request could not be met by this identity provider.

Explanation: The identity provider could not create a name identifier that adhered to the policy in the authentication request. Usually, this means that the policy specified an unsupported format or not did specify that a persistent identifier could be created.

System action: The operation will be halted.

Administrator response: Verify that authentication requests specify supported name identifier policies, or do not specify a policy at all.

FBTSML216E The user account could not be federated.

Explanation: The identity provider could not federate the user account. Usually, this means that there is something wrong with the identity service.

System action: The operation will be halted.

Administrator response: Verify that the identity service is configured properly and that the registry server is available.

FBTSML217E This provider cannot accept an unsolicited authentication response.

Explanation: The authentication response being processed does not have a corresponding authentication request. This provider is not configured to accept unsolicited authentication responses.

System action: The operation will be halted.

Administrator response: Verify that the service provider is configured properly regarding acceptance of unsolicited authentication responses.

FBTSML218E The specifications for the *endpoint* endpoint are not valid.

Explanation: The endpoint specified by the SAML message cannot be validated.

System action: The operation will be halted.

Administrator response: Verify that configuration is correct and that endpoint specifications such as index, URL and binding in the message are correct.

FBTSML219E Cannot determine the name identifier for the logout request.

Explanation: The NameID attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Examine the trace logs to see why no name identifier information was set.

FBTSML220E Cannot determine the session index for the logout request.

Explanation: The SessionIndex attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Examine the trace logs to see why no session index was set.

FBTSML221E The logout requester is not a valid partner.

Explanation: The issuer of the logout request message cannot be determined as a valid partner to this provider. On an identity provider, the request issuer must be a provider to which this provider has issued an assertion. On a service provider, the request issuer must be a provider that has issued an assertion to this provider.

System action: The operation will be halted.

Administrator response: If the request is legitimate, examine the trace logs to see why the request issuer was not found in the list of known logout partners.

FBTSML222E The response message does not correlate to the pending request.

Explanation: The response message contains an InResponseTo attribute that does not match the ID attribute of the pending request. It is possible that the response was received in error.

System action: The operation will be halted.

Administrator response: If the response is legitimate, examine the trace logs to see why the InResponseTo attribute does not match the ID attribute of the currently pending request.

FBTSML223E Logout failed.

Explanation: The locally authenticated user was not logged out successfully.

System action: The operation will be halted.

Administrator response: Examine the trace logs to see why logout failed.

FBTSML224E Cannot find partner configuration for provider *partner*.

Explanation: The required configuration for the partner provider cannot be found.

System action: The operation will be halted.

Administrator response: Ensure that the partner provider's metadata has been imported into this federation and that the configuration file is not corrupted.

FBTSML225E Token exchange failed.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration. In addition, examine the trace logs to see why the token exchange failed.

FBTSML226E The message has an Issuer attribute that is not valid.

Explanation: The SAML message is required by the specification to have an Issuer attribute. The Issuer format, if specified, must be urn:oasis:names:tc:SAML:2.0:nameid-format:entity. The message is either missing the Issuer attribute or has the wrong format specified.

System action: The message will be ignored.

Administrator response: Examine the trace logs on the provider that issued the message to see why the message was constructed without the Issuer attribute or with the incorrect Issuer format.

FBTSML227E The issuer of the ArtifactResolve message, *issuer*, does not match the intended recipient of the artifact message, *recipient*.

Explanation: An ArtifactResolve message was received from a provider which is not the intended recipient of the message associated with the artifact.

System action: The artifact in the ArtifactResolve message will not be exchanged for a SAML protocol message. An empty ArtifactResponse message will be returned.

Administrator response: The system is behaving correctly by disregarding potential attacks.

FBTSML228E Cannot initialize the SOAP client for the *endpoint* endpoint.

Explanation: Unable to initialize the SOAP client.

System action: The request will be halted.

Administrator response: Validate the SOAP client configuration. In addition, examine the trace logs for additional information.

FBTSML229E The artifact exchange failed. The message could not be retrieved using artifact: *artifact*.

Explanation: This provider attempted to exchange an artifact for a SAML protocol message but no message was returned.

System action: The operation will be halted.

Administrator response: Examine the artifact issuer to see why the artifact was not exchanged. The artifact may have expired and its associated message purged from the system, for example.

FBTSML230E A SAML response message was received that is not valid.

Explanation: A SAML response message was received, but a corresponding SAML request message could not be found. The response is considered invalid.

System action: The operation will be halted.

Administrator response: If the SAML response is expected, examine the trace logs to see why the corresponding SAML request was not found. Otherwise, no action is needed.

FBTSML231E A SAML response message was received that is not valid.

Explanation: A SAML response message was received, but it did not contain any AuthnStatements. The response is considered invalid for purposes of authentication.

System action: The operation will be halted.

Administrator response: Examine the issuer of the SAML message to see why it issued a SAML assertion with no AuthnStatement.

FBTSML232E No alias was found for user *User* and provider *PartnerProvider*.

Explanation: There was no alias found for the currently authenticated user for the specified partner provider.

Administrator response: Enable trace for detailed messages about the error.

FBTSML233E The identity service request to remove an alias for *userId* and provider *providerId* failed.

Explanation: The identity service operation was not successful.

Administrator response: Ensure that the identity and provider are valid and check the log for messages returned from the identity service.

FBTSML234E No principal was found for alias *aliasId* and partner provider *providerId*.

Explanation: The identity service operation was not successful.

Administrator response: Validate that the alias and provider are valid and check the log for messages returned from the identity service.

FBTSML235E The identity service request to update an alias for *userId* and provider *providerId* failed.

Explanation: The identity service operation was not successful.

Administrator response: Validate that the identity and provider are valid and check the log for messages returned from the identity service.

FBTSML236E The assertion issued by *partnerProvider* could not be validated or decrypted.

Explanation: The assertion could not be validated or decrypted.

Administrator response: Make sure that the validation keys, decryption keys and decryption parameters are configured properly for the provider that issued the assertion. The trace log will indicate which operation failed, validation or decryption.

FBTSML237E The SAML message could not be decrypted.

Explanation: The SAML message could not be decrypted.

Administrator response: Make sure that the decryption keys and decryption parameters are configured properly for the provider that sent the message.

FBTSML238E The SAML message signature could not be validated.

Explanation: The SAML message signature could not be validated.

Administrator response: Make sure that the validation key is configured properly for the provider that sent the message.

FBTSML239E The SAML message could not be parsed.

Explanation: The SAML message could not be parsed.

Administrator response: Make sure that incoming message is properly formatted.

FBTSML240E The SAML artifact could not be parsed.

Explanation: The SAML artifact could not be parsed.

Administrator response: Make sure that incoming artifact is properly formatted.

FBTSML241E The incoming HTTP message is not valid.

Explanation: The incoming HTTP message is not valid.

Administrator response: Make sure that incoming HTTP message is properly formatted.

FBTSML242E Authentication failed at the identity provider.

Explanation: The SAML status included in the authentication response message indicates that authentication failed at the identity provider.

System action: The operation will be halted.

Administrator response: Examine the trace logs on the identity provider that issued the response message to see why the authentication operation failed.

FBTSML243E The name identifier in the request is not valid.

Explanation: The name identifier in the request does not match the information that was stored for that provider during login. If the service provider was acting as a member of an affiliation group during login, the name identifier in the request must reflect that fact.

System action: The operation will be halted.

Administrator response: If the request is legitimate, examine the trace logs to see why information in the request name identifier does not match the information stored for that provider.

FBTSML244E Cannot perform the name ID management operation on a name identifier with format *Format*.

Explanation: The name identifier established during authentication in the current session is not persistent. Name ID update and termination management operations can be performed only on persistent name identifiers.

System action: The operation will be halted.

Administrator response: The user should authenticate using a means that establishes a persistent name identifier and then retry the operation.

FBTSML245E The request was missing the TARGET parameter.

Explanation: The initial request to the service provider must contain a TARGET parameter.

System action: The operation will be halted.

Administrator response: Modify the initial request to the service provider to contain a TARGET parameter, which should point to the desired SSO target URL.

FBTSML246E The request failed due to an internal error on the identity provider.

Explanation: The identity provider encountered an internal error preparing the samlp:Response for the service provider.

System action: The operation will be halted.

Administrator response: Check the identity provider log to determine the root cause of this error. The identity provider configuration for this partner might not be correct.

FBTSML247E The SAML request for artifact *Artifact* **could not be created using signing key** *KeyIdentifier***.**

Explanation: The service provider was unable to generate a signed samlp:Rquest message.

System action: The operation will be halted.

Administrator response: Check that the service provider signing key identifier is correctly configured.

FBTSML248E The SAML artifact *Artifact* **has already been presented to the identity provider.**

Explanation: The identity provider has detected that this artifact has already been presented for exchange.

System action: The operation will be halted.

Administrator response: This could be a replay attack, or the browser user may have simply reloaded the page containing the redirect to the service provider with the artifact.

FBTSML249E The federation group type specified in the configuration is not supported. Group ID: '*id***', Group display name: '***id***', federation group type '***type***'.**

Explanation: The federation group defined is not a supported type.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a supported group type in the configuration.

FBTSML250E The *partnerEndpointType* **endpoint for partner '***id***' and display name '***displayName***' for federation group with ID '***id***' and display name '***displayName***' is not valid. Endpoint value is '***displayName***'.**

Explanation: The specified partner endpoint is not valid.

System action: The SAML Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTSML251E The *partnerEndpointType* **endpoint for self '***id***' and display name '***displayName***' for federation group with ID '***id***' and display name '***displayName***' is not valid. Endpoint value is '***displayName***'.**

Explanation: The specified self endpoint is not valid.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid endpoint value in the configuration.

FBTSML252E The *partnerEndpointType* **endpoint is missing from the provider '***id***' and display name '***displayName***' configuration for federation group with ID '***id***' and display name '***displayName***'.**

Explanation: A required endpoint is missing from the provider's configuration.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify the required endpoint in the provider's configuration.

FBTSML253E The *propertyName* **property is missing from the provider '***id***' and display name '***displayName***' configuration for federation group with ID '***id***' and display name '***displayName***'.**

Explanation: A required property is missing from the provider's configuration.

System action: The SAML Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify the required property in the provider's configuration.

FBTSML254E The property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid.

Explanation: The specified property value is not valid.

System action: The SAML Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid property value in the configuration.

FBTSML255E The boolean property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. For Boolean properties the permitted values are 'true' or 'false'.

Explanation: The specified Boolean property value is not valid.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid Boolean property value in the configuration.

FBTSML256E The numeric property value '*propertyValue*' for property '*propertyName*' specified for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. The minimum value for this property is '*displayName*'.

Explanation: The specified numeric property value is not valid.

System action: The SAML Module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid numeric property value in the configuration.

FBTSML257E The Identity provider succinct id value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. The identity provider succinct ID is a required property.

Explanation: The specified numeric property value is not valid.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid identity provider succinct ID value in the configuration.

FBTSML258E The common domain service host value '*commonDomainServiceHost*' specified using property '*propertyName*' for partner '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' is not valid. The common domain service host must start with http:// or https:// and end with the common domain value '*displayName*'.

Explanation: The specified common domain service host is not valid.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid common domain service host in the configuration.

FBTSML259E The provider source id value '*propertyValue*' specified under property '*propertyName*' for provider '*id*' and display name '*displayName*' for federation group with ID '*id*' and display name '*displayName*' does not match the message digest of the provider ID.

Explanation: The specified provider source ID value is not valid.

System action: The SAML module could not be initialized.

Administrator response: Verify that configuration files are present and have not been corrupted. Specify a valid provider source ID value in the configuration.

FBTSML260E The binding value *value* for attribute *attr* is not valid for profile *profile*.

Explanation: The specified binding is not valid for the profile being executed.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTSML261E Unobfuscation of the basic authentication password for SOAP client authentication failed.

Explanation: Unobfuscation of the basic authentication password for SOAP client authentication failed.

System action: The request will be halted.

Administrator response: Check the logs for a runtime exception.

FBTSML262E The ECP profile is not enabled for the provider.

Explanation: The ECP profile is not enabled.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTSML263E The name identifier policy in the request is not valid.

Explanation: The name identifier policy in the request is not valid. The format is not a supported format or the SPNameQualifier is not known to the provider.

System action: The operation will be halted.

Administrator response: If the request is legitimate, examine the trace logs to see why the name identifier policy is considered invalid.

FBTSML264E The SAML assertion contains a session index value that has been invalidated by a previously received logout request.

Explanation: The current request could not be completed because a SAML assertion is not considered valid.

System action: The request will be halted.

Administrator response: If the response is legitimate, examine the trace logs to see why the session index attribute was included on a logout request.

FBTSML265E The SAML assertion with the specified assertion ID *value* was not found.

Explanation: The current request could not be completed because a SAML assertion was not stored or the assertion ID is not valid.

System action: The request will be halted.

Administrator response: Please submit the request with a valid assertion ID.

FBTSML266E The index '*value*' for endpoint type '*value*' specified using query string parameter '*value*' does not exist.

Explanation: The current request could not be completed because a the endpoint index is not valid.

System action: The request will be halted.

Administrator response: Please submit the request with a valid endpoint index.

FBTSML267E The value '*value*' specified using query string parameter '*value*' is not valid integer value.

Explanation: The current request could not be completed because a query string parameter is not valid.

System action: The request will be halted.

Administrator response: Please submit the request with a valid integer value.

FBTSML268E Logout from one or more partners failed.

Explanation: A failed status was returned from one or more partner logout attempts.

System action: The request did not complete successfully.

Administrator response: Check the logs for failure reason.

FBTSML269E The users account was not successfully deferated from the partner.

Explanation: The users account was not successfully deferated from the partner

System action: The request did not complete successfully.

Administrator response: Check the logs for failure reason.

FBTSML270E The user provided to the administrative command does not have an active session.

Explanation: The users could not be logged out because they do not currently have a valid session.

System action: The request did not complete successfully.

FBTSML271E The SAML assertion cannot be retrieved using artifact: *artifact*

Explanation: The current request could not be completed because a SAML assertion could not be retrieved.

System action: The request is halted.

Administrator response: Validate that the service provider is configured correctly and that the identity provider is configured to store the assertions for a sufficient time.

FBTSML272E The SAML module was unable to query the user attributes.

Explanation: The current request could not be completed because the SAML module was unable to create a attribute query service claims object.

System action: The request will be halted.

Administrator response: Check the logs for failure reason.

FBTSML273E The SAML module was unable to obtain the subject name id from the attribute query request.

Explanation: The current request could not be completed because the subject name id is not valid.

System action: The request will be halted.

Administrator response: Please submit a valid attribute query request.

FBTSML274E The SAML module was unable to obtain the subject principal name using the name id included with the attribute query request.

Explanation: The current request could not be completed because the subject principal name can not be obtained.

System action: The request will be halted.

Administrator response: Please submit a valid attribute query request.

FBTSML275E The SAML message could not be retrieved using artifact: *artifact***.**

Explanation: The provider could not retrieve the SAML message using the supplied artifact.

System action: The request will be halted.

Administrator response: Ensure that the artifact is valid and the provider is properly configured.

FBTSML276E The SAML artifact: *artifact* **is expired.**

Explanation: The artifact received is no longer valid.

System action: The request will be halted.

Administrator response: Ensure that the artifact is valid and the provider is properly configured.

FBTSOC001E The SOAP endpoint passed in the SOAP client is not valid. The passed-in value was *parameter***.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Make sure that the correct SOAP endpoint URL is configured.

FBTSOC002E An error occurred in initializing SSL with the SOAP endpoint.

Explanation: The server might not be enabled for SSL. The SSL parameters passed in might not be valid.

System action: The request will be halted.

Administrator response: Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC003E The TrustStore identifier passed in SOAPClientImpl is null. The SSL connection with the endpoint *parameter* **cannot be initialized.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC004E The KeyStore name *parameter* **cannot be obtained from KessService.**

Explanation: The specified keystore cannot be obtained from KessService.

System action: The request will be halted.

Administrator response: Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC005E The TrustStore cannot be initialized from the passed in identifier *parameter***.**

Explanation: The truststore parameter passed in is not valid.

System action: The request will be halted.

Administrator response: Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC006E The SOAP client is unable to parse the response SOAP message.

Explanation: The SOAP client was unable to parse the incoming response SOAP message.

System action: The request will be halted.

Administrator response: Validate the Access Control List configuration in the destination endpoint.

FBTSOC007E The Client Keystore cannot be initialized from the passed in identifier *parameter*.

Explanation: The client keystore parameter passed in is not valid.

System action: The request will be halted.

Administrator response: Validate the partner's SSL configuration for the SOAP back channel.

FBTSOC008E The SOAP client is unable to send the request SOAP message.

Explanation: The SOAP client was unable to send the outgoing request SOAP message.

System action: The request will be halted.

Administrator response: Validate the Access Control List configuration in the destination endpoint.

FBTSOC009E Unobfuscation of the basic authentication password for SOAP client authentication failed.

Explanation: Unobfuscation of the basic authentication password for SOAP client authentication failed.

System action: The request will be halted.

Administrator response: Check the logs for a runtime exception.

FBTSOC010E Unable to construct a SOAP fault because the compulsory parameter *parameter* was null.

Explanation: A constructor of a SOAP fault attempted to build it without the required parameter.

System action: The SOAP fault will not be build.

Administrator response: Contact support.

FBTSOC011E The AccessApproval module: *module* has denied access to the endpoint: *url*

Explanation: A custom AccessApproval module has denied access to the endpoint.

System action: The connection is rejected.

Administrator response: If the URL is supposed to be accessible, modify the custom access approval module to permit access to it.

FBTSOC012E Unable to load an AccessApproval module with the extension ID: *module*

Explanation: The extension manager could not load an AccessApproval module.

System action: The request is not processed.

Administrator response: Verify that an extension with the specified ID is included in the published plug-ins.

FBTSPS002E The requester cannot be prompted for an identity provider. No defined federations are valid for the request.

Explanation: The current request and delegate protocol do not match any known defined federation.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service.

FBTSPS003E The template *identifier* cannot be located.

Explanation: The current request action cannot be processed.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service.

FBTSPS004E The template document used to request a requester's identity provider is not valid.

Explanation: The template document is missing the required tokens or is not a valid XML document.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service.

FBTSPS006E The request message could not be understood by the adapter.

Explanation: The request adapter was unable to adapt the input message.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS007E The single sign-on protocol service is in a state such that the status cannot be displayed with a template page.

Explanation: This error can be caused by an input request before the single sign-on protocol service is fully bootstrapped or it is caused by a configuration that is not valid.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS008E Requests cannot be accepted.

Explanation: This error can be caused by an input request before the single sign-on protocol service is fully bootstrapped or it can be caused by a configuration that is not valid.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS010E The request to address *address* cannot be accepted.

Explanation: This error might be caused by misconfiguration or by a request that is not valid.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the input message.

FBTSPS011E The protocol for address *address* could not be determined.

Explanation: This error typically occurs because the configuration is not valid or because a configuration has not been received.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and replication latency.

FBTSPS012E The single-sign on protocol service has not started.

Explanation: This error typically occurs because the configuration is not valid or because a configuration has not been received.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and replication latency.

FBTSPS014E An instance of a distributed map cannot be retrieved.

Explanation: Without the distributed map, the single sign-on protocol service cannot be configured.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and environment.

FBTSPS015E An error occurred while moving to a new configuration.

Explanation: The newly set or retrieved configuration could not be used.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and environment.

FBTSPS017E An error occurred while bootstrapping the single sign-on protocol service.

Explanation: The configuration could not be found or contains items that are not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service. A detailed message can be found in the trace.

FBTSPS018E The version of the configuration *inputVersion* is not valid for the single sign-on protocol service.

Explanation: The configuration version is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS020E The configured component *className* cannot be loaded.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS021E The configured endpoint *endpoint* is not valid.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS025E Unable to register a management bean.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Check the log file for errors.

FBTSPS027E The configured delegate protocol *delegate* is not valid.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and valid configuration versions

FBTSPS029E The configured delegate protocol *delegate* has a configuration entry that is not valid for the configuration file location.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and valid configuration versions.

FBTSPS037E The single sign-on protocol service configuration file cannot be located. This result might be expected.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS038E The configuration file at *confLocation* cannot be read. This file is specified in the configuration and is required for the single sign-on protocol service to start.

Explanation: The configuration file is not valid. This result might be due to access violations or an XML validation error.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS039E The component *component* cannot be created.

Explanation: The configuration file is not valid, or a specified class could not be loaded.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS040E The component *component* cannot be created. The provided configuration is not valid.

Explanation: The configuration file is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS041E No input was received with the management operation.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS042E The property, *property*, is required for this operation.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS043E The page factory root, *root*, does not exist.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS044E The page factory default language, *root*, does not exist.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS045E The given reference ID, *id*, is not valid.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS046E The given classname ,*classname*, could not be loaded.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS047E The given entity, *entity*, does not exist.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS048E The given value, *value*, is not valid for configuration item *item*.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS051E The WebSEAL authentication service client cannot be initialized.

Explanation: The management operation is not valid.

System action: The operation will be halted.

Administrator response: Validate the management operation.

FBTSPS052E The WebSEAL authentication service client is not in a valid state because the configuration is not valid and cannot be used.

Explanation: The sign in or sign out operation cannot be performed.

System action: The operation will be halted.

Administrator response: Validate the configuration of the authentication service and policy server configuration files.

FBTSPS053E The credential included with the request, *cred*, is not valid.

Explanation: The credential format is not understandable.

System action: The operation will be halted.

Administrator response: Validate the configuration of the authentication service and WebSEAL.

FBTSPS054E The entity ID, *id*, is not valid.

Explanation: The configuration component is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS055E The configured class, *classN*, does not implement or extend the required class or interface, *intf*.

Explanation: The configuration file is not valid.

System action: The startup will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service and the configuration versions.

FBTSPS056E The token included with the sign in request, *cred*, is not valid.

Explanation: The token type and format is not understandable.

System action: The operation will be halted.

Administrator response: Validate the configuration of the authentication service and caller.

FBTSPS057E The required WebSEAL header, *cred*, is missing.

Explanation: The header is required for proper operation.

System action: The operation will be halted.

Administrator response: Validate the WebSEAL configuration.

FBTSPS058E The sign out operation has failed.

Explanation: Sign out failed.

System action: The operation will be halted.

Administrator response: Check the trace log for detailed output from the policy server.

FBTSPS059E The configured default page factory selector, *selector*, is not valid.

Explanation: The specified default selector is not valid.

System action: The management operation will be halted.

Administrator response: Check the configured default against the available selectors.

FBTSPS060E Page factory operation requires at least one page selector.

Explanation: The specified page factory configuration does not specify any selectors.

System action: The management operation will be halted.

Administrator response: Check the configuration of the page factory.

FBTSPS061E An unexpected error has occurred with a protocol module ***module*****.**

Explanation: This error might be caused by misconfiguration or by a request that is not valid.

System action: The request will be halted.

Administrator response: Validate the configuration of the single sign-on protocol service, protocol module, and the input message.

FBTSPS062E The Point of Contact protocol module is missing the required action, specified by parameter ***parameter*****.**

Explanation: This error is typically caused by a request that is not valid. The action parameter is necessary to determine the behavior of the module.

System action: The request will be halted.

Administrator response: Validate the request message.

FBTSPS063E The Point of Contact protocol module is missing the required token for the chosen action.

Explanation: This error is typically caused by a request that is not valid. The token is necessary to perform the specified action.

System action: The request will be halted.

Administrator response: Validate the request message.

FBTSPS064E The configured module with ID ***id*** **and version** ***version*** **was not found when searching for modules.**

Explanation: The module with the specified ID and version was not found while attempting to load modules. This can occur if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action: The request to load the module will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS065E The configured module with ID ***id*** **does not expose a class with ID** ***id*****.**

Explanation: The module with the given ID and exposed class ID was not found while attempting to load modules. This can occur if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action: The request to load the module will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS066E The configured module with ID ***id*** **referencing a module with ID** ***moduleId*** **with java class** ***className*** **cannot be instantiated.**

Explanation: When attempting to load a module with the given ID and class name, an error occurred. This can occur if the if the Federated Identity Manager modules have not been configured correctly or the module does not exist.

System action: The request to load the module will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS067E The configured module reference, ***referenceId*****, could not be located in the configuration.**

Explanation: In order to load a module, a valid reference ID is required.

System action: The request to load the module will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS068E An attempt was made to retrieve a component with identifier '***id*****' which does not exist.**

Explanation: In order to load a component, a valid reference ID is required.

System action: The request to load the component will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS069E The delegate protocol instance ***delegateId*** **requires a protocol action** ***actionClassName*** **which could not be created.**

Explanation: The actions for the delegate protocol need to be located and created in order to be invoked.

System action: The request to load the component will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS073E The group membership *group* specified for delegate *id* is not valid and will be ignored.

Explanation: The specified group ID does not exist or could not be found.

System action: The protocol module will not have access to that group's properties.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS074E The delegate protocol *id* will not be available at runtime because the properties provided in the groups that it is a member of are not valid.

Explanation: The properties for the delegate group memberships are not correct. This typically indicates that federation configuration is not valid.

System action: The protocol module will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration. Additional messages in the error and trace logs by the protocol implementation will display the exact error condition.

FBTSPS075E The delegate protocol *id* will not be available at runtime because the protocol action *className* could not be created.

Explanation: A protocol action used by this delegate could not be created.

System action: The protocol module will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS076E An error occurred reading page templates. The SPS will continue startup, but no pages will be available at runtime.

Explanation: An error occurred reading the pages directory. The directory may not exist or the service may not have the required permissions to read the files.

System action: Startup will continue, but pages will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS077E An error occurred creating the service factory *id*. This service factory will not be available to protocols at runtime.

Explanation: An error occurred creating the service factory.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS078E An error occurred creating the point of contact client *id*. The service will not be available to protocols at runtime.

Explanation: An error occurred creating the point of contact client.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS079E An error occurred creating the global handler *id*. The service will not be available at runtime.

Explanation: An error occurred creating the global handler.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS080E An error occurred creating the protocol determination module *id*. The service will not be available at runtime.

Explanation: An error occurred creating the protocol determination module.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS081E Unable to retrieve an instance of the IdServiceClientFactory.

Explanation: An error occurred retrieving an instance of the alias service client factory.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS082E Unable to retrieve an instance of the Token Command Factory with endpoint *endpoint*.

Explanation: An error occurred retrieving an instance of the token service client factory.

System action: Startup will continue, but the service will not be available at runtime.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS083E The single sign-on protocol service was unable to locate a directory where template pages are stored.

Explanation: The Federated Identity Manager application does not contain the directory containing template page directories.

System action: No template pages can be used.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS084E An internal error has occurred within the SPS.

Explanation: The current request could not be processed because of an internal error.

System action: Processing of the current request will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS085E The current request cannot be accepted because the component that is required to process it is missing.

Explanation: The current request could not be processed because of an internal error.

System action: Processing of the current request will be halted.

Administrator response: Validate the Federated Identity Manager configuration.

FBTSPS087E Unable to retrieve an instance of the Name Identifier Generator with key *id*.

Explanation: An error occurred retrieving an instance of the specified NameId generator from the alias service.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS088W The time zone identifier given, [*id*], is not valid.

Explanation: The given time zone identifier is not a supported time zone.

System action: The default UTC time zone will be used.

Administrator response: Ensure that the time zone identifier in the configuration is correct. Check the returned exception for more details.

FBTSPS089W The time display pattern [*id*] is not supported.

Explanation: The given time display pattern is not supported.

System action: The default ISO8601 time format will be used.

Administrator response: Ensure that the time format in the configuration is correct. Check the returned exception for more details.

FBTSPS090W The callback [*id*] could not be initialized.

Explanation: An error was encountered during the initialization of the given callback.

System action: The given callback will be removed from the list of running callbacks.

Administrator response: Check the logs for a related exception and correct the problem. The error is most likely caused by a configuration error.

FBTSPS092E Access denied.

Explanation: The user does not have permission to access the Web page.

System action: The user will be shown a Web page indicating that access is not allowed.

Administrator response: If the user should be permitted to access the Web page, the administrator should grant the user permission. The administrator may need to add a user to the group being used for SOAP endpoint access control, for instance.

FBTSPS096E The point of contact implementation failed to perform programmatic login.

Explanation: An error occurred performing JAAS login.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS097E The point of contact implementation failed to authenticate the user performing the request.

Explanation: An error occurred performing JAAS login.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS098E The point of contact implementation failed to obtain the initial request URL.

Explanation: An error occurred obtaining the initial request URL from the user session.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS106E ITFIM Form Login Error

Explanation: See message.

System action: No action taken.

Administrator response: Check the trace and message logs for further details.

FBTSPS107E Form Login Error

Explanation: See message.

System action: No action taken.

Administrator response: Check the trace and message logs for further details.

FBTSPS109E Form authentication failed.

Explanation: See message.

System action: No action taken.

Administrator response: Check the trace and message logs for further details.

FBTSPS110E Check the user ID and password, and try again.

Explanation: See message.

System action: No action taken.

Administrator response: Check the trace and message logs for further details.

FBTSPS111E The point of contact endpoint requires the user to be authenticated. Please validate the point of contact settings.

Explanation: Unable to obtain user information from the request.

System action: The request is stopped.

Administrator response: Validate that the security roles are mapped properly to users and the point of contact settings.

FBTSPS112E Access to the URL '*url***' by the user '***user name***' was denied because the user was not assigned the role '***role name***'.**

Explanation: A user attempted to access the specified URL, but was denied access.

System action: The request is stopped.

Administrator response: Validate that the security roles are mapped properly to users. If the request was a SOAP request, verify that the partner has a valid password or certificate. Verify that the SOAP Endpoint Security Settings have been configured properly. If you are using groups to control access to the SOAP endpoint, verify that the partner's user ID is in the correct group.

FBTSPS113E The query service factory was configured with a class name that cannot be loaded. The class name is: '*class***'**

Explanation: This is an internal error in the configuration of the query service factory in the sps.xml configuration file.

System action: The query service factory cannot be configured.

Administrator response: Report this error to IBM Software Support; this error should not happen.

FBTSPS114E The query service was unable to complete the request with the trust service.

Explanation: An exception was thrown when communicating with the trust service.

System action: The request is stopped.

Administrator response: Examine the exception reported in the log file.

FBTSPS115E The claims object passed to the query service for update was of type: '*class*' and did not support the required interface: '*interface*'.

Explanation: An internal programming error has been detected.

System action: The request is stopped.

Administrator response: Report this error to IBM Software Support; this error should not happen.

FBTSPS116W Cannot locate the domain mapping file. Will not try to initialize ITFIMRuntime components.

Explanation: The Tivoli Federated Identity Manager domain mapping properties file could not be located in the WebSphere configuration repository. This could be that the Tivoli Federated Identity Manager runtime has not yet been deployed.

System action: The Tivoli Federated Identity Manager runtime components will not be initialized.

Administrator response: Deploy the Tivoli Federated Identity Manager runtime.

FBTSPS120E The Tivoli Federated Identity Manager runtime components cannot be initialized because the runtime cannot connect to a remote configuration repository.

Explanation: If the Tivoli Federated Identity Manager runtime components are deployed in a WebSphere cluster, then the runtime components need to acquire a handler to a remote deployment manager's configuration repository. This connection may fail if the deployment manager was not started, or that the managed nodes were started before launching the deployment manager.

System action: The runtime components are left in an uninitialized state.

Administrator response: Restart the WebSphere cluster by first starting the deployment manager, then starting the node agents, and finally starting the managed node servers.

FBTSPS121W The credential attribute '*attribute*' with value '*attribute value*' could not be added to the SSO token because the attributes size limit has been reached.

Explanation: The Tivoli Federated Identity Manager PoC implementation was not able to add the attribute to the SSO token.

System action: The SSO token will not include the attribute.

Administrator response: Increase the attributes size limit.

FBTSPS122E The Tivoli Federated Identity Manager runtime components are not initialized.

Explanation: The Tivoli Federated Identity Manager runtime components are not initialized. The runtime node is probably not configured. The following components will not be operational: Security Token Service, Single Sign-on Protocol Service, Info Service, and Audit Service.

System action: No action taken.

Administrator response: Configure the runtime nodes.

FBTSPS123E The point of contact client callback mapping rule is invalid.

Explanation: The point of contact client callback mapping rule is invalid.

System action: The point of contact client callback mapping fails.

Administrator response: Verify that the point of contact client callback is configured correctly.

FBTSPS124E The point of contact client callback could not determine mapping rule type.

Explanation: The point of contact client callback cannot determine the rule type based on the configuration.

System action: The point of contact client callback mapping fails.

Administrator response: Verify that the point of contact client callback is configured correctly.

FBTSPS125E The point of contact client callback failed to execute the mapping rule.

Explanation: The point of contact client callback could not execute the mapping rule.

System action: The point of contact client callback mapping fails.

Administrator response: Verify that the point of contact client callback is configured correctly.

FBTSPS127E The point of contact client callback attribute {0} in the universal user is invalid.

Explanation: The point of contact client callback attribute value in the universal user is invalid.

System action: The request is stopped.

Administrator response: Verify that the authentication policy callback is configured correctly.

FBTSPS128E The point of contact client callback failed to create the authentication policies.

Explanation: The point of contact client callback failed to create the authentication policies.

System action: he request is stopped.

Administrator response: Verify that the authentication policy callback is configured correctly.

FBTSPS129E The point of contact implementation failed to obtain the authentication target URL or transaction id from the supplied query string parameters.

Explanation: An error occurred obtaining the target URL or transaction id from the query string.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS130E The point of contact multi phase authentication callback implementation failed to obtain the authentication target URL.

Explanation: An error occurred obtaining the target URL.

System action: The request is stopped.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS131W The point of contact callback query string parameters {0} value {1} is not valid.

Explanation: An error occurred obtaining the query string parameter value.

System action: The request will continue using a default value.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS132W The point of contact callback mapping rule context attribute {0} value {1} is not valid.

Explanation: An error occurred obtaining the mapping rule context attribute value.

System action: The request will continue using a default value.

Administrator response: Validate the Federated Identity Manager configuration and check the trace and message logs for further details.

FBTSPS133E The system cannot read the 'dscclient.properties' file

Explanation: The client configuration containing information on available DSCs is missing.

System action: The in memory HttpSession will be used.

Administrator response: Ensure the file named dscclient.properties exists with the correct values present.

FBTSPS134E No DSC can be reached at this time.

Explanation: All configured DSCs in the dscclient.conf are not responding.

System action: The in memory HttpSessions will be used.

Administrator response: Check that the dscclient.properties contains valid DSC information, and check that the DSCs are responsive.

FBTSTM006E The given TokenType or AppliesTo (*TokenType/AppliesTo*) in the request is not supported by this server's configuration for *RequestType* RequestType.

Explanation: The request requested a TokenType or AppliesTo that is not supported by the server's configuration. This error can occur because the request data did not map to any processing chains or because the expected processing chain that the request maps to did not start correctly.

System action: The request has been halted.

Administrator response: Ensure that the request has all the required data.

FBTSTM007E STSModule *module_name* not found.

Explanation: The server attempted to load the STSModule but could not because an error occurred.

System action: The module has not been loaded possibly because the chains that the module is in have not been loaded.

Administrator response: Check the server logs for errors and exceptions to identify the problem.

FBTSTM008E The QName namespace prefix (*QName*) does not match any defined namespaces.

Explanation: The given namespace prefix does not match any defined namespaces.

System action: The request has been halted.

Administrator response: Ensure that the request uses supported XML namespaces.

FBTSTM009E The server did not start correctly.

Explanation: The trust server did not start correctly because of internal errors.

System action: The server will not accept requests.

Administrator response: Inspect logs and configuration files and ensure that data in the configuration file is correct.

FBTSTM010E A TokenType or AppliesTo must be specified in the request.

Explanation: According to the specification, at least one of TokenType or AppliesTo must be specified in the request.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM011E The date and time are not in the expected UTC format.

Explanation: The date and time given in the request was not in the expected UTC time format.

System action: The request has been halted.

Administrator response: Ensure that the correct time format is used for the request.

FBTSTM013E A RequestType must be specified in the request.

Explanation: According to the specification, a RequestType must be specified in the request.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM014E The given RequestType (*RequestType*) is not supported by this server's configuration.

Explanation: The RequestType does not apply to any of the STSChainMappingDefinitions located in the server's configuration.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM015E Either no configured XPath selected a node from the request, or the given TokenType or AppliesTo (*TokenType/AppliesTo*) in the request is not supported by this server's configuration for *RequestType* RequestType and Issuer (*Issuer*).

Explanation: Either no XPath in the configuration selected a node from the request, or the request requested a TokenType or AppliesTo that is not supported by the server's configuration.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM016E The given Issuer (*Issuer*) is not supported by this server's configuration.

Explanation: The Issuer does not apply to any of the STSChainMappingDefinitions located in the server's configuration.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM017E The server could not find the expected token included in the request.

Explanation: The given request did not include the expected token based on the server's configuration.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM018E An incorrect namespace was encountered and received *QName*, but expected *QName*.

Explanation: The client sent a request that used a namespace that was not expected. This error is typically caused by an old namespace being used.

System action: The request has been halted.

Administrator response: Ensure that the supported XML namespaces are used.

FBTSTM019E The expected namespace *URI* for the WS-Trust schema was not found in the request.

Explanation: The client did not specify a valid WS-Trust schema in the request.

System action: The request has been halted.

Administrator response: Ensure that the required request data is given.

FBTSTM020E An error was encountered when attempting to open file *filename*.

Explanation: The server attempted to open the specified file and encountered an error.

System action: The operation did not complete.

Administrator response: Ensure that the file exists and has the correct file permissions.

FBTSTM021E Either the properties file (*filename*) was not found in the classpath or the key (*key*) returned no data.

Explanation: The given properties file could not be found in the classpath or the key to look up data in the properties file did not return the expected data.

System action: The operation did not complete.

Administrator response: Ensure that the given properties file is located in the classpath, or that the key given has data associated with it, or both.

FBTSTM022E The message passed to the service from the webservices runtime was not complete or did not exist.

Explanation: A possible cause of this problem is that the Trust Service System Handler was not installed correctly or was removed from the system.

System action: The request was halted.

Administrator response: Ensure that the Trust Service System Handler is installed and located in the WebSphere Application Server classpath.

FBTSTM023E The trust service did not start successfully because it could not locate the local or distributed configuration data.

Explanation: The trust service could not locate the configuration data.

System action: The service did not start.

Administrator response: If the service is the only service for the domain, ensure that the configuration file exists. If the service is in a cluster, ensure that the cluster is operating correctly.

FBTSTM030E The trust service did not fully stop.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM031E The trust service did not fully start.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM032E The trust service did not fully start, stop, or both.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM033E The trust service failed to write configuration to persistent storage.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM034E The context was not found.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM035E The management method requested is not implemented.

Explanation: See message.

System action: No action taken.

Administrator response: No response required.

FBTSTM036E An error occurred while retrieving the server's configuration for the management operation.

Explanation: The server encountered an error when it attempted to retrieve its configuration.

System action: The operation was halted.

Administrator response: Check logging messages for errors related to retrieving the server's configuration and ensure that the correct file permissions are set on the server's configuration file.

FBTSTM038E A classname must be provided.

Explanation: The caller-requested operation requires a classname but did not provide a classname.

System action: The operation was halted.

Administrator response: Ensure that a classname is given.

FBTSTM039E The classname provided (*classname*) was not found in the server's classpath.

Explanation: A classname was provided that does not exist in the server's classpath.

System action: The operation was halted.

Administrator response: Ensure that the given class exists in the server's classpath.

FBTSTM041E The classname provided (*classname*) does not implement the required interface for modules.

Explanation: The classname provided exists but does not implement the required interface for modules.

System action: The operation was halted.

Administrator response: Ensure that the classname provided implements the required interface for modules.

FBTSTM042E The classname provided (*classname*) does not implement the expected model.

Explanation: The classname provided does not have a no-argument public constructor.

System action: The operation was halted.

Administrator response: Ensure that the classname provided includes a no-argument public constructor.

FBTSTM043E The given unique identifier (*identifier*) does not exist in the configuration.

Explanation: The given unique identifier does not exist.

System action: The operation was halted.

Administrator response: Ensure that the provided identifier exists in the current configuration.

FBTSTM044E The remove request could not be completed. There must be no references to the object being removed in order for the request to complete.

Explanation: There must be no references to the configuration data being removed.

System action: The operation was halted.

Administrator response: Ensure that the configuration data being removed does not have any references to it.

FBTSTM046E The unique identifier did not match the expected type.

Explanation: The given unique identifier did not match the expected type in the configuration. This error might also mean that the unique identifier did not exist in the configuration.

System action: The operation was halted.

Administrator response: Ensure that the entire unique identifier is for the correct data.

FBTSTM047E A unique identifier must be provided.

Explanation: A unique identifier was not provided.

System action: The operation was halted.

Administrator response: Ensure that a unique identifier is provided.

FBTSTM048E The request type is already in the configuration.

Explanation: The management request to add a new request type was denied because there cannot be duplicate request types in the configuration.

System action: The operation was halted.

Administrator response: Ensure that the request type is not already in the configuration.

FBTSTM049E To add a request type, a request type URI must be provided.

Explanation: A request type URI was not provided and is required.

System action: The operation was halted.

Administrator response: Ensure that a unique request type URI is provided.

FBTSTM050E The mapping type given is not a supported mapping type.

Explanation: Either the mapping type was not given or it did not match one of the supported mapping types.

System action: The operation was halted.

Administrator response: Ensure that the mapping type is one of the supported mapping types.

FBTSTM051E The request-type mapping requested to be modified does not exist.

Explanation: The request-type mapping requested to be modified does not exist in the server's configuration.

System action: The operation was halted.

Administrator response: Ensure that the request type mapping that is being modified exists in the server's configuration.

FBTSTM058E The chain (*chain identifier*) could not be initialized due to errors.

Explanation: The given chain could not be started without errors being returned.

System action: The operation was halted.

Administrator response: Check the trace logs for a more specific error for the given chain.

FBTSTM059E The request failed to process successfully.

Explanation: The given request failed to process successfully. See the server logs for a specific cause of the failure.

System action: The request was halted.

Administrator response: Check the trace logs for a more specific error for the given chain.

FBTSTM060E The module reference ID used in the configuration of module chain ID '*chainId*', (*chainReference*) is not valid. The module reference does not exist.

Explanation: The referenced identifier does not exist.

System action: The module chain will not be available at runtime.

Administrator response: Validate the STS configuration.

FBTSTM061E The module reference used in the configuration of module chain ID '*chainId*', (*referenceId*) is not valid. The module does not exist.

Explanation: The referenced module does not exist.

System action: The module chain will not be available at runtime.

Administrator response: Validate the STS configuration and installed STS plug-ins.

FBTSTM062E The class '*className*' referenced in module chain ID '*chainId*' could not be initialized. The init method did not successfully complete.

Explanation: The module implementation did not successfully initialize.

System action: The module chain will not be available at runtime.

Administrator response: Validate the STS configuration and installed STS plug-ins.

FBTSTM063E The module chain with ID '*id*' could not be created because of an earlier error.

Explanation: The module chain could not be successfully created.

System action: The module chain will not be available at runtime.

Administrator response: Validate the STS configuration and installed STS plug-ins.

FBTSTM064E The module chain with ID '*id*' does not exist.

Explanation: The module chain could not be located in the configuration.

System action: The module chain will not be available at runtime.

Administrator response: Validate the STS configuration and installed STS plug-ins.

FBTSTM065E The input request did not contain any data and cannot be processed.

Explanation: The input request was null or was not provided.

System action: The request cannot be processed.

Administrator response: Validate the configuration of the caller and the input message.

FBTSTM067E The module chain mapping with ID '*id*' references a group that does not exist.

Explanation: The group membership was either not specified or does not exist in the configuration. Modules with the module chain may need information from this group to operate.

System action: The module chain mapping will not be available at runtime.

Administrator response: Validate the STS configuration and installed STS plug-ins.

FBTSTM068W The server encountered an exception while processing a request in validate mode. If the environment has trace enabled, the exception will appear in the trace log.

Explanation: The STS encountered an exception while processing a request in the validate mode. According to specifications, the server must return a status code similar to the following: http://schemas.xmlsoap.org/ws/2005/02/trust/status/invalid. The exception was caught and logged, allowing the server to return the correct message.

System action: The request failed. The server returned an http://schemas.xmlsoap.org/ws/2005/02/trust/status/invalid status message.

Administrator response: Validate the request parameters and retry the operation.

FBTSTM069E The security token service could not create a logger in the given directory (*directory name*) because it is not a directory.

Explanation: The Security Token Service was not able to create a logger in the given directory because it is not a directory.

System action: The logger will not log messages.

Administrator response: Ensure the given directory is a valid directory.

FBTSTM070E The security token service message logger encountered an error and could not log the message.

Explanation: The security token service message logger encountered an error that is preventing it from logging messages.

System action: The logger will not log messages.

Administrator response: Confirm that the system is allocated enough resources and there are no initialization errors.

FBTSTM071E The security token service message logger encountered an error while creating the log file. The error text is: *file name*.

Explanation: The Security Token Service was not able to create a log file because an error occurred.

System action: The logger will not log messages.

Administrator response: Correct the logger name.

FBTSTM072E The security token service message for chain mapping (*Mapping*) failed signature validation.

Explanation: The Security Token Service was not able to validate the signature on the trust message. This may be caused by an incorrect key alias configured for this chain mapping or the SOAP request was modified along the way or the message was not signed by a trusted signer.

System action: The message is rejected.

Administrator response: Verify that the correct key alias is configured and the SOAP message was not modified en route.

FBTSTM073E The security token service is configured to validate signatures for chain mapping (*Mapping*) but the request received was not signed.

Explanation: The Security Token Service was not able to validate the signature on the trust message. Threceived request was not signed.

System action: The message is rejected.

Administrator response: Ensure that the message came from a trusted source and that the message must be signed.

FBTSTS001E The given SAML assertion is not valid yet.

Explanation: The given SAML assertion's NotBefore time has not been reached.

System action: The request has been halted.

Administrator response: Ensure that the server's clock is synchronized with the other server's clocks that it participates with in the secure domain.

FBTSTS002E The given SAML assertion has expired.

Explanation: The given SAML assertion has expired.

System action: The request has been halted.

Administrator response: Ensure that the server's clock is synchronized with the other server's clocks that it participates with in the secure domain.

FBTSTS003E The given SAML assertion token's digital signature is not valid.

Explanation: The given SAML assertion token's digital signature is not valid.

System action: The request has been halted.

Administrator response: Ensure that the assertion token has not been modified after the signing.

FBTSTS004E The given SAML assertion was not signed, a valid signature was expected with the assertion.

Explanation: The given SAML assertion was not signed, a valid signature was expected with the assertion.

System action: The request has been halted.

Administrator response: If signature validation is not required, re-configure the SAML module so it does not verify signatures.

FBTSTS005E Issuing SAML assertion has failed, none of the supported Subject types were present.

Explanation: Issuing SAML assertion has failed, none of the supported Subject types were present.

System action: The request has been halted.

Administrator response: Subject types should be emailAddress, X509SubjectName or WindowsDomainQualifiedName.

FBTSTS006E No audience has been found in the given assertion.

Explanation: An Audience element with valid URI is missing from the AudienceRestrictionCondition element in the assertion xml document.

System action: The request has been halted.

Administrator response: An Audience URI should exist in the request.

FBTSTS007E Issuing SAML assertion has failed, no authentication method was given.

Explanation: The AuthenticationMethod attribute should exist as part of the given assertion AuthenticationStatement element.

System action: The request has been halted.

Administrator response: Ensure that the AuthenticationMethod attribute exists as part of the given assertion AuthenticationStatement element, for example, password, X509-PKI, PGP, etc.

FBTSTS008E Assertion issuer is not configured.

Explanation: An issuer was not configured but assertion signing was configured.

System action: The request has been halted.

Administrator response: If assertion signing is required, an issuer must be configured. Reconfigure this application and re-start the server.

FBTSTS009E Keystore alias is not configured.

Explanation: A keystore alias must be configured if assertion signing or validation is configured.

System action: The request has been halted.

Administrator response: If assertion signing or validation is required, a keystore alias must be configured. Reconfigure this application and restart the server.

FBTSTS010E The Identity Provider [*IDP*] provided a name identifier [*alias*] that could not be mapped to a valid principal name by the Identity Service.

Explanation: The Identity provider's name identifier was not found in the Identity Service.

System action: The request has been halted.

Administrator response: Ensure that the principal is federated.

FBTSTS011E Invalid security token. Claims element was not found.

Explanation: Liberty requires that a valid Claims element must be in the security token.

System action: The request has been halted.

Administrator response: This is an internal error.

FBTSTS012E The Access Manager Java Runtime configuration file is not specified.

Explanation: The path to the Access Manager Java Runtime configuration file is not specified in the STS modules configuration file.

System action: The request has been halted.

Administrator response: If issuing of IVCreds is enabled, ensure that a configuration file location of AM Java Runtime is specified.

FBTSTS013E The digital signature of the given IV-Cred token is invalid.

Explanation: The given IV-Cred token's digital signature is invalid.

System action: The request has been halted.

Administrator response: Ensure that the IV-Cred token has not been modified after the signing.

FBTSTS014E There was an invalid Principal Chain given in the Access Manager credential.

Explanation: The Access Manager credential has a internal structure called Principal Chain which is required for the credential to be a valid credential.

System action: The request has been halted.

Administrator response: This is an internal error.

FBTSTS015E The IV-Cred binary token is invalid or not present.

Explanation: The IV-Cred module requires that a valid BinarySecurityToken element must be in the security token.

System action: The request has been halted.

Administrator response: This is an internal error.

FBTSTS016E A principal name was not provided to create an Access Manager credential.

Explanation: Creating an IV-Cred credential requires a principal name.

System action: The request has been halted.

Administrator response: Provide a principal entity in the request.

FBTSTS017E An Access Manager credential could not be created for the given principal.

Explanation: A principal name was provided that is not valid.

System action: The request has been halted.

Administrator response: Ensure that a valid principal name is provided.

FBTSTS018E Unexpected exception was caught.

Explanation: An unexpected exception was caught.

System action: The request has been halted.

Administrator response: This is an internal error.

FBTSTS019E The audience in the assertion does not match the Service Provider's URI.

Explanation: The audience restriction value in an assertion must match the URI of the Service Provider.

System action: The request has been halted.

Administrator response: Ensure that the application is properly configured.

FBTSTS020E The InResponseTo attribute in the assertion does not match the request ID of an Authentication request.

Explanation: The InResponseTo attribute, if specified, must match an Authentication request.

System action: The request has been halted.

Administrator response: This may be due to an attempt to replay an assertion.

FBTSTS021E The Keystore service is not available for signing or validating assertions.

Explanation: The Keystore service was not started or has encountered an error.

System action: The request has been halted.

Administrator response: Validate the configuration and restart the server.

FBTSTS022E The given Username Token has expired.

Explanation: The given Username Token has expired.

System action: The request has been halted.

Administrator response: Ensure that the server's clock is synchronized with the other server's clocks that it participates with in the secure domain.

FBTSTS023E The given Username token's digital signature is not valid.

Explanation: The given Username token's digital signature is not valid.

System action: The request has been halted.

Administrator response: Ensure that the token has not been modified after the signing.

FBTSTS024E The given same Username token was replayed.

Explanation: The given Username token was verified before and now it is being reused. This server's configuration does not allow Username tokens to be reused.

System action: The request has been halted.

Administrator response: Each Username token has a unique Nonce to protect it from Replay Attack. Check to see whether the token has been cached and re-issued again without refreshing the Nonce.

FBTSTS025E A principal name was not provided to create a Username token.

Explanation: Creating a Username Token requires a Principal name.

System action: The request has been halted.

Administrator response: Provide a Principal entity in the request.

FBTSTS026E The given Username token's digital signature is missing.

Explanation: The given Username token's digital signature is missing.

System action: The request has been halted.

Administrator response: Ensure that the application is properly configured.

FBTSTS027E The expected security token type is missing.

Explanation: The expected security token type is missing.

System action: The request has been halted.

Administrator response: Ensure that the application is properly configured.

FBTSTS028E The given SAML assertion was verified before and now it is being reused. This server's configuration does not allow assertions to be reused.

Explanation: The use-once enforcement has been enabled and the given SAML assertion has been verified before.

System action: The request has been halted.

Administrator response: Ensure assertions are used only once.

FBTSTS030E The Liberty AuthnContext contains unsupported Authentication Context Statement references.

Explanation: Authentication Context Statement references are not supported.

System action: The request has been halted.

Administrator response: Ensure that the sending Service Provider specifies only Authentication Context class references.

FBTSTS031E The Liberty AuthnContext contains an invalid Authentication Context Class reference.

Explanation: The Liberty architecture specifies the valid set of Authentication Context classes. The received AuthnRequest contained a class reference that is not valid.

System action: The request has been halted.

Administrator response: Ensure that the sending Service Provider sends only supported Authentication Context class references.

FBTSTS032E The authentication request requires an authentication method that is not supported.

Explanation: The authentication request specifies authentication class references that must be used to authenticate the principal, but none of these classes are supported by this implementation.

System action: The request has been halted.

Administrator response: Ensure that the sending Service Provider specifies at least one Authentication Context class reference that is supported by this application.

FBTSTS033E The Access Manager Java Runtime configuration file is not specified.

Explanation: The path to the Tivoli Access Manager Java Runtime configuration file is not specified.

System action: The request has been halted.

Administrator response: Ensure a configuration file location for the Tivoli Access Manager Java Runtime is specified.

FBTSTS034E A principal name was not provided with which to create an Access Manager principal.

Explanation: Creating an Access Manager principal requires a principal name.

System action: The request has been halted.

Administrator response: Provide a principal name in the request.

FBTSTS035E The Status Token Module has not been enabled.

Explanation: The configuration key 'status.module.enable' must be present and set to true on every federation where the status token is used.

System action: The request has been halted.

Administrator response: Enable the status module.

FBTSTS036E The IV-Cred token module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'issue' or 'validate'.

FBTSTS037E The IV-Cred token module configuration is missing a required parameter, '*param*'.

Explanation: The specified parameter is required for operation.

System action: The module will not be available at runtime.

Administrator response: Add the specified parameter to the configuration.

FBTSTS038E The token module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'issue' or 'validate'.

FBTSTS039E The specified keystore alias (*alias*) was not found or is not valid.

Explanation: The key service could not find a key with the provided alias or the alias has an invalid type.

System action: The token module will be disabled.

Administrator response: Ensure you have the correct keystore configured.

FBTSTS040E An anonymous principal name is not configured for partner *identity provider*.

Explanation: An assertion was received from the identity provider with a onetime name identifier, but an anonymous principal name is not specified in the configuration for the partner.

System action: The token exchange cannot be performed.

Administrator response: Configure an anonymous principal name for the partner.

FBTSTS041E A username token was not present in the current request.

Explanation: The current request did not contain a user name token for validation.

System action: The token exchange cannot be performed.

Administrator response: Ensure that clients are sending the username token.

FBTSTS042E The input token [*namespace*][*local*] is not a username token and cannot be parsed.

Explanation: The current request did not contain a user name token for validation.

System action: The token exchange cannot be performed.

Administrator response: Ensure that clients are sending the username token.

FBTSTS043E The received message does not contain a created time element.

Explanation: The current request did not contain a created time element, although configuration specifies that it is required.

System action: The token exchange cannot be performed.

Administrator response: If clients do not send the username token or created time, then they must disable lifetime checking.

FBTSTS046E The AppliesTo element is missing from the request or is badly formed.

Explanation: The AppliesTo element is missing from the request or is badly formed.

System action: The request has been halted.

Administrator response: Ensure the configuration is correct.

FBTSTS047E None of the requested authentication context requirements can be met.

Explanation: The authentication request contained one or more authentication contexts whose requirements cannot be met by the identity provider.

System action: The request has been halted.

Administrator response: Ensure the configuration is correct.

FBTSTS048E The attribute profile specified in the request is not supported.

Explanation: The request specified an attribute profile that is not supported by the identity provider.

System action: The request has been halted.

Administrator response: Ensure the configuration is correct.

FBTSTS049E The Attribute in the request contained an unexpected content for the name or the value.

Explanation: The request specified an attribute that is not supported by the identity provider.

System action: The request has been halted.

Administrator response: Ensure the configuration is correct.

FBTSTS050E A Keystore alias is not configured for encryption.

Explanation: A keystore alias must be configured if encryption is to be used.

System action: The request has been halted.

Administrator response: An encryption keystore alias is required for sending or receiving encrypted elements. Reconfigure this application and re-start the server.

FBTSTS051E The Assertion does not contain a valid recipient or the bearer subject confirmation is missing.

Explanation: The Subject in the assertion must contain a bearer subject confirmation with a recipient value that matches the Assertion Consumer service endpoint of the Service Provider.

System action: The request has been halted.

Administrator response: Ensure that the identity provider conforms with the SAML 2.0 SSO profile.

FBTSTS052E A Keystore alias is not configured for decryption and the assertion is encrypted or contains encrypted elements.

Explanation: A keystore alias must be configured in order to process encrypted assertion elements.

System action: The request has been halted.

Administrator response: An decryption keystore alias is required for receiving encrypted elements. Reconfigure this application and re-start the server.

FBTSTS053W A Keystore alias is not configured for encryption. Attribute *attrname* will not be encrypted.

Explanation: The mapping rule has indicated a preference for encrypting an attribute, but a keystore alias has not been configured for encryption.

System action: The request for encryption is ignored.

Administrator response: An encryption keystore alias is required for sending or receiving encrypted elements. Reconfigure this application and re-start the server.

FBTSTS054E An unrecognized SAML Condition element has been found in the Assertion: [*Element*].

Explanation: The Assertion state is indeterminate because of an unrecognized Condition element.

System action: The request has been halted.

Administrator response: Ensure that the federation is properly configured.

FBTSTS055E Validation of the digital signature on the given element failed.

Explanation: The validation of the digital signature on the given element failed. Either the signature is corrupted or the wrong validation key was used.

System action: The STS request fails and returns an error.

Administrator response: Determine whether the cause of the failure is a corrupted signature or invalid key, fix the problem, and regenerate the request.

FBTSTS056E A valid JAAS principal was not found.

Explanation: A valid JAAS principal was not found.

System action: The request fails; the system returns an error.

Administrator response: Determine the reason why the requestor is not authenticated to WebSphere, fix the problem, then try again.

FBTSTS057E Generation of the binary security token failed.

Explanation: The STS failed to issue a binary security token.

System action: The request fails; the system returns an error

Administrator response: Check the logs to determine the cause of the failure, fix the problem, and try again.

FBTSTS058E An error occurred validating the attributes of the RequestSecurityToken.

Explanation: An error occurred validating the attributes of the RequestSecurityToken.

System action: The request fails; the system returns an error

Administrator response: Check the logs for the cause of the error, fix the problem, and try again.

FBTSTS059E The required parameter DSIG.VerificationKeyIdentifier was not found.

Explanation: The required parameter DSIG.VerificationKeyIdentifier was not found.

System action: The request fails; the system returns an error.

Administrator response: Ensure that the parameter is set correctly and try again.

FBTSTS060E The protected object name for the web service is not specified.

Explanation: The protected object name configuration parameter has not been specified.

System action: The request has been halted.

Administrator response: Ensure a protected object name configuration parameter is specified.

FBTSTS062E JAAS authentication for user *insert* **failed.**

Explanation: The system failed to authenticate the given user through JAAS.

System action: The request has been halted.

Administrator response: Ensure that the user's credentials are valid and resubmit the request.

FBTSTS063E The X.509 security token is missing or is not valid.

Explanation: The X.509 security token to be validated is either missing or is not valid.

System action: The request has been halted.

Administrator response: Ensure that the X.509 security token is valid and resubmit the request.

FBTSTS064E The X.509 certificate path is not valid.

Explanation: The X.509 certificate path for the certificate or certificates, contained within the security token, is not valid.

System action: The request has been halted.

Administrator response: Ensure that the X.509 security token is valid and resubmit the request.

FBTSTS065E The Kerberos security token is missing or is not valid.

Explanation: The Kerberos security token to be validated is either missing or is not valid.

System action: The request has been halted.

Administrator response: Ensure that the Kerberos security token is valid and resubmit the request.

FBTSTS066E STSUniversalUser has more than one Principal 'name' attribute: *param1* **param2:** *param2*

Explanation: The STSUniversalUser should have only one Principal attribute with the key 'name'. Otherwise, the STSUniversalUser is ambiguous.

System action: The request has been halted.

Administrator response: Ensure that the STSUniversalUser has only one 'name' Principal attribute and resubmit the request.

FBTSTS067E The Kerberos service name is not configured.

Explanation: The Kerberos service name is not configured.

System action: The request has been halted.

Administrator response: Ensure that the Kerberos service name is configured.

FBTSTS068E The signature generation process for the given element has failed.

Explanation: The server attempted to digitally sign something and has failed to do so.

System action: The request has been halted.

Administrator response: Determine the cause of the failure and resubmit the request.

FBTSTS069E The received assertion failed signature verification.

Explanation: The server's attempt to verify an assertion's digital signature has failed.

System action: The request has been halted.

Administrator response: Determine the cause of the failure and resubmit the request.

FBTSTS070E Required assertion signature not found.

Explanation: The assertion was not signed as required.

System action: The request has been halted.

Administrator response: Determine the cause of the failure and resubmit the request.

FBTSTS071W The delegation module was not given any delegate modules at initialization. The module will do nothing when called.

Explanation: The delegation module was placed in a module chain, but was not given any modules for delegation. When this module is invoked, it will do nothing.

System action: No action taken.

Administrator response: Ensure that the module is properly configured by providing it a list of delegate modules.

FBTSTS072E Cannot find module instance with ID *insert*.

Explanation: See message.

System action: No action taken.

Administrator response: Verify the module instance ID exists.

FBTSTS073E The token presented is not an LTPA token.

Explanation: The token presented was not a binary security token and therefore not an LTPA token.

System action: Request fails.

Administrator response: Make sure that the Base in the request contains an LTPA token as a binary security token.

FBTSTS074E The LTPA token is empty.

Explanation: An empty token was presented to the module.

System action: Request fails.

Administrator response: Make sure that the request contains an LTPA Token.

FBTSTS075E Token creation failed.

Explanation: The token could not be created.

System action: Request fails.

Administrator response: Make sure that the correct password was presented for the keys. Otherwise, read the description of the exception that caused this and check the trace log for errors.

FBTSTS076E LTPA Token is invalid.

Explanation: The LTPA token presented for validation is not valid. Extended error information should be available in the exception stack trace.

System action: Request fails.

Administrator response: Make sure that the request contains a valid LTPA token.

FBTSTS077E Validated token information is empty, incorrect keys are the probable reason.

Explanation: The information gathered from the token is empty.

System action: Request fails.

Administrator response: Make sure that the correct keys and password are used for token consumption.

FBTSTS078E The STS Universal User cannot be empty.

Explanation: The STS Universal User document passed into the module was empty.

System action: Request fails.

Administrator response: Make sure that the STS Universal User document presented to the module is not empty.

FBTSTS079E The realm used for token creation is not specified. You must specify a realm in either the configuration or the STS Universal User principal.

Explanation: The realm that was going to be used for token creation was empty. This must be specified in order for the user ID to be created.

System action: Request fails.

Administrator response: Either reconfigure the module to insert a static realm, or specify a realm in the STS Universal User principal.

FBTSTS080E The User ID is not specified. Each token created must have a User ID.

Explanation: No name attribute was specified in the STS Universal User.

System action: Request fails.

Administrator response: Check the STS Universal User document and make sure that a name is specified in the principal.

FBTSTS081E The LTPA token module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'issue', 'exchange' or 'validate'.

FBTSTS082E The password for the keys is not valid.

Explanation: The password configured to decrypt the keys is not valid.

System action: The module will not be available at runtime.

Administrator response: Enter the correct password for the LTPA keys.

FBTSTS083E The public key is not valid.

Explanation: The public key entered is not a valid public key.

System action: The module will not be available at runtime.

Administrator response: Enter a valid public key value.

FBTSTS084E The private key is not valid.

Explanation: The private key entered is not a valid private key.

System action: The module will not be available at runtime.

Administrator response: Enter a valid private key value.

FBTSTS085E The shared key is not valid.

Explanation: The shared key entered is not a valid shared key.

System action: The module will not be available at runtime.

Administrator response: Enter a valid shared key value.

FBTSTS086E The JCE provider specified, '*provider*', does not exist.

Explanation: The JCE provider entered is not a valid provider.

System action: The module will not be available at runtime.

Administrator response: Enter a valid provider, or use the default provider.

FBTSTS087E The algorithm specified, '*algorithm*', does not exist.

Explanation: The algorithm entered is not a valid algorithm.

System action: The module will not be available at runtime.

Administrator response: Enter a valid algorithm, or use the default.

FBTSTS088E The padding specified in the cipher suite, '*padding*', does not exist.

Explanation: The padding entered is not valid.

System action: The module will not be available at runtime.

Administrator response: Enter valid padding, or use the default.

FBTSTS089E The decryption of the token failed. This could be caused by an invalid token, invalid shared key or an invalid password for the key.

Explanation: The decryption of the token failed. This could be caused by a token, shared key, or password that is not valid.

System action: Request fails.

Administrator response: Verify that the LTPA shared key and password are correct.

FBTSTS090E The encryption of the token failed. This could be caused by an invalid token, invalid shared key or an invalid password for the key

Explanation: The encryption of the token failed. This could be caused by a token, shared key, or password that is not valid.

System action: Request fails.

Administrator response: Verify that the LTPA shared key and password are correct.

FBTSTS091E The Version specified in the configuration for issuing a token: '*version*' is not valid. It must be either 1 or 2.

Explanation: The LTPA token version number is not valid.

System action: Request fails.

Administrator response: Verify that the LTPA token being sent to the module is LTPAv1 or LTPAv2.

FBTSTS092E The expiration parameter in the STSUniversalUser not a valid number: '*expiration*'.

Explanation: The LTPA expiration time is not valid. It must be a valid positive integer representing the number of milliseconds since the epoch that this token expires.

System action: Request fails.

Administrator response: Verify that the mapping rule sets the expiration Principal attribute correctly.

FBTSTS093E The LTPA token has expired. Expiration time: '*expiration*'. Current time: '*now*'.

Explanation: The LTPA token has expired.

System action: Request fails.

Administrator response: Verify that the expiration time of the token is valid and that the clock on the system where the token is generated is in sync with the clock on the FIM Runtime.

FBTSTS100E The text block for variable '*variable*' is '*text*', which is not a valid XML node.

Explanation: The variable is being used to add an XML node as a value to an STSUniversalUser; however, the text for that variable is not a valid XML node string.

System action: Conversion of TDI Variable to XML Node fails.

Administrator response: Modify the Tivoli Directory Integrator assembly line to produce valid a XML string for the node value, or use a string value.

FBTSTS101E The assembly line identified by '*al*' could not be executed.

Explanation: The assembly line could not be successfully invoked.

System action: Request fails.

Administrator response: Check the causing exception to determine if this was an assembly line error, or an RMI error invoking the assembly line.

FBTSTS102E The assembly line represented by [Hostname: *hostname* **Port:** *port* **ConfigurationFilename:** *config* **AssemblyLineName:***alname***] cannot be loaded.**

Explanation: The assembly line cannot be loaded. Check that the connection details are correct and that the server is running.

System action: Request fails.

Administrator response: Validate that the Tivoli Directory Integrator connection, configuration and assembly line details are correct, and that the Tivoli Directory Integrator server is running.

FBTSTS105W Invalidating connection to TDI Server *rmiurl***.**

Explanation: The connection to the Tivoli Directory Integrator server has been invalidated due to an exception during a remote operation. This can occur, for example, if the Tivoli Directory Integrator server is restarted.

System action: The server connection will be dropped and a reconnection will be attempted on the next transaction.

Administrator response: No immediate administration intervention is necessary. If this message appears regularly, validate that the Tivoli Directory Integrator server is running correctly and is reachable.

FBTSTS106E The Tivoli Directory Integrator server at hostname *hostname* **and port** *port* **cannot be reached.**

Explanation: The connection to the Tivoli Directory Integrator server cannot be established. This could be an invalid configuration, a networking problem, or an inactive server.

System action: The request will fail.

Administrator response: Check that the Tivoli Directory Integrator server is running and reachable, and that the configuration of the hostname and port for the Tivoli Directory Integrator server is correct.

FBTSTS107W Another thread has detected that the connection to Tivoli Directory Integrator server at hostname *hostname* **and port** *port* **is invalid. One retry for this request will be attempted.**

Explanation: The connection to the Tivoli Directory Integrator server failed, and was detected by another thread while waiting for an available connection.

System action: The request will be retried once.

Administrator response: Check that the Tivoli Directory Integrator server is running and reachable.

FBTSTS108E Too many threads (*numthreads***) were waiting for access to the assembly line: [Hostname:** *hostname* **Port:** *port* **ConfigurationFilename:** *config* **AssemblyLineName:***alname***]**

Explanation: The threshold for the maximum number of waiting threads on the assembly line has been exceeded.

System action: The request will fail, and should be retried later when traffic eases.

Administrator response: Check that the Tivoli Directory Integrator server is functioning normally. It may be necessary to increase the pool size for the assembly line, or increase the maximum number of threads that can wait.

FBTSTS109E A timeout (*timeoutval* **msec) occurred while waiting for a connection to the Tivoli Directory Integrator server for assembly line: [Hostname:** *hostname* **Port:** *port* **ConfigurationFilename:** *config* **AssemblyLineName:***alname***]**

Explanation: The thread was waiting for a connection to the Tivoli Directory Integrator server, and the timeout was reached.

System action: The request will fail, and may be retried later.

Administrator response: Check that the Tivoli Directory Integrator server is functioning normally. It may be necessary to increase the pool size for the assembly line, or increase the maximum timeout.

FBTSTS110E A thread was unexpectedly interrupted while waiting for an assembly line handler for: [Hostname: *hostname* **Port:** *port* **ConfigurationFilename:** *config* **AssemblyLineName:***alname***]**

Explanation: A thread was waiting for an assembly line handler, and was unexpectedly interrupted. This error should not occur.

System action: The request will fail.

Administrator response: Contact IBM Software Support.

FBTSTS120E The TAM GSO module does not operate in the given mode, '*mode***'**

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'map'.

FBTSTS121E The token representing the current user was empty.

Explanation: This indicates an error in the request to the trust service, or a processing error in a previous module in the trust chain.

System action: Request fails.

Administrator response: Validate your trust chain configuration and the request to the trust service.

FBTSTS122E Could not retrieve GSO credentials from Tivoli Access Manager for the GSO resource '*rsrc***' for user '***user***'.**

Explanation: Tivoli Access Manager could not be contacted, or the returned credentials were empty.

System action: Request fails.

Administrator response: Validate that the Tivoli Access Manager policy server is running and that the Tivoli Access Manager user has a matching GSO resource.

FBTSTS123E The Tivoli Access Manager credentials do not contain a username for the GSO resource '*rsrc***' for user '***user***'.**

Explanation: The Tivoli Access Manager configuration is not valid.

System action: Request fails.

Administrator response: Validate that the Tivoli Access Manager GSO credentials for this user are correctly populated.

FBTSTS124E The token representing the current user did not contain a username.

Explanation: This indicates an error in the request to the trust service, or a processing error in a previous module in the trust chain.

System action: Request fails.

Administrator response: Validate your trust chain configuration and the request to the trust service.

FBTSTS125E The configuration for the Tivoli Access Manager GSO resource name is missing.

Explanation: This message indicates a configuration error.

System action: Request fails.

Administrator response: Validate your trust chain configuration.

FBTSTS126E The Access Manager Java Runtime configuration file is not specified or does not exist.

Explanation: The path to the Tivoli Access Manager Java Runtime configuration file is not specified or the file does not exist.

System action: The request has been halted.

Administrator response: Ensure that Tivoli Access Manager Java Runtime is configured for this domain.

FBTSTS130E Invalid security token. Claims element is missing the required attribute '*name***'.**

Explanation: The Claims element must contain the specified attribute or element.

System action: The request has been halted.

Administrator response: This is an internal error.

FBTSTS131E Invalid security token. The Assertion does not contain an AuthnStatement element.

Explanation: The SAML 20 SSO protocol requires the presence of at least one authentication statement (AuthnStatement) element.

System action: The request has been halted.

Administrator response: Ensure that the Identity Provider is compliant with the SAML 2.0 SSO protocol.

FBTSTS132E The SAML STS module was unable to locate the issued assertion.

Explanation: The selection criteria specified to query the issued assertion does not match any of the assertions cached or the assertion has expired.

System action: The request has been halted.

Administrator response: Provide a valid selection criteria.

FBTSTS140E The STSUniversalUser STS module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'issue' or 'validate'.

FBTSTS141E The token passed to the STS module for validation was not an STSUniversalUser token.

Explanation: This indicates the token module has been called in validate mode with a token that is not an STSUniversalUser.

System action: Request fails.

Administrator response: Validate that the client of the trust service is passing the correct token type.

FBTSTS142E The incoming security token did not contain the required browser request claims.

Explanation: An STS module requires BrowserRequestClaims in the incoming security token.

System action: The request has been halted.

Administrator response: Ensure that the STS module requiring the claims is invoked by a protocol that provides the claims.

FBTSTS150E The Access Manager Java Runtime configuration file does not exist.

Explanation: The Tivoli Access Manager Java Runtime configuration file does not exist.

System action: The request has been halted.

Administrator response: Ensure that Tivoli Access Manager Java Runtime is configured for this domain.

FBTSTS151E A Tivoli Access Manager principal name was not provided.

Explanation: An authentication check requires a principal name.

System action: The request has been halted.

Administrator response: Provide a principal name in the STS universal user.

FBTSTS160E The Access Manager Java Runtime configuration file does not exist.

Explanation: The Tivoli Access Manager Java Runtime configuration file does not exist.

System action: The request has been halted.

Administrator response: Ensure that Tivoli Access Manager Java Runtime is configured for this domain.

FBTSTS161E A Tivoli Access Manager principal name was not provided.

Explanation: An authorization check requires a principal name.

System action: The request has been halted.

Administrator response: Provide a principal name in the STS universal user.

FBTSTS162E A Tivoli Access Manager protected object name was not provided.

Explanation: An authorization check requires a protected object name.

System action: The request has been halted.

Administrator response: Provide a protected object name in the STS universal user.

FBTSTS163E A Tivoli Access Manager action was not provided.

Explanation: An authorization check requires an action.

System action: The request has been halted.

Administrator response: Provide an action in the STS universal user.

FBTSTS165E The LTPA token configuration is missing the required secret shared key.

Explanation: The LTPA token requires a secret shared key to be able to encrypt or decrypt LTPA tokens.

System action: Request fails.

Administrator response: Verify that the secret shared key was given for the LTPA token module. Also, verify that there wasn't an error during startup when initializing the LTPA token module's configuration.

FBTSTS166E The LTPA token configuration is missing the required public key.

Explanation: The LTPA token requires a public key to be able to validate LTPA tokens.

System action: Request fails.

Administrator response: Verify that the public key was given for the LTPA token module. Also, verify that there wasn't an error during startup when initializing the LTPA token module's configuration.

FBTSTS167E The LTPA token configuration is missing the required private key.

Explanation: The LTPA token requires a private key to be able to issue LTPA tokens.

System action: Request fails.

Administrator response: Verify that the private` key was given for the LTPA token module. Also, verify that there wasn't an error during startup when initializing the LTPA token module's configuration.

FBTSTS168E The LTPA token configuration validation failed.

Explanation: The LTPA token configuration validation failed.

System action: Request fails.

Administrator response: Verify that the configuration for the LTPA module is correct. Also, examine the system log for any reported exceptions.

FBTSTS180E The mapping extension utility function *fnc* failed.

Explanation: The mapping extension utility function failed, and the error message should contain a caused-by exception which explains the root cause.

System action: Request fails.

Administrator response: Examine the system log for the reported root-cause exception.

FBTSTS181E WebSphere Registry authentication for user *insert* failed.

Explanation: The system failed to authenticate the given user through the WebSphere Registry.

System action: The request has been halted.

Administrator response: Ensure that the user's credentials are valid and resubmit the request.

FBTSTS190E The Kerberos realm name is missing or invalid.

Explanation: The Kerberos realm name is missing or invalid.

System action: The request has been halted.

Administrator response: Ensure that the Kerberos realm name is present in the STS universal user by defining the appropriate mapping rule.

FBTSTS191E The Kerberos client name is missing or invalid.

Explanation: The Kerberos client name is missing or invalid.

System action: The request has been halted.

Administrator response: Ensure that the Kerberos client name is present in the STS universal user by defining the appropriate mapping rule.

FBTSTS192E The Kerberos client password is missing or invalid.

Explanation: The Kerberos client password is missing or invalid.

System action: The request has been halted.

Administrator response: Ensure that the Kerberos client password is present in the STS universal user by defining the appropriate mapping rule.

FBTSTS193E The Kerberos service name is missing or invalid.

Explanation: The Kerberos service name is missing or invalid.

System action: The request has been halted.

Administrator response: Ensure that a mapping rule the Kerberos service name is present in the STS universal user by defining the appropriate mapping rule.

FBTSTS200E The KESS STS module does not operate in the given mode, '*mode*'

Explanation: The configured mode is invalid.

System action: The module is not available at runtime.

Administrator response: Change the operation mode to 'map'.

FBTSTS201E The KESS STS token configuration is not valid for a required parameter: '*param*'. Value: '*value*'

Explanation: The KESS STS token module has been configured with an invalid option.

System action: Request fails.

Administrator response: Verify that the configuration for the token module contains the required parameters for the operation.

FBTSTS202E The STSUniversalToken is missing the required 'ElementID' Context Attribute.

Explanation: When performing signing operations, the STSUniversalUser must contain a Context Attribute called 'ElementID'. This attribute must have a value that matches the value of a reference attribute in the element to sign.

System action: Request fails.

Administrator response: Verify that the STSUniversalUser processed by this module contains a Context Attribute called 'ElementID'. Verify that value of the attribute matches the value of a reference attribute that can be signed.

FBTSTS203E The KESS STS Module cannot determine a node to sign from the attribute: '*attrname*'.

Explanation: The STSUniversalUser attribute did not contain a node value that the KESS STS module can sign.

System action: Request fails.

Administrator response: Verify that the STSUniversalUser processed by this module contains a node value in the configured attribute that can be signed.

FBTSTS204E The KESS STS Module failed to validate a signature for XML: '*xml*'.

Explanation: The KESS STS Module cannot complete the signing operation because the signature is invalid.

System action: Request fails.

Administrator response: Verify that the client is sending XML with a valid signature and that KESS contains a matching signature validation key.

FBTSTS205E The KESS STS Module cannot determine a node to validate from the attribute: '*attrname*'.

Explanation: The KESS STS module cannot validate the signature because the STSUniversalUser attribute containes an invalid node value.

System action: Request fails.

Administrator response: Verify that the STSUniversalUser processed by this module contains a node value in the configured attribute that can be validated.

FBTSTS206E The KESS STS Module cannot determine a node to encrypt from the attribute: '*attrname*'.

Explanation: The KESS STS module cannot complete the encryption operation because the STSUniversalUser attribute contains a node value that cannot be encrypted.

System action: Request fails.

Administrator response: Verify that the STSUniversalUser processed by this module contains a node value in the configured attribute that can be encrypted.

FBTSTS207E The KESS STS Module cannot determine a node to decrypt from the attribute: '*attrname*'.

Explanation: The KESS STS module cannot complete the decryption operation because the STSUniversalUser attribute contains a node value that cannot be decrypted.

System action: Request fails.

Administrator response: Verify that the STSUniversalUser processed by this module contains a node value in the configured attribute that can be decrypted.

FBTSTS208E The Default Map Module could not determine mapping rule type.

Explanation: The Default Map Module cannot determine the rule type based on the configuration.

System action: Identity mapping fails.

Administrator response: Verify that the default mapping module is configured correctly.

FBTSTS220E The SAML Attribute Query STS module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module will not be available at runtime.

Administrator response: Change the operation mode to 'map'.

FBTSTS221E The SAML Attribute Query STS module could not find an assertion on the attribute query saml response.

Explanation: The attribute authority did not returned an assertion on the saml response.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS222E The SAML Attribute Query STS module could parse the assertion from the attribute query saml response.

Explanation: The SAML attribute query sts module was not able to parse the assertion on the saml response.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS223E The SAML Attribute Query STS module could not validate the xml digital signature.

Explanation: The SAML attribute query sts module was not able to validate the xml digital signature.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS224E The SAML Attribute Query STS module signature validation key is not properly configured.

Explanation: The SAML attribute query sts module signature validation key is not properly configured.

System action: Request fails.

Administrator response: Verify that the validation key is configured on the partner configuration.

FBTSTS225E The SAML Attribute Query STS module could not get the saml response from the soap envelope.

Explanation: The SAML attribute query sts module could not get the saml response from the soap envelope.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS226E The assertion included on the SAML Attribute Query SAML Response is not signed. This module is configure to reject unsigned assertions.

Explanation: The SAML attribute query sts module expects the assertion to be signed.

System action: Request fails.

Administrator response: Verify the configuration and modify the settings to make assertion signature optional.

FBTSTS227E The SAML Attribute Query STS module could not parse the saml response.

Explanation: The SAML attribute query sts module could not parse the saml response.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS228E The SAML Attribute Query STS module could not decrypt the xml message.

Explanation: The SAML attribute query sts module was not able to decrypt the xml message.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS229E The SAML Attribute Query STS module decryption key is not properly configured.

Explanation: The SAML attribute query sts module decryption key is not properly configured.

System action: Request fails.

Administrator response: Verify that the validation key is configured on the partner configuration.

FBTSTS230E The SAML Attribute Query SAML Response is not signed. This module is configure to reject unsigned saml response.

Explanation: The SAML attribute query sts module expects the saml response to be signed.

System action: Request fails.

Administrator response: Verify the configuration and modify the settings to make saml response signature optional.

FBTSTS231E The SAML Attribute Query STS module could not sign the attribute query xml message.

Explanation: The SAML attribute query sts module was not able to sign the attribute query xml message.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS232E The SAML Attribute Query STS module could not create the attribute query xml message.

Explanation: The SAML attribute query sts module could not create the attribute query xml message.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS233E The SAML Attribute Query STS module was not able to send the attribute query xml message.

Explanation: The SAML attribute query sts module could not send the attribute query xml message to the attribute authority.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS234E The SAML Attribute Query STS module was not able to obtain the user principal name.

Explanation: The SAML attribute query sts module could not obtain the user principal name.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Verify that the mapping module is setting the universal user values properly.

FBTSTS235E The SAML Attribute Query STS module was not able to obtain the partner alias from the alias service.

Explanation: The SAML attribute query sts module could not obtain the partner alias from the alias service.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS236E The SAML Attribute Query STS module received an invalid saml response.

Explanation: The saml response received by the SAML attribute query sts module is not valid.

System action: Request fails.

Administrator response: Verify that the configuration is correct. Also, examine the system log for any reported exceptions.

FBTSTS237E The response message InResponseTo attribute does not correlate to the pending request ID attribute.

Explanation: The response message contains an InResponseTo attribute that does not match the ID attribute of the pending request. It is possible that the response was received in error.

System action: The operation will be halted.

Administrator response: If the response is legitimate, examine the trace logs to see why the InResponseTo attribute does not match the ID attribute of the currently pending request.

FBTSTS238E The timestamp in the SAML message is out of range. The message timestamp, *msgTime*, is not within *tolerance* seconds of *compareTime*.

Explanation: The SAML message has a timestamp that is not valid.

System action: The message will be ignored.

Administrator response: There are several reasons that a SAML message timestamp might be out of range: The clocks on the communicating providers systems are skewed beyond the acceptable tolerance, network delays are hampering message flow, or the acceptable tolerance for message timestamp is set too low. The administrator should check these points and make any necessary adjustments.

FBTSTS239E Cannot determine the SAML status.

Explanation: The SAML status attribute is required for this message and cannot be determined.

System action: The operation will be halted.

Administrator response: Examine the trace logs to see why the SAML status was not set.

FBTSTS240E The attribute query request failed at the attribute authority.

Explanation: The SAML status included in the saml response message indicates that the request failed at the attribute authority.

System action: The operation will be halted.

Administrator response: Examine the trace logs at the attribute authority or the saml response to see why the request operation failed.

FBTSTS241E The SAML Attribute Query STS token configuration is not valid for a required parameter: '*param*'. Value: '*value*'

Explanation: The SAML Attribute Query STS token module has been configured with an invalid option.

System action: Request fails.

Administrator response: Verify that the configuration for the token module contains the required parameters for the operation.

FBTSTS242E The SAML Attribute Query STS token configuration is not valid for a required parameter: '*param*'. Value: '*value*' is out of range. Minimum value: '*value*' Maximum Value: '*value*'

Explanation: The SAML Attribute Query STS token module has been configured with an invalid option.

System action: Request fails.

Administrator response: Verify that the configuration for the token module contains the required parameters for the operation.

FBTSTS260E The OAuth validation request for token type: '*type*' failed.

Explanation: The OAuth validation request failed because the syntax of the request message or the parameters is not valid.

System action: The request is rejected.

Administrator response: Ensure that the request message and the parameters have the correct syntax.

FBTSTS261E The OAuth token type: '*type*' cannot be created.

Explanation: The OAuth server cannot issue an OAuth token for the requested token type.

System action: The OAuth token request is rejected.

Administrator response: Check the trace logs to determine the cause of the error.

FBTSTS262E The OAuth server failed to authorize the OAuth token: '*token*' and user name: '*username*'.

Explanation: The OAuth server cannot generate a verification code.

System action: The authorization of the client is rejected.

Administrator response: Check the trace logs to determine the cause of the error.

FBTSTS263E The validation for the OAuth token: '*token*' failed.

Explanation: The OAuth server cannot validate the token.

System action: The token validation fails.

Administrator response: Check the trace logs to determine the cause of the error.

FBTSTS265E The token type:'*type*' that was received is not valid.

Explanation: The token type value is not recognized.

System action: The request is rejected.

Administrator response: Ensure that the token type sent to the OAuth server is valid.

FBTSTS266E The STSUU token passed to the STS does not have the required parameter:'*param*'.

Explanation: The STSUU token sent to the server does not have all the required parameters.

System action: The request is rejected.

Administrator response: Check the trace log to see which parameter is not present and to determine the cause of the error.

FBTSTS268E The configuration value for the parameter: '*param*' is not valid. The value found was: '*value*'. The default value '*default value*' is used instead.

Explanation: The value of the configuration parameter is not valid.

System action: The operation stops.

Administrator response: Ensure that the configuration parameter type is correct and that the value is valid.

FBTSTS269E An OAuth parameter with the name: '*param*' already exists.

Explanation: There is a duplicate parameter in the request.

System action: The request is rejected.

Administrator response: Ensure that there are no duplicate parameters in the request message.

FBTSTS270E The OAuth token with lookup: '*token string*' and type: '*type*' cannot be found.

Explanation: The token for the given token type does not exist in the cache.

System action: The request is rejected.

Administrator response: Ensure that the token is valid and is mapped to the token type.

FBTSTS271E Invalid STS mode: '*mode*'.

Explanation: The STS mode is not mapped to the STS module.

System action: The request is halted.

Administrator response: Ensure that the STS module is configured with the correct mode.

FBTSTS272E A two-legged OAuth request from client: '*client identifier*' failed.

Explanation: The OAuth server is not configured to accept two-legged OAuth requests.

System action: The request is rejected.

Administrator response: Ensure that two-legged OAuth is enabled at the OAuth server.

FBTSTS273E The OAuth client with identifier: '*client identifier*' cannot be found.

Explanation: The client identifier in the request does not match any registered client or the client is disabled at the OAuth server.

System action: The request is rejected.

Administrator response: Ensure that the client is valid and is registered correctly.

FBTSTS290E Invalid STS mode: '*mode*'.

Explanation: The STS mode is not mapped to the STS module.

System action: The request is halted

Administrator response: Ensure that the STS module is configured with the correct mode.

FBTSTS292E The OAuth 2.0 request type: '*request_type*' is not valid.

Explanation: The value of the request_type parameter is not valid.

System action: The operation stops.

Administrator response: Ensure your OAuth 2.0 enforcement point is providing the correct value for this parameter, or no value at all.

FBTSTS293E The OAuth 2.0 token module request failed due to the following exception: '*name*'.

Explanation: An internal exception caused the request to stop.

System action: The operation stops.

Administrator response: Check the exception that caused this error.

FBTSTZ001E The Keystore service is not available for generating, signing, or validating RACF PassTicket Tokens.

Explanation: Internal Error:The Keystore service could not be accessed.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTSTZ002E RACF PassTicket Processing Failed! SAF rc=*VALUE_0*, RACF rc=*VALUE_1*, RACF reason code=*VALUE_2*.

Explanation: RACF returned an error while processing a PassTicket.

System action: The request has been halted.

Administrator response: Refer to the z/OS Security Server RACF Messages and Codes for more information on the SAF/RACF return and reason codes.

FBTSTZ003E The value provided is not a valid PassTicket.

Explanation: The given Username token's password was not a valid PassTicket.

System action: The request has been halted.

Administrator response: Ensure the defined Username token's password was generated by a standard PassTicket generator with the correct secret key for the specified user ID and configured application name.

FBTSTZ004E The PassTicket cannot be validated for the user ID <*VALUE_0*>, application name <*VALUE_1*>, and key profile <*VALUE_2*>.

Explanation: The given PassTicket does not validate for the given user ID, application name, and secret key.

System action: The request has been halted.

Administrator response: Ensure the defined Username token's password was generated by a standard PassTicket generator with the correct secret key for the specified user ID and configured application name.

FBTSTZ005E The specified user ID <*VALUE_0*>, application name <*VALUE_1*>, and/or key profile <*VALUE_2*>, do not meet the minimal PassTicket requirements.

Explanation: The configuration and/or the Username token's username do not meet the PassTicket requirements.

System action: The request has been halted.

Administrator response: Validate the configuration and ensure the user ID and application name satisfy PassTicket requirements.

FBTSTZ006E An encryption error occurred during PassTicket processing.

Explanation: Internal Error: An error was encountered during the encryption phase of PassTicket processing.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTSTZ007E An unknown error occurred during PassTicket processing.

Explanation: Internal Error: An unknown internal error was encountered.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTSTZ008E The value specified for encryption and decryption of PassTickets was invalid. The value specified must be exactly sixteen characters long and should contain only hexadecimal digits 0-9 and a-f. Please reconfigure your PassTicket module specifying a valid key.

Explanation: The PassTicket module requires that an administrator specify a DES key as sixteen hexadecimal digits. The administrator failed to do so.

System action: The request has been halted.

Administrator response: Use the console to reconfigure the PassTicket module, specifying an appropriate encryption key.

FBTTAC003E An error occurred when reading or writing the file *file name***:\n***error text***\n**

Explanation: An error occurred when either reading or writing a file. The error text contains additional information about the error.

System action: If the file is a non-critical file, the tool will attempt to proceed. If the file is critical to the operation being performed, the tool will exit.

Administrator response: Attempt to resolve the problem described by the error text. Verify that the file exists. If the error occurs because the tool does not have permission to modify the file, verify the file is writable.

FBTTAC004E Unable to understand file *file name***, line** *line number***.\n The text** *invalid line from stanza file* **is not valid.\n**

Explanation: An error occurred when interpreting a stanza file. The file format does not appear to be correct.

System action: The file will not be read. The tool will exit.

Administrator response: The most likely cause of this error is that the file specified is not a Security Access Manager stanza file. Verify that the file specified is the correct file to use. If necessary, refer to the documentation for examples of how to use the autoconfiguration tool.

FBTTAC005E Unable to connect to host *host name or IP address***, port** *TCP port number***:\n***error text***\n**

Explanation: The tfimcfg tool tried to create a TCP connection to the server and port specified. The connection failed.

System action: The action taken depends on what connection failed. In some cases, the connection will be retried or the configuration will continue even though the connection failed. In other cases, the configuration will stop. Subsequent messages will explain what action is being taken.

Administrator response: The administrative response depends on which TCP connection failed and for what reasons. As a general rule, the administrator should verify connectivity to the machine to which the connection failed. Administrators should also verify that they entered the correct hostname and port information if they were prompted to do so.

FBTTAC006W Please verify the WebSEAL server is running.\n

Explanation: The WebSEAL server does not appear to be running, so the autoconfiguration cannot proceed.

System action: The autoconfiguration tool will exit without modifying any configuration.

Administrator response: Start the WebSEAL server. If the WebSEAL server is already running, verify that the configuration file specified is correct.

FBTTAC007E The file *file name* indicates that\n PDJrte has not been fully configured for your Java runtime. Please configure\n the PDJrte in 'full' mode before running the Security Access Manager autoconfiguration tool.\n

Explanation: The Security Access Manager autoconfiguration tool requires that the PDJrte package be fully configured before the tool is run.

System action: The autoconfiguration tool will exit without modifying any configuration.

Administrator response: Use the pdconfig program to configure the PDJrte in 'full' mode, and then rerun the Security Access Manager autoconfiguration tool.

FBTTAC008W The stanza entry [*stanza name*]*entry name* was not found.\n

Explanation: The Security Access Manager autoconfiguration tool checked for but did not find the configuration file entry described in the message.

System action: If it is possible to proceed without that configuration entry, the autoconfiguration tool will do so. Otherwise the tool will exit.

Administrator response: Verify that the configuration file specified to the autoconfiguration tool belongs to a configured WebSEAL server.

FBTTAC011W The value *property name* was not specified in the response file.\n

Explanation: The Security Access Manager autoconfiguration tool checked for but did not find the response file entry described in the message.

System action: If it is possible to proceed without the response file entry, the autoconfiguration tool will do so. Otherwise the tool will exit.

Administrator response: If the configuration proceeds, no action is necessary. If the configuration fails, attempt an interactive configuration by omitting the '-rspfile' option.

FBTTAC015E An unexpected error occurred:\n*exception text*:\n*exception stack trace*\n

Explanation: Most error conditions are handled automatically by the autoconfiguration tool. This messages means an unexpected error occurred, and could not be handled automatically.

System action: The autoconfiguration tool will give the administrator an opportunity to make different selections for the configuration.

Administrator response: Attempt to diagnose the cause of the error based on the exception text. If possible, choose different configuration options.

FBTTAC019E None of the endpoints for this federation are handled by this WebSEAL server. Configuration cannot continue. Federation endpoint URLs:

Explanation: The tool examined the URLs hosted by this WebSEAL server and the URLs used by the federation specified. None of the URLs for the federation are intended for this WebSEAL server. The message is followed by a list of endpoints for the federation.

System action: The autoconfiguration tool will give the administrator an opportunity to choose a different federation to configure.

Administrator response: Make sure that you have configured your WebSEAL server to specify on the appropriate hostnames and port number for the federation you are configuring.

FBTTAC022E No capabilities are configured on this WebSEAL server.\n

Explanation: The tool checked for federations or capabilities that had been configured on this WebSEAL server, and there were none.

System action: The autoconfiguration tool will do nothing.

Administrator response: No administrative response is necessary unless the administrator wishes to configure federation information that was not detected by the autoconfiguration tool. In that case, the unconfiguration should be performed manually.

FBTTAC034E The group *group name* exists in the registry but has not been imported into Security Access Manager.\n

Explanation: The group specified exists in the user registry, but has not been imported into Security Access Manager.

System action: The autoconfiguration tool will prompt the administrator to select a different group.

Administrator response: The administrator should either use a different group, or else use pdadmin or WPM to import the user into Security Access Manager.

FBTTAC035E Unable to determine junction point for endpoint URL *URL*\n You may need to manually create a junction for that endpoint.\n

Explanation: The federation uses an endpoint that would require a junction / on the WebSEAL server. The autoconfiguration tool cannot create that junction.

System action: The autoconfiguration tool will skip creating that junction.

Administrator response: The administrator should either reconfigure their federation to use a different endpoint, or else manually create the / junction.

FBTTAC045E Error creating ACL *acl name* **and attaching it\n to** *object name*: *exception message***\n**

Explanation: An error occurred in the process of creating and attaching an ACL.

System action: The autoconfiguration tool will continue with the configuration.

Administrator response: The administrator may attempt to diagnose the error condition and fix the problem, or they may create the ACL manually.

FBTTAC046E Junction creation failed with error code *error code***.\n**

Explanation: An error occurred in the process of creating a junction. Other messages may have more information on the root cause of the problem.

System action: The autoconfiguration tool will continue with the configuration.

Administrator response: The administrator may attempt to diagnose the error condition and fix the problem, or they may create the junction manually.

FBTTAC047E Junction creation failed.\n

Explanation: An error occurred in the process of creating a junction. Other messages may have more information on the root cause of the problem.

System action: The autoconfiguration tool will continue with the configuration.

Administrator response: The administrator may attempt to diagnose the error condition and fix the problem, or they may create the junction manually.

FBTTAC048W Unable to locate the *library name* **library.\n Using default library** *library name***.\n**

Explanation: The autoconfiguration tool could not find a library.

System action: The autoconfiguration tool will continue with the configuration, inserting a standard library path for the library location. The WebSEAL server may fail to start properly after the configuration is done.

Administrator response: If WebSEAL does not start after the configuration is complete, the administrator should check the WebSEAL log file to verify the problem is the library name, and then specify the correct name in the WebSEAL configuration file.

FBTTAC049W Error interpreting federation endpoint '*endpoint type***', URL** *url***:\n** *exception text***\n**

Explanation: The autoconfiguration tool could not interpret a URL associated with the federation.

System action: The autoconfiguration tool will continue with the configuration, ignoring the malformed URL.

Administrator response: The administrator may need to perform manual configuration for the endpoint.

FBTTAC054E Error connecting to *url***:\n***exception text***\n**

Explanation: The autoconfiguration tool could not connect to a URL.

System action: The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response: The administrator should correct the URL.

FBTTAC055E The URL *url* **does not appear to connect to a Web server.\n**

Explanation: The autoconfiguration tool could not connect to a URL.

System action: The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response: The administrator should correct the URL.

FBTTAC056E The request to the Web server failed. Response: *http error code http status message***:\n Response text:\n \n** *text from web server***:\n \n \n**

Explanation: The Web server returned an error for an HTTP request.

System action: The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response: The administrator may need to update the Web server configuration to fix the problem.

FBTTAC057W Warning: the URL *url* **appears to connect directly to WebSphere. For better performance and stability, connecting to a Web server running the WebSphere Web server plug-in is recommended.**

Explanation: The administrator specified a URL that connects directly to WebSphere, which is not a recommended configuration.

System action: The autoconfiguration tool will prompt the administrator to correct the URL.

Administrator response: The administrator may need to update the Web server configuration to fix the problem.

FBTTAC059E No federations were returned from the Security Access Manager InfoService.\n Response body:\n\n *response text* **\n**

Explanation: The Federated Identity Manager InfoService did not return any federations.

System action: The autoconfiguration tool will prompt the administrator to correct the URL for the InfoService.

Administrator response: The administrator should make sure that federations have been configured on the Federated Identity Manager server. It may be necessary to restart the WebSphere server if the configuration has been changed recently.

FBTTAC081E Unable to create Security Access Manager administration context.\n

Explanation: An error occurred creating the Security Access Manager administration context. Other error messages with more detail may be displayed.

System action: The autoconfiguration tool will give the administrator an opportunity to specify a different Security Access Manager user-id ans password.

Administrator response: Attempt to diagnose the cause of the error based on the other error messages. Verify the administrator user-id and password are correct.

FBTTAC087E ACL deletion failed:\n*error messages***\n.**

Explanation: An error occurred in the process of deleting an ACL. Other messages may have more information on the root cause of the problem.

System action: The autoconfiguration tool will continue with the unconfiguration.

Administrator response: The administrator should delete the junction manually.

FBTTAC088E Attribute deletion failed:\n*error messages***\n.**

Explanation: An error occurred in the process of deleting extended attributes from an object. Other messages may have more information on the root cause of the problem.

System action: The autoconfiguration tool will continue with the unconfiguration.

Administrator response: The administrator should delete the attributes manually.

FBTTAC098E An error occurred when restarting the WebSEAL server. Please check\n the log file *log file* **to diagnose and fix the problem.\n**

Explanation: The configuration tool tried to restart WebSEAL, but the server did not start.

System action: The autoconfiguration tool will not proceed until the WebSEAL server is operational.

Administrator response: The administrator should check the WebSEAL log file and correct the problem.

FBTTAC101W An error occurred when executing the command *command***:\n** *exception text***\n**

Explanation: Executing a command failed.

System action: The action taken depends on which command failed, and for what reasons.

Administrator response: No response is necessary unless other problems occur.

FBTTAC102E The Security Access Manager policy server was unable to modify an\n entry in the user registry because of insufficient access rights. You may\n need to update the ACLs applied to your user registry to grant the policy\n server access. The error message from the policy server was:\n *Security Access Manager error messages***\n**

Explanation: An attempt to create a user or group failed, and the error message from the Security Access Manager policy server indicates that the problem is due to insufficient LDAP access rights.

System action: The user or group will not be created. If the user or group is not critical, the remainder of the configuration will proceed.

Administrator response: Refer to the Security Access Manager documentation on applying Security Access Manager ACLs to new LDAP suffixes for additional information on how to correct the LDAP ACLs.

FBTTAC111W The Web server did not provide a CA certificate for the SSL handshake. You will need to contact the Web server administrator to obtain the CA certificate. Once you have obtained the CA certificate, add it to the WebSEAL key database manually.

Explanation: The fimtamcfg tool attempts to download the CA certificate from the Web server, since many Web servers include the CA certificate as part of the SSL handshake. The CA certificate was not included in the SSL handshake, so the administrator will need to obtain the certificate through other means.

System action: The configuration will continue without the CA certificate, but the junction from WebSEAL to the application server will not function correctly until WebSEAL has the CA certificate.

Administrator response: Refer to the message for instructions on how to resolve this problem. For assistance with adding the CA certificate to the WebSEAL key database, refer to the WebSEAL administration guide chapters discussing SSL and GSKit.

FBTTAC113E Unable to convert key database *file name* **from .kdb format to .jks format. The gsk7cmd program returned error code** *numeric error code***.***log data*

Explanation: The fimtamcfg tool attempts to convert the WebSEAL key database from .kdb format to .jks (Java Key Store) format. This conversion failed with the specified error code and error text.

System action: The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response: Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC114E Unable to add the certificate *cert file* **to the key database** *file name***. The gsk7cmd program returned error code** *numeric error code***.***log data*

Explanation: The fimtamcfg tool attempts to add a Web server's CA certificate to the WebSEAL key database. This process failed with the specified error code and error text.

System action: The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response: Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC117E The values provided in the response file for the SSL certificate did not match the values presented by the SSL server. Invalid value: *Certificate DN or fingerprint* **Configuration cannot continue.**

Explanation: The fimtamcfg tool checks the certificate presented by an SSL partner against the expected values recorded in a response file from previous configurations. The certificates did not match.

System action: The fimtamcfg tool will not continue configuration until the partner's certificate can be validated.

Administrator response: The administrator should make sure that the values they have provided for the Security Access Manager hostname and port are correct. If those values are correct, the administrator should verify the SSL certificate presented by the Web server is the correct certificate. If the hostname, port, and certificate are all correct, the administrator should run the configuration in interactive mode, without the -rspfile flag, to complete the task.

FBTTAC122E The option *command line option* **must be specified.**

Explanation: The tfimcfg tool was passed invalid command line options.

System action: The tfimcfg tool will exit.

Administrator response: Review the tfimcfg usage message and documentation and correct the command line options.

FBTTAC123E The argument to the option *command line option* **must be specified.**

Explanation: The tfimcfg tool was passed invalid command line options.

System action: The tfimcfg tool will exit.

Administrator response: Review the tfimcfg usage message and documentation and correct the command line options.

FBTTAC124E The configuration option *command line option* **is not valid.**

Explanation: The tfimcfg tool was passed invalid command line options.

System action: The tfimcfg tool will exit.

Administrator response: Review the tfimcfg usage message and documentation and correct the command line options.

FBTTAC125E The file *file name* **does not appear to belong to a WebSEAL server.**

Explanation: The tfimcfg tool examined the configuration file specified and determined it did not belong to a WebSEAL server.

System action: The tool will exit without changing any configuration.

Administrator response: The most likely cause of this error is that the file specified is not a Security Access Manager for Web stanza file that belongs to a WebSEAL server. Verify that the file specified is the correct file to use. If necessary, refer to the documentation for examples of how to use the autoconfiguration tool.

FBTTAC140W LDAP server type '*ldap server type*' unknown. You should manually update the ACLs for the LDAP suffixes.

Explanation: The tfimcfg tool tries to set appropriate ACLs on LDAP suffixes, but does not support all LDAP server types. The ACLs could not be updated because the LDAP server was not recognized.

System action: The configuration will continue without updating the ACLs.

Administrator response: The administrator should manually update the ACLs on the LDAP suffixes.

FBTTAC145W Object already exists. Reusing existing object.

Explanation: The tfimcfg tool tries to create LDAP objects as needed. An object already exists.

System action: The configuration will reuse the object.

Administrator response: No response necessary.

FBTTAC146W Missing required property *property name*.

Explanation: A required property was not specified in the response file.

System action: The configuration will stop.

Administrator response: Correct the response file.

FBTTAC147W Suffix already exists. Reusing existing suffix.

Explanation: The tfimcfg tool tries to create LDAP suffixes as needed. A suffix already exists.

System action: The configuration will reuse the suffix.

Administrator response: No response necessary.

FBTTAC148W LDAP server type '*ldap server type*' unknown. You should manually add LDAP suffixes.

Explanation: The tfimcfg tool tries to automatically create suffixes, but does not support all LDAP server types. The suffixes could not be created because the LDAP server was not recognized.

System action: The configuration will continue without creating the suffixes.

Administrator response: The administrator should manually create the LDAP suffixes.

FBTTAC150E Unable to connect to LDAP server:*exception*.

Explanation: The tfimcfg tool was unable to make a connection to the LDAP server.

System action: The configuration will halt.

Administrator response: Verify that the hostname and port number specified for the connection are correct and that the LDAP server can be contacted.

FBTTAC151E Unable to authenticate to LDAP server:*exception*. Verify that the user-id and password are correct.

Explanation: The tfimcfg tool was unable to make a connection to the LDAP server.

System action: The configuration will halt.

Administrator response: Verify that the user-id and password specified for the connection are correct.

FBTTAC152E Permission denied by LDAP server:*exception*. Verify that you are binding to LDAP as an administrative user with sufficient permissions to complete the configuration tasks.

Explanation: The tfimcfg tool was unable to access the LDAP server because of insufficient access rights.

System action: The configuration will halt.

Administrator response: Verify that the user you are using to bind to LDAP has sufficient access rights to perform the failing configuration task.

FBTTAC153E Object not found:*exception*. You may have specified an incorrect object DN, or you may need to create an LDAP suffix manually.

Explanation: The tfimcfg tool was unable to create an object in the LDAP server because the parent object was not found.

System action: The configuration will halt.

Administrator response: Verify that you have specified the object DN correctly. You may need to create the suffix for the object manually.

FBTTAC154W Configuration of authenticated SOAP endpoints with the IVT application is not recommended. Authentication for the IVT application can conflict with authentication for the SOAP endpoints.

Explanation: The IVT application requires forms authentication, while SOAP endpoints require certificate or BA authentication. Attempting to use both those authentication types simultaneously can cause one or both to stop functioning.

System action: The configuration will continue.

Administrator response: The administrator should use a separate WebSEAL server for SOAP endpoints.

FBTTAC166E Unable to convert key database *file name* **from .kdb format to .jks format. The** *program name* **program returned error code** *numeric error code***.***log data*

Explanation: The tfimcfg tool attempts to convert the WebSEAL key database from .kdb format to .jks (Java Key Store) format. This conversion failed with the specified error code and error text.

System action: The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response: Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC167E Unable to add the certificate *cert file* **to the key database** *file name***. The** *program name* **program returned error code** *numeric error code***.***log data*

Explanation: The tfimcfg tool attempts to add a Web server's CA certificate to the WebSEAL key database. This process failed with the specified error code and error text.

System action: The administrator will be prompted to either correct the problem or else cancel the configuration.

Administrator response: Read the messages printed to the screen to diagnose the root cause of the problem. Correct the problem, and then repeat the configuration.

FBTTAC172W Unable to find running reverse proxy instances when connecting to host *host URL***.** *error text*

Explanation: The tfimcfg tool tried to query the number of running reverse proxy instances on a Web Gateway Appliance. No running instances were found.

System action: The tfimcfg utility will not proceed until a running reverse proxy instance is found on a Web Gateway Appliance.

Administrator response: The administrative response should be to check that the URL of the Web Appliance Gateway that needs to be configured is valid and correct. The administrator should also ensure that there are running reverse proxy instances on the target Web Gateway Appliance.

FBTTAC173E Error interpreting configuration URL *url***:\n** *exception text***\n**

Explanation: The tfimcfg tool could not interpret the Web Gateway Appliance configuration URL.

System action: The tfimcfg utility will not proceed until a valid Web Gateway Appliance configuration URL is specified.

Administrator response: The administrator may need to specify a valid Web Gateway Appliance configuration URL.

FBTTAC174E An error occurred when restarting the reverse proxy instance '*instance name***' on the Web Gateway Appliance. Please check\n the log file of the reverse proxy instance on the Web Gateway Appliance to diagnose and fix the problem.\n**

Explanation: The configuration tool tried to restart a reverse proxy instance on a Web Gateway Appliance, but the server did not start.

System action: The autoconfiguration tool will not proceed until the reverse proxy instance is operational.

Administrator response: The administrator should check the Web Gateway Appliance's reverse proxy instance log file and correct the problem.

FBTTAC176E An error occurred during an attempt to connect to the Web Gateway Appliance. The response code was *response code***:\n***error text***\n**

Explanation: An error occurred during an attempt to connect to the Web Gateway Appliance. The response code and error text contains additional information about the error.

System action: If the change being made is non-critical file, the tool will attempt to proceed. If the change is critical to the operation being performed, the tool will exit.

Administrator response: Attempt to resolve the problem described by the error text. Ensure that the tool has access to the network where the Web Gateway Appliance is running.

FBTTAC187E POP creation failed:\n*error messages***\n.**

Explanation: An error occurred in the process of creating a POP. Other messages may have more information on the root cause of the problem.

System action: The autoconfiguration tool will continue with the configuration.

Administrator response: Attempt to diagnose the error condition and fix the problem, or create the POP manually.

FBTTAC188E An invalid URL value was entered.

Explanation: The value entered was not a valid URL.

System action: The autoconfiguration tool will show the URL entry prompt again.

Administrator response: Enter a valid URL.

FBTTAC189E No OAuth federations were returned from the Security Access Manager InfoService.\n

Explanation: The Federated Identity Manager InfoService did not return any OAuth federations.

System action: The autoconfiguration tool will do nothing.

Administrator response: The administrator should make sure that OAuth federations were configured on the Federated Identity Manager server. It may be necessary to restart the WebSphere server if the configuration was recently changed.

FBTTAC190E The file *file name* **does not exist in the file system.\n**

Explanation: The file does not exist on the file system.

System action: The autoconfiguration tool will do nothing.

Administrator response: Verify that the file exists.

FBTTAC228E The Security Access Manager autoconfiguration tool requires *tool name* **on the system PATH.**

Explanation: A tool required by the Security Access Manager autoconfiguration tool was not available on the system PATH.

System action: The autoconfiguration tool will exit without modifying any configuration.

Administrator response: Add the appropriate tool (gsk7ikm or ikeycmd) to the system PATH and then rerun the Security Access Manager autoconfiguration tool.

FBTTRC002W The service stub cannot be retrieved using a JNDI Lookup. Falling back on Service Locator. The handler configuration is likely to fail.

Explanation: See message.

System action: Processing continued.

Administrator response: Check the log files for more information.

FBTTRC003E The Trust Service Client handler is missing or improperly configured.

Explanation: The handler is missing from the client side handler chain. If this handler is missing or not present, or the client is not running as a managed application, the Trust Client cannot retrieve nor set the messages sent to the trust server.

System action: No action taken.

Administrator response: No response required.

FBTTRC004W The returned RequestSecurityTokenResponse did not have a wsu:Id

Explanation: Without an element ID, the client cannot receive the original message.

System action: No action taken.

Administrator response: No response required.

FBTTRC006E No DOM message implementation was passed.

Explanation: The Trust Client implementation is expecting the passed-in message to contain a DOM tree that represents the SOAP envelope.

System action: No action taken.

Administrator response: No response required.

FBTUSC000E Internal Error. Contact the System Administrator.

Explanation: An internal error occurred.

System action: The STS request processing has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTUSC001E The required attribute *attributeName* **was not found in the incoming STS Request.**

Explanation: The required attribute was not found in the incoming STS Request. The required attribute is expected to be added to the request by another STS module earlier in the trust chain.

System action: The STS request processing has been halted.

Administrator response: Enable tracing to help determine why the attribute was not added.

FBTUSC002E The required configuration parameter *configParameterName* was not provided to the STS module.

Explanation: The required configuration parameter was not provided.

System action: The STS request processing has been halted.

Administrator response: Ensure that the configuration for the module has been correctly performed.

FBTUSC003E The required service handle *handleName* was not provided to the STS module.

Explanation: The required service handle was not available.

System action: The STS request processing has been halted.

Administrator response: This error is a significant internal error. Check the logs for error messages indicating why the required service was not properly created.

FBTUSC004E E-mail could not be sent to the following address: *address*.

Explanation: An e-mail could not be sent to the requested address. This error is not an internal error.

System action: The User Self Care operation could not be completed.

Administrator response: The User Self Care application could not send e-mail to the indicated address. If details are required, please enable trace logging and examine the nested exception.

FBTUSC005E An e-mail could not be sent due to a problem with the messaging component.

Explanation: An e-mail could not be sent due to a problem with the messaging component.

System action: The User Self care operation could not be completed.

Administrator response: The User Self Care application could not a message due to a problem with the messaging component. If details are required, please enable trace logging and examine the nested exception.

FBTUSC006E An error occurred during the construction of the contents of a message.

Explanation: The messaging component failed to build a message to send to the user.

System action: The User Self care operation could not be completed.

Administrator response: The User Self Care application could not send a message due to a problem constructing the message contents. If details are required, please enable trace logging and examine the nested exception.

FBTUSC007E The page contents might be missing the required information such as [*requiredInfo*] that is used to process an e-mail message request.

Explanation: The E-mail Message STS module requires certain information in order to process the request. The required information is missing.

System action: The STS request processing has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC010E Password change failed.

Explanation: The password change operation failed.

System action: The password for the user has not been changed.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC011E Profile lookup failed.

Explanation: The profile lookup operation failed.

System action: The request has been halted.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC012E Profile update failed.

Explanation: The profile update operation failed.

System action: The request was halted without modifying the user profile.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC013E User account creation failed.

Explanation: The user account creation operation failed.

System action: The request was halted without creating the user account.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC014E User account deletion failed.

Explanation: The user account deletion operation failed.

System action: The request was halted without deleting the user account.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC015E Group membership update failed.

Explanation: The group membership update operation failed.

System action: The request has been halted.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC016E User lookup failed.

Explanation: The user lookup operation failed.

System action: The request has been halted.

Administrator response: Ensure that the registry server is available. Check the log file for more information about the cause of the problem.

FBTUSC017E Context attributes required to perform the operation are missing: *data*

Explanation: This operation requires one or more context attributes that are not present. This error usually indicates a problem with a custom mapping rule.

System action: The request has been halted.

Administrator response: Ensure that any custom mapping rules in the chain pass on all incoming context attributes.

FBTUSC020E You must specify a user name.

Explanation: The user has not specified a user name. This message is displayed to the user.

System action: No action is necessary. The enrollment request has not been processed.

Administrator response: No action is necessary.

FBTUSC021E The specified passwords do not match.

Explanation: The specified passwords do not match. This message is presented to the user.

System action: No action is necessary. The user enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC022E The enrollment validation data must be supplied.

Explanation: The user has submitted the enrollment completion form without the enrollment validation data. This message is presented to the user.

System action: No action is necessary. The user enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC023E The enrollment validation data is not correct, or the enrollment process has already been completed.

Explanation: The user has submitted enrollment validation data that does not match a current enrollment request or has resubmitted the enrollment completion form.

System action: No action is necessary. The user enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC024E The requested user name, *username* **is already in use.**

Explanation: The requested user name is already in use. This message is displayed to the user.

System action: No action is necessary. The enrollment request has not been processed.

Administrator response: No action is necessary.

FBTUSC025E Account creation failed.

Explanation: The user account could not be created. This message is displayed to the user.

System action: The enrollment process has not been completed.

Administrator response: Examine the application server logs to determine the cause of the problem.

FBTUSC026E Unable to generate a confirmation ID: *error***.**

Explanation: Unable to generate a confirmation ID.

System action: The enrollment request has not been processed.

Administrator response: Examine the application server logs to determine the cause of the problem.

FBTUSC027E You must enter values in both the password and password confirmation fields.

Explanation: The user has not supplied either the password or the password confirmation.

System action: The enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC028E The specified e-mail addresses do not match.

Explanation: The specified e-mail addresses do not match. This message is presented to the user.

System action: No action is necessary. The user enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC029E You must enter both the e-mail address and e-mail address confirmation fields.

Explanation: The user has not supplied either the e-mail address or the e-mail address confirmation.

System action: The enrollment request has not been processed.

Administrator response: No response is necessary.

FBTUSC030E The USCChangePassword STS module does not operate in the given mode, '*mode*'.

Explanation: The mode that was configured for the module is not valid.

System action: The module is not available at runtime.

Administrator response: Change the operation mode to 'map'.

FBTUSC031E Additional data is required to perform the operation: *data*

Explanation: The operation requires additional data.

System action: The request has been halted.

Administrator response: Ensure that the specified data items are present before requesting the operation.

FBTUSC032E The new password and confirmation password do not match.

Explanation: The new password and the confirmation password must match.

System action: The request has been halted.

Administrator response: Ensure that the new password and confirmation password are the same.

FBTUSC033E The current password is incorrect.

Explanation: The current password is incorrect.

System action: The request has been halted.

Administrator response: Ensure that the current password is correct.

FBTUSC034E The password change operation failed.

Explanation: The password change operation failed.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC035E The new password does not meet the password policy requirements.

Explanation: The new password does not meet the password policy requirements.

System action: The request has been halted.

Administrator response: Select a new password that complies with the password policy requirements.

FBTUSC040E Unable to find your account validation questions.

Explanation: The secret question module did not provide any account validation questions to present to the user and did not provide a failure reason.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTUSC041E This account has been locked due to too many failed account validation attempts.

Explanation: The user made too many failed attempts to validate the account, so the account has been locked.

System action: The request has been halted.

Administrator response: No response is necessary.

FBTUSC042E There is already a password change request in progress for this account.

Explanation: The user already started the password change process. The user can make only one password change request at a time.

System action: The request has been halted.

Administrator response: No response is necessary.

FBTUSC043E The password change request has already been processed.

Explanation: The password change request identifier supplied by the user does not identify a current password change request.

System action: The request has been halted.

Administrator response: No response is necessary.

FBTUSC044E The information required to locate your user name is missing.

Explanation: The information required to locate the user name was not supplied.

System action: The request has been halted.

Administrator response: No response is necessary.

FBTUSC045E Account validation failed.

Explanation: You provided an incorrect answer to the account validation question.

System action: The request has been halted.

Administrator response: No response is necessary.

FBTUSC046E Unable to retrieve your account validation details.

Explanation: The secret question mapping module did not provide the name of the profile attribute used to store the answer to the account validation question.

System action: The request has been halted.

Administrator response: The account recovery module chain contains a mapping module. Check that the mapping rule correctly maps the secret question identifiers to the profile attributes.

FBTUSC047E Unable to retrieve your account validation details.

Explanation: Unable to find a value for the profile attribute that holds the answer to the selected account validation question.

System action: The request has been halted.

Administrator response: Check that the mapping rule used in the account recovery module chain maps secret question identifiers to the correct profile attributes.

FBTUSC048E You must specify a user name.

Explanation: The user has not specified a user name. This message is displayed to the user.

System action: No action is necessary. The account recovery request has not been processed.

Administrator response: No action is necessary.

FBTUSC049E You must specify the answer to the account validation question.

Explanation: The user has not supplied the answer to the account validation question.

System action: The account recovery request has not been processed.

Administrator response: No response is necessary.

FBTUSC050E No authenticated user identity is available.

Explanation: The requested operation can only be performed using an authenticated user identity, but none is available.

System action: The request has been halted.

Administrator response: Check the security configuration to ensure that authentication is required to access this operation.

FBTUSC051E The account could not be deleted.

Explanation: The account could not be deleted.

System action: The request has been halted.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC060E The required Context Attributes were not found in the incoming STSUU.

Explanation: A User Self Care STS module requires Context Attributes in the STSUU.

System action: The request has been halted.

Administrator response: Investigate the previous modules in the trust chain to ensure that none of them remove the context attributes from the STSUU, and correct if necessary. If removal is not the problem, the protocol service invoking the chain might have failed to provide the context attributes. In this case, the error is an internal error.

FBTUSC061E The module received the context attribute: ***handleName*** **containing a value that is not valid:** ***value*****.**

Explanation: The module received a required context attribute, but the value is not valid.

System action: The STS request processing has been halted.

Administrator response: Determine whether any STS modules preceding this module in the chain have incorrectly set the value of the required attribute and correct.

FBTUSC062E The User Self Care module cannot create a local token.

Explanation: The User Self Care module cannot create a local token.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC063E The User Self Care module cannot locate the context attributes.

Explanation: The User Self Care cannot locate the context attributes.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC064E The User Self Care module cannot invoke the STS.

Explanation: The User Self Care module cannot contact the STS to fulfill the user request.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC065E The User Self Care module failed to send a response to the user request.

Explanation: The User Self Care module cannot send a response to the user request.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC066E The User Self Care module cannot locate a redirect URL on the context attributes.

Explanation: The User Self Care cannot locate the redirect URL on the context attributes.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC067E The User Self Care module failed to send a browser redirect response to the user request. Redirect URL: ***pageID*****.**

Explanation: The User Self Care module failed to send a browser redirect response to the user request.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC068E The User Self Care module cannot find the page template for page identifier: ***pageID*****.**

Explanation: The User Self Care module cannot find the page template with the specified page identifier.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC069E The User Self Care module failed to return a browser form to the user. Page ID: ***formID*****.**

Explanation: The User Self Care was unable return a browser form to the user.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC070E The User Self Care module cannot find the form page identifier from the context attributes.

Explanation: The User Self Care module cannot find the form page identifier from the context attributes.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC071E The User Self Care module cannot process the error generated.

Explanation: The User Self Care module cannot process the error generated.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC072E The User Self Care module cannot process the request.

Explanation: The User Self Care module cannot process the request.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem.

FBTUSC073E The User Self Care module request was sent using a transport that is not valid.

Explanation: The User Self Care module was sent using a transport that is not valid. The request was sent using the SOAP binding.

System action: The User Self Care request processing stopped.

Administrator response: Examine the logs to determine the cause of the problem. Ensure that the request is being sent using the appropriate binding.

FBTUSC080E Unable to locate your profile details.

Explanation: A profile retrieval or update operation returned an error that the user was not in the registry. This error might occur when users have been recently deleted.

System action: The STS request processing stopped.

Administrator response: Check that the user registry is correctly configured and is currently available. Check that the configuration of the entity management STS module specifies the correct user registry suffix.

FBTUSC081E One or more of the specified profile attributes might not be updated.

Explanation: A profile update request included one or more profile attributes that users cannot edit. This error might indicate malicious user activity.

System action: The STS request processing stopped.

Administrator response: Enable tracing in the profile management STS module to identify the attribute names. Check that the profile update form includes only profile attributes from the list of permitted attributes in the profile management STS module configuration. Verify that the set of permitted attributes is correct.

FBTUSC082E The specified e-mail addresses do not match.

Explanation: The specified e-mail addresses do not match. This message is presented to the user.

System action: No action is necessary. The profile update request has not been processed.

Administrator response: No response is necessary.

FBTUSC084E The account recovery STS module configuration is incorrect.

Explanation: The account recovery STS module configuration includes the account recovery lookup attribute and the account recovery validation attributes.

System action: The account recovery STS module has not been initialized. Account recovery operations fail until this error is corrected.

Administrator response: Correct the configuration of the account recovery STS module. Ensure that the account recovery lookup attribute and the account recovery validation attributes are specified.

FBTUSC085E The e-mail message STS module configuration is incorrect.

Explanation: The e-mail message STS module configuration includes the SMTP server name, SMTP user name, SMTP user name password, and enrollment e-mail address.

System action: E-mail message operations fail until the e-mail message STS module is initialized.

Administrator response: Correct the configuration of the e-mail message STS module. Ensure that the SMTP server name, SMTP user name, SMTP user name password and enrollment e-mail address are specified.

FBTUSC086E The group membership STS module configuration is incorrect.

Explanation: The group membership STS module configuration lists the groups into which a new user is to be added.

System action: The group membership STS module has not been initialized. Group membership operations fail until this error is corrected.

Administrator response: Correct the configuration of the group membership STS module.

FBTUSC087E The password does not meet the password policy requirements.

Explanation: The password does not meet the password policy requirements.

System action: The request has been halted.

Administrator response: Select a password that complies with the password policy requirements.

FBTUSC088E The password is incorrect.

Explanation: The user has not specified the current password correctly.

System action: The request has been halted.

Administrator response: Correct the password and resubmit the form.

FBTUSC089E The secret question STS module is not configured correctly.

Explanation: The secret question STS module configuration includes the minimum number of secret questions, maximum number of secret questions, and the number of required secret questions to be answered correctly for users to be validated.

System action: The secret question STS module has not been initialized. Secret question operations cannot function correctly until his error is corrected.

Administrator response: Correct the configuration settings of the secret question STS module. Ensure that the following fields are configured correctly: minimum number of secret questions, maximum number of secret questions, and the number of required secret questions to be validated.

FBTUSC090E You have not answered enough secret questions.

Explanation: The user answered less than the minimum number of secret question required for validation.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTUSC091E You have answered more secret questions than what is allowed.

Explanation: The number of secret question answered is more than maximum number of secret question permitted.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTUSC092E You did not provide an answer to the required secret question fields.

Explanation: No input from the secret question fields was retrieved.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTUSC093E You are not allowed to answer the same question more than once.

Explanation: There are duplicate question input in secret questions.

System action: The request has been halted.

Administrator response: Examine the log to determine the cause of the failure.

FBTUSC098E Migration cannot be done because the hashing algorithm SHA-256 is not supported.

Explanation: The hashing algorithm SHA-256 is not supported.

System action: Operation canceled.

Administrator response: Check JVM support for hashing algorithm.

FBTUSC099E The required host parameter is missing. Please specify the hostname of the directory machine using the -h option.

Explanation: A host parameter is required to do the migration.

System action: Operation canceled.

Administrator response: Specify a directory host parameter to proceed with the migration.

FBTUSC100E The required bind distinguished name parameter is missing. Please specify the bind distinguished name of the directory using the -D option.

Explanation: A bind distinguished name parameter is required to do the migration.

System action: Operation canceled.

Administrator response: Specify a value for the bind distinguished name parameter to proceed with the migration.

FBTUSC101E The required bind credential parameter is missing. Please specify the bind credential of the directory using the -w option.

Explanation: A bind credential parameter is required to do the migration.

System action: Operation canceled.

Administrator response: Specify a value for the bind credential parameter to proceed with the migration.

FBTUSC102E The required base distinguished name parameter is missing. Please specify the base distinguished name of the directory using the -baseDn option.

Explanation: A base distinguished name parameter is required to do the migration.

System action: Operation canceled.

Administrator response: Specify a value for the base distinguished name parameter to proceed with the migration.

FBTUSC103E The required secret question attribute parameter is missing. Please specify the secret question attribute using the -attribute option.

Explanation: A secret question attribute parameter is required to do the migration.

System action: Operation canceled.

Administrator response: Specify a value for the secret question attribute parameter to proceed with the migration.

FBTUSC104E The parameter *parameter* **was not recognized.**

Explanation: The migration cannot be done because one or more of the specified parameters were not recognized.

System action: Operation canceled.

Administrator response: Use only the supported parameters.

FBTUSC105E The user *parameter* **does not have a valid secret question format. The tool is not going to migrate the secret question value for this user.**

Explanation: The secret question value for this user cannot be migrated because the secret question format is not valid.

System action: Migration of secret question value for user not done.

Administrator response: The user record is not valid for migration.

FBTUSR000E Internal Error. Contact the System Administrator.

Explanation: An internal error occurred.

System action: User info encountered an error, process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTUSR100E The user info provider plugin *pluginName* **failed to initialize.**

Explanation: A user info provider plugin encountered an error during initialization.

System action: The user info provider plugin initialization encountered an error, the process has been halted.

Administrator response: Check the log file for more information about the cause of the problem.

FBTWSF001E The received request is missing the required parameter: *parameter*

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTWSF002E The received request at '*age***' seconds, is expired.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTWSF003E The logout failed.

Explanation: The logout failed for the current session.

System action: The logout request will continue.

Administrator response: Ensure that the point of contact is configured to send the correct session HTTP header.

FBTWSF004E The requesting realm, *realm***, is unknown.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTWSF005E The value *value* **for attribute** *attr* **is not valid.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTWSF006E The current user making the request is not authenticated.

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the incoming message.

FBTWSF007E The token for the service provider cannot be exchanged.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration.

FBTWSF008E No token was available to return to the service provider.

Explanation: The current request could not be completed because the token exchange failed.

System action: The request will be halted.

Administrator response: Validate the incoming message and the trust service configuration.

FBTWSF009E No configured post page was available to use to return the token to the identity provider.

Explanation: The current request could not be completed. The token exchange succeeded but no configured post page was available.

System action: The request will be halted.

Administrator response: This error is a configuration error. Ensure that the post page exists in the template directory.

FBTWSF010E The response from the identity provider, *wresult*, could not be understood.

Explanation: The current request could not be completed because the identity provider response was not understandable.

System action: The request will be halted.

Administrator response: Validate that the identity provider is configured to send the correct XML element response.

FBTWSF011E The identity provider token could not be determined as the one that is valid for the resource.

Explanation: The current request could not be completed because the identity provider response was not understandable.

System action: The request will be halted.

Administrator response: Validate that the identity provider is configured to send the correct XML element response.

FBTWSF012E The user cannot be authenticated.

Explanation: The current request could not be completed because the trust service response could not authenticate the user.

System action: The request will be halted.

Administrator response: Validate that the trust service and point of contact are properly configured.

FBTWSF013E The timestamp provided, *time*, does not match any known time format.

Explanation: The current request could not be completed because the lifetime could not be validated.

System action: The request will be halted.

Administrator response: Validate that the partner is configured to send the correct time values.

FBTWSF014E The Tivoli Access Manager configuration for the service is not configured correctly or the Tivoli Access Manager context is no longer valid.

Explanation: When the Tivoli Access Manager operation was attempted an error was returned.

System action: The request will be halted.

Administrator response: Ensure that the configuration of Tivoli Access Manager for the service is pointing to a valid Tivoli Access Manager Runtime for the Java configuration file.

FBTWSF016E The template *template filename* for sign-out is not valid.

Explanation: When the server attempted to build the WS-Federation sign-out to all the service providers, the template was not valid.

System action: The sign-out request will be halted.

Administrator response: Ensure that the provided template is correct.

FBTWSF017E An identity provider cannot be determined for the current requester.

Explanation: When attempting to determine the current requester's identity provider, a failure occurred.

System action: The sign-in request will be halted.

Administrator response: Ensure that configuration is correct.

FBTWSF018E Invalid configuration; missing configuration for self IP/STS endpoint in federation with ID '*id*' and display name '*displayName*'.

Explanation: The IP/STS endpoint has not been specified in the configuration. This value is used at runtime to redirect requestors back to this endpoint.

System action: The initialization of this module will be halted.

Administrator response: Ensure that configuration is correct.

FBTWSF019E Invalid configuration; missing configuration for partner '*id*' IP/STS endpoint in federation with ID '*id*' and display name '*displayName*'.

Explanation: The IP/STS endpoint has not been specified in configuration. This value is used at runtime to redirect requestors back to this endpoint.

System action: The initialization of this module will be halted.

Administrator response: Ensure that configuration is correct.

FBTWSF020E Invalid configuration; invalid lifetime for partner '*id*' in federation with ID '*id*' and display name '*displayName*'.

Explanation: The configured message lifetime is in an invalid format, expecting integer values. This parameter is used at runtime for message validation.

System action: The initialization of this module will be halted.

Administrator response: Ensure that the configuration is correct.

FBTWSP001E The provisioning configuration file *insert* is missing or is not valid.

Explanation: The configuration cannot be read or its format is incorrect.

Administrator response: Enable a trace for detailed messages and ensure that the configuration is present and valid.

FBTWSP002E The provisioning configuration file *insert* could not be written.

Explanation: The configuration cannot be written to file.

Administrator response: Enable a trace for detailed messages and ensure that the file path is correct and that writing to the file is permitted.

FBTWSP003E The target provisioning service URL is not configured.

Explanation: The configuration is incorrect as it doesn't include the mandatory target provisioning service URL.

Administrator response: Enable a trace for detailed messages and validate the configuration.

FBTWSS001E The command line arguments are not valid.

Explanation: The syntax of the command line arguments is incorrect.

Administrator response: Correct the syntax and try again.

FBTWSS004E An error occurred while accessing the Tivoli Access Manager server using the configuration URL *insert*.

Explanation: The Tivoli Access Manager configuration or the configuration URL is incorrect.

Administrator response: Ensure that the Tivoli Access Manager configuration and the configuration URL are correct.

FBTWSS011E The security token is not valid or is missing.

Explanation: The security token syntax is not valid or the security token is missing.

Administrator response: Check the log and ensure the configuration is correct.

FBTWSS021E The configuration is in error.

Explanation: The configuration is incorrect.

Administrator response: Check the log and ensure the configuration is correct.

FBTWSS031E An error occurred accessing the Trust Service.

Explanation: An error occurred accessing the Trust Service or the Trust Service returned an error response.

Administrator response: Check the log and ensure the configuration is correct.

FBTWSS032E An XML processing error occurred.

Explanation: A parsing or some other error related to XML processing occurred.

Administrator response: Check the log and ensure the configuration is correct.

FBTXRD001E A value for the attribute *AttributeName* **must be provided for the <***ElementName***> element.**

Explanation: The application is in error. Required data was not set in the XRDS document.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and check with the XRDS document provider.

FBTXRD002E The member element *MemberElementName* **must be provided for the <***ElementName***> element.**

Explanation: The application is in error. Required data was not set in the XRDS document.

System action: The request has been halted.

Administrator response: Enable a trace for detailed messages and check with the XRDS document provider.

FBTXRD003W An XRDS document parse error has occurred. This was non-fatal due to HTML discovery fall back.

Explanation: The XRDS document could not be parsed correctly. Discovery will fall back to HTML based discovery.

System action: The system will fall back to HTML discovery and ignore the XRDS document.

Administrator response: Retrieve the XRDS document from the log to check the validity of the document.

FBTXRD004E The canonicalID from the first XRI resolution request *ClaimedIdentifier* **did not resolve to the same XRI as the second XRI resolution request** *CanonicalID***.**

Explanation: An incorrect CanonicalID was found in the first XRDS document request. This may have been an attempt by the user to impersonate another person using their XRI.

System action: The request has been halted.

Administrator response: Inspect the logs and, if appropriate, report the abuse to the CanonicalIDs authorative XRI provider.

FBTXRD005E Unable to perform XRDS resolution on the XRI *XRI* **supplied.**

Explanation: An appropriate service was not found in the XRDS document.

System action: The request has been halted.

Administrator response: Retrieve the XRDS document from the log to check the validity of the document and if the required service is included.

FBTXRD006E Unable to perform XRDS resolution because XRIs are not supported.

Explanation: XRI support has been disabled in this configuration.

System action: The request has been halted.

Administrator response: To enable XRI resolution, modify the XRIProxies and SupportXRI configuration items in the federation properties.

Chapter 4. Authorization Service Messages

These messages are provided by the authorization service component.

CTGVM0220W The audit service cannot locate a Work Manager. Asynchronous logging will be disabled.

Explanation: The audit service cannot locate a work manager, asynchronous processing of audit records cannot be performed. This may result in a performance degradation.

System action: No action taken.

Administrator response: Refer to the administration guide for how to setup a WebSphere Work Manager.

CTGVS0001E An error occurred while working with protocol *protocol_name* **.**

Explanation: An error occurred during an attempt to retrieve a policy update using the specified protocol.

System action: The policy distribution request did not complete.

Administrator response: Ensure that the policy management server is available and retry the policy distribution.

CTGVS0002E While processing the common authorization configuration property values, required property *property* **was found not be set.**

Explanation: The required property identified above was not set.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Make changes as needed and retry the request.

CTGVS0003E The common authorization configuration data derived from the property file cannot have a null context.

Explanation: The context must contain a valid value.

System action: The request has been halted.

Administrator response: Ensure the context is set and retry the operation.

CTGVS0004E Cannot get the security environment for extension ID *extension_ID* **.**

Explanation: Cannot get the security runtime environment for the specified extension.

System action: The request has been halted.

Administrator response: Ensure the extension specified exists. Review the operating environment and ensure components are available. Retry the operation after making the necessary changes.

CTGVS0005E Cannot get the runtime environment for extension ID *extension_ID* **.**

Explanation: Cannot get the runtime environment for the specified extension.

System action: The request has been halted.

Administrator response: Ensure the extension specified exists. Review the operating environment and ensure components are available. Retry the operation after making the necessary changes.

CTGVS0006E Component or service *component_name* **was requested but it does not exist.**

Explanation: The component or service specified does not exist, it is not defined.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS0007E A request was made for command *command_name* **which does not exist.**

Explanation: The command specified does not exist, it is not defined.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS0008E Unable to location configuration file path *config_file_path* **.**

Explanation: The config_file_path specified cannot be located.

System action: The request has been halted.

Administrator response: Investigate the config_file_path configuration file specified and related settings. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS0009E A request was made for an unregistered security service *service_name* **.**

Explanation: A request was made for security service service_name which is an unknown service.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS0010W The service manager is already initialized.

Explanation: The service manager is already initialized.

System action: The request has been halted.

Administrator response: No further action is required.

CTGVS0011E An error occurred creating service *service_name* **.**

Explanation: An error occurred creating the specified service.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS0012E Unable to parse configuration file *config_file* **.**

Explanation: The config_file specified cannot be parsed.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS0013E The service manager is not initialized.

Explanation: The service manager is not initialized.

System action: The request has been halted.

Administrator response: Investigate the specified configuration file and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS0014E The eclipse property *propertyName* **contains an invalid value** *value***. The value** *defaultValue* **will be used instead.**

Explanation: An invalid OSGi eclipse property is configured, and will be ignored.

System action: Default values will be used instead of the configured values.

Administrator response: Edit the OSGi eclipse property and replace with a valid value.

CTGVS0015E localhost:*consolePort* **is already in use and cannot be used as the Eclipse console port.**

Explanation: The console port configured is in use by another application.

System action: The console will not be available.

Administrator response: Select a different port for the OSGi Eclipse console.

CTGVS0016E The specified Eclipse console port *consolePort* **is not available.**

Explanation: The console port configured is not available.

System action: The Eclipse OSGi console will not be available.

Administrator response: Select a different port for the OSGi Eclipse console.

CTGVS0017E Error while starting Eclipse: *targetException***.**

Explanation: The Eclipse OSGi framework failed to start.

System action: The application will not be run.

Administrator response: Examine the error message for possible cause.

CTGVS0018E Failed to delete *fileName*

Explanation: The program failed to delete a file while cleaning a temporary copy of the Eclipse OSGi environment

System action: The failure will be ignored

Administrator response: Manually remove the temporary file the next time the application is stopped. Examine the permissions on the file and the containing directory to ensure the problem does not re-occur.

CTGVS0019E No services manager has been registered by the OSGi framework.

Explanation: An internal runtime component could not be loaded.

System action: The application did not start successfully. This could be due to an improper or corrupted installation.

Administrator response: Ensure that the application has been properly installed and configured.

CTGVS0020E Exception while loading extensions.

Explanation: An internal service component could not be loaded. This could be due to an improper or corrupted installation.

System action: The application did not start successfully.

Administrator response: Ensure that the application has been properly installed and configured.

CTGVS0021E An error was encountered while checking security permissions for method *methodName***.**

Explanation: A Java 2 security check failed for the operation.

System action: Access to the operation is denied. The method invocation fails.

Administrator response: Ensure that the application has been granted the appropriate security permission.

CTGVS0022E An error was encountered while calculating the startup sequence of the service framework. A dependency cycle on service *serviceName* **has been detected.**

Explanation: A security service was modified or plugged and introduced a cycle dependency on the framework.

System action: Stop initialization.

Administrator response: Ensure that the application has been properly installed and configured. Remove any service plug-ins that were not part of the original installation and verify its dependencies.

CTGVS0023W A dependency for service *serviceName* **on service** *serviceDep* **cannot be satisfied since the latter service is not available.**

Explanation: A security service has an unsatisfied dependency due to missing services in the installation.

System action: Stop initialization.

Administrator response: Ensure that the application has been properly installed and configured.

CTGVS0024E The application runtime could not be loaded. Ensure that the application runtime plug-ins have been installed to this server.

Explanation: The application runtime has not been deployed to the server. The application can not start.

System action: The applcation initialization does not complete.

Administrator response: Ensure that all application components, including the application runtime extension, have been installed.

CTGVS0027E The platform manager has not been started.

Explanation: The application runtime could not be initialized for the application platform. The application can not start.

System action: The application initialization does not complete.

Administrator response: Ensure that all application components, including the application runtime, have been installed.

CTGVS0028E An end point reference could not be generated for the target address *urladdress***.**

Explanation: The communication channel to the target end point could not be secured for transport. The communication attempt is aborted.

System action: Communication events such as policy retrieval are aborted.

Administrator response: Ensure that all application components are installed and properly configured.

CTGVS0029E The platform manager could not be loaded.

Explanation: The application runtime could not load the appropriate platform manager for this platform.

System action: The application initialization does not complete normally.

Administrator response: Ensure that all application components are installed and properly configured for this application server platform.

CTGVS0030E The cell name could not be determined.

Explanation: The initialization process could not complete because the local cell name could not be determined.

System action: Runtime initialization does not complete.

Administrator response: Enable the finest level of logging and restart the server. Review the log files. Make changes as needed and retry.

CTGVS0031E The configuration deployement manager could not be loaded.

Explanation: The application runtime could not load the appropriate deployment manager for this platform.

System action: The application initialization does not complete normally.

Administrator response: Ensure that all application components are installed and properly configured for this application server platform.

CTGVS0501E A fault occurred. Review the log files for further trace information.

Explanation: An unexpected fault condition occurred. This condition cannot be handled internally.

System action: The request has been halted.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed and retry the request.

CTGVS0502W Expected message with an unexpected format *format1* **but found format** *format2* **instead.**

Explanation: An unexpected message was received.

System action: The operation did not complete.

Administrator response: Suspect applications creating these message are not compatible. Ensure the release levels of the applications support each other's formats.

CTGVS0503W Expected *format1* **metadata sections in the registration response but found** *format2* **instead.**

Explanation: A registration response with an unexpected number of metadata sections was received.

System action: The operation did not complete.

Administrator response: Investigate whether the applications creating these message are compatible. Ensure the release levels of the applications support each other's response formats.

CTGVS0504E A service named *service_name* **was not found.**

Explanation: The specified service name was not found.

System action: No action taken.

Administrator response: Request a service that exists.

CTGVS0505E The command or service specified does not exist: *command_service_name* **.**

Explanation: The command handler was not found.

System action: No action taken.

Administrator response: Retry using a different command request.

CTGVS0506E A not valid element passed to function, expected *expected name* **but found** *found name***.**

Explanation: When parsing XML, an different element to the one expected was found.

System action: Parsing halted.

Administrator response: Examine the system log, and ensure the XML being parsed is correct.

CTGVS0507E An error occurred while parsing a *element name* **XML element.**

Explanation: An error occurred while an element of the given local name was being parsed.

System action: Parsing halted.

Administrator response: Examine the system log, and ensure the XML being parsed is correct.

CTGVS0508E An error occurred while serializing data to XML.

Explanation: An error occurred while data was being serialized to XML.

System action: Serialization halted.

Administrator response: Examine the system log to determine the cause of this error.

CTGVS0509W A certificate with name *cert_name* **and expiration date** *exp_date* **was not found.**

Explanation: The certificate was expected to be in the keystore but was not found

System action: The operation did not complete.

Administrator response: Ensure the certificate has been received as a signer certificate.

CTGVS0510W A certificate with name *cert_name* **and expiration date** *exp_date* **has expired.**

Explanation: The certificate has expired and cannot be used for signature verification.

System action: The operation did not complete.

Administrator response: Refresh the certificate on the policy source machine and import it's public certificate as a signer certificate.

CTGVS0511W The element with attribute of *id_name* had a signature that is not valid .

Explanation: The signature of this element could not be verified using the public key certificate.

System action: The operation did not complete.

Administrator response: Refresh the certificate on the policy source machine and import its public certificate as a signer certificate.

CTGVS0512E An error occurred while extracting data from the configuration file. The requested element could not be found.

Explanation: An administrative command requested information from the configuration file that could not be located.

System action: Returning a failure status code to the caller.

Administrator response: Examine the request and ensure the desired section is present in the configuration file.

CTGVS0513E A context element was not found in the message headers. The context of the request can not be determined.

Explanation: A service request did not have a required ContextId element in the message header. The operation could not be fullfilled.

System action: The service request fails.

Administrator response: The source of the request is not providing the required information. Correct the sender of the request and re-try the operation.

CTGVS0514E An invalid element was supplied for parsing, expected Metadata but instead found *localName*.

Explanation: An incorrect response was received from the policy management server while retrieving a policy update.

System action: The policy update request does not complete. No new polices are retrieved.

Administrator response: Ensure that the policy management server is functioning properly and retry the operation.

CTGVS0515E An invalid element was supplied for parsing, expected MetadataSection but instead found *localName*.

Explanation: An incorrect response was received from the policy management server while retrieving a policy update.

System action: The policy update request does not complete. No new polices are retrieved.

Administrator response: Ensure that the policy management server is functioning properly and retry the operation.

CTGVS0516E The required attribute Dialect was not found on the MetadataSection element.

Explanation: An incorrect response was received from the policy management server while retrieving a policy update.

System action: The policy update request does not complete. No new polices are retrieved.

Administrator response: Ensure that the policy management server is functioning properly and retry the operation.

CTGVS0517E Invalid element supplied for parsing, expected GetMetadata but instead found *localName*.

Explanation: An incorrect response was received from the policy management server while retrieving a policy update.

System action: The policy update request does not complete. No new polices are retrieved.

Administrator response: Ensure that the policy management server is functioning properly and retry the operation.

CTGVS0518E Processing the notification message failed with the following error: *errorMsg*

Explanation: The notification message was not sent because an error occurred processing the message.

System action: Processing halted.

Administrator response: Examine the system log for more detailed information.

CTGVS0519E The required Security Assertion Markup Language (SAML) element *nodeName* has a wrong name space. Expected: *uri* **found:** *badUri*

Explanation: Failed to parse an element in an XML document. The document does not have the expected name space.

System action: Processing halted.

Administrator response: Examine the system log for more detailed information.

CTGVS0520E The required Security Assertion Markup Language (SAML) element *nodeName* was unexpected. Expected: *name*

Explanation: Failed to parse element in an XML document. The document does not have the expected element.

System action: Processing halted.

Administrator response: Examine the system log for more detailed information.

CTGVS0521E The required Security Assertion Markup Language (SAML) XML string failed to parse. Input XML string: *xmlString*

Explanation: Failed to parse the SAML assertion XML string into a document.

System action: Processing halted.

Administrator response: Examine the system log for more detailed information.

CTGVS0522E The received element <*ElementName*> does not contain the required attribute *MemberElementName*.

Explanation: Failed to parse the SAML assertion because it is missing a required attribute.

System action: Processing halted.

Administrator response: Examine the system log for more detailed information.

CTGVS1001E Cannot load the configuration file or configuration input string.

Explanation: Unable to load the configuration file or configuration input string due to invalid format. The expected document root maybe missing because the parsed configuration file does not contain the correct configuration document.

System action: The configuration request will be halted.

Administrator response: Ensure that configuration file is valid. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1002W Configuration file can not be located. A default configuration file is created.

Explanation: Unable to find the configuration file. Configuration file does not exist.

System action: A default configuration will be created.

Administrator response: New configuration file will be created. If there is a need to add additional configuration data, modify the configuration file and restart the application.

CTGVS1003E The configuration file content can not be parsed.

Explanation: The configuration file's format may be incorrect. The expected document root maybe missing because the parsed configuration file does not contain the correct configuration document.

System action: The configuration request will be halted.

Administrator response: Ensure that that configuration file is valid. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1004E Can not save the configuration data back to the configuration file.

Explanation: An exception occurred while saving configuration data to file. The configuration data's format may be incorrect or file may not exist.

System action: The configuration request will be halted.

Administrator response: Ensure that that configuration file is valid. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1005E The configuration information can not be loaded for use in the obfuscation.

Explanation: An exception occurred while loading configuration data to be used for the obfuscation. The configuration information for the obfuscation might be missing.

System action: No action taken.

Administrator response: Ensure that that configuration file is valid and contain the configuration information about the obfuscation. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1006E The application failed to perform password obfuscation.

Explanation: An exception occurred while doing password obfuscation. There might be a problem with the keystore, keystore password, or the keystore alias password.

System action: The request has been halted.

Administrator response: Verify to make sure the keystore in the installation directory and that the configuration file contains the correct information for the obfuscation. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1007E The application failed to convert an obfuscated password to the original password.

Explanation: An exception occurred while converting an obfuscated password back to the original password. There might be a problem with the keystore, keystore password or the keystore alias password.

System action: The request has been halted.

Administrator response: Verify to make sure the keystore in the installation directory and that the configuration file contains the correct information for the obfuscation. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1008E Configuration component or sub-component *compName* **either not valid or doesn't exist in the configuration file.**

Explanation: The specified component or sub-component doesn't exist in the configuration file.

System action: The request has been halted.

Administrator response: Ensure that the configuration file contains the correct information. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1009E The required property *property* **for the Policy Information Point (PIP) configuration entry** *finder* **is either invalid or does not exist in the configuration file. The PIP entry will not be registered for use.**

Explanation: Required properties might be missing or invalid for the specified PIP configuration entry.

System action: The specified PIP entry will not be registered for information lookup.

Administrator response: Ensure that the configuration file contains the correct information. Make sure all the required properties are set correctly for the PIP. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1010E Unable to obtain the application server ConfigRepository handle.

Explanation: Failed to obtain a ConfigRepository handle to modify configuration data. The Server may not be up or reachable.

System action: Unable to read or write to and from the ConfigRepository.

Administrator response: Ensure the application server environment is set up correctly and that the server is up and running. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1011E Configuration file *file* **doesn't exist.**

Explanation: Unable to find the configuration file. Configuration file does not exist.

System action: No action taken.

Administrator response: Ensure the configuration file exists. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1012E Unable to backup configuration file *filePath* **.**

Explanation: Failed to backup the configuration file. The file path might be invalid or the application server configuration repository might not be available.

System action: No action taken.

Administrator response: Ensure the configuration file exists. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS1013E Required system property user.install.root not present.

Explanation: The value for the System property user.install.root could not be obtained. Its value is required in order to determine the location to place configuration files and temporary files.

System action: The application may fail to start.

Administrator response: It is very unusual for this System property not to be present in a normal application server configuration. Ensure that it is defined.

CTGVS1014E The wrong type of configuration locator was provided.

Explanation: Each different type of environment this application is run in may require a different method of storing and access configuration information. There has been an application design limitation that has caused this mismatch.

System action: The application may fail to start.

Administrator response: The application is not running as designed. Perhaps it is running in an environment it has not been verified for.

CTGVS1015E An error occurred while establishing a connection to the DataSource name *dataSourceName*. . The data source will not be used for the storage of configuration data.

Explanation: Failed to find the configuration data source. The data source will not be used for storage of configuration.

System action: The configuration will not be stored in the database.

Administrator response: Ensure that the configuration datasource property is configured correctly in the security-services.xmi file. Ensure that the dataSource is defined correctly in the application server configuration.

CTGVS1017E The configuration data storage is not enabled.

Explanation: The configuration data storage is not enabled.

System action: The configuration will not be stored in the database.

Administrator response: Ensure that the configuration datasource property is configured correctly in the security-services.xmi file. Ensure that the dataSource is defined correctly in the application server configuration.

CTGVS1018E An error was encountered when reading the file *path* from the DB.

Explanation: Failed to read data from the DB.

System action: Failed to read data from the DB.

Administrator response: Ensure that the configuration database is setup properly and is operational. Ensure that the dataSource is defined correctly in the application server configuration.

CTGVS1019E An error was encountered when writng the file *path* into the DB.

Explanation: Failed to write in the DB.

System action: Failed to write data in the DB.

Administrator response: Ensure that the configuration database is setup properly and is operational. Ensure that the dataSource is defined correctly in the application server configuration.

CTGVS1020E An error was encountered when deleting the file *path* from the DB.

Explanation: Failed to delete data from the DB.

System action: Failed to delete data from the DB.

Administrator response: Ensure that the configuration database is setup properly and is operational. Ensure that the dataSource is defined correctly in the application server configuration.

CTGVS1501E The service named *role_name* was not found.

Explanation: The specified service name was not found.

System action: No action taken.

Administrator response: Specify a service that exists.

CTGVS1502E The *operation* request failed.

Explanation: Either a connection could not be established to the Security Policy Manager or an error condition occurred while the policy manager was processing the request.

System action: The request has been halted.

Administrator response: If a remote exception was detected, make sure that the policy manager is started. Check for port, administrator, or administrator password errors.

CTGVS1505W The registration operation for application failed.

Explanation: The tspm.configured entry missing from the security-services.xmi file. Registration operation was not done.

System action: The request has been halted.

Administrator response: The security-services.xmi file is missing the tspm.configured value. Check the security-services.xmi file to ensure that the registration stanza is defined.

CTGVS1506W Check for using HTTPS failed or no session parameters defined.

Explanation: The HTTPS.enabled value SSL session parameters were not found. An HTTP transport will be used instead.

System action: The request has been halted.

Administrator response: The security-services.xmi file is missing the HTTPS.enabled value or other HTTPS values necessary to define a session, such as keystore and keystore.password. Check the security-services.xmi file to ensure that the registration stanza is defined and has the HTTPS values defined.

CTGVS1507E An error occurred while trying to obtain a policy update.

Explanation: While trying to get a policy update, an error occurred.

System action: The request has been halted.

Administrator response: Investigate the policy update request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1508E An error occurred while trying create a URL address for the policy management service.

Explanation: While trying to create a URL address for the policy management service, an error occurred.

System action: The request has been halted.

Administrator response: Investigate the policy management service URL create request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1509W The admin command must be a string data type, it was found to be of type: *admin_cmd_data_type* **.**

Explanation: While trying to process the admin command, the command data was found to be of type admin_cmd_data_type and not of type string. The admin command cannot be processed.

System action: The request has been halted.

Administrator response: Investigate the admin command request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1510W The admin command XML string *admin_XML_string* **cannot be parsed into an element.**

Explanation: Could not parse the admin command admin_XML_string into an element. The admin command cannot be processed.

System action: The request has been halted.

Administrator response: Investigate the admin command request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1511E An error occurred while trying to initialize the handler for the *protocol name* **protocol.**

Explanation: While trying to initialize the handler to retrieve policy updates for a given protocol, an error occurred.

System action: The specified protocol will not be available.

Administrator response: Enable the finest level of logging and retry. Review the log files.

CTGVS1512E No handler was found for any of the following list of protocols: *protocol list***.**

Explanation: None of the protocols specified in the notification could be used to retrieve the update.

System action: The request has been halted.

Administrator response: Investigate the policy update request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1513E The signatures in the policy distribution could not be validated. The policy distribution request has been ignored.

Explanation: Could not validate the signature(s) in the policy distribution. This indicates a problem with the integrity of the signed distribution request.

System action: The request has been halted.

Administrator response: Investigate whether the public certificate of the policy distribution source has expired. Otherwise there is a problem with the transport integrity.

CTGVS1514E A problem with accessing the configuration file or keystore has been detected.

Explanation: A problem occurred during the opening of the keystore for signature verification.

System action: The request has been halted.

Administrator response: Investigate the service and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request. Ensure that the keystore has been defined in the security-services.xmi file of the Websphere Application Server's profile.

CTGVS1515W An update notification message could not be verified. The message notification was not handled.

Explanation: An update notification was received but the signature was either missing or could not be verified.

System action: The request has been halted.

Administrator response: Investigate the service and related settings. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request. Ensure that the keystore has been defined in the security-services.xmi file of the application server's profile.

CTGVS1517E The required argument *missing_argument* is missing from the command line.

Explanation: A required argument that was needed for this operation is missing.

System action: The request has been halted.

Administrator response: Supply the required argument and retry the command.

CTGVS1518W A property *missing_property* was not supplied, using the default property value of *default_property* for the value.

Explanation: A property was not supplied using the default property value instead.

System action: No action taken.

CTGVS1519E The argument supplied for the operation, -o flag, is not valid. choose either register,refresh, or unregister.

Explanation: Bad argument used with the -o flag.

System action: The request has been halted.

Administrator response: Supply the a valid argument with the -o flag and retry the command.

CTGVS1520W The certificate-interval was not found in the properties file, the default interval of 365 days will be used.

Explanation: No certificate-interval property was found in the properties file. Using default of 365 days.

System action: No action taken.

Administrator response: Supply the desired number of days that the certificate should be valid with the certificate-interval property and retry the command.

CTGVS1527E Could not determine the local host name. Please enter host name using the pdt-host-name property.

Explanation: Could not determine the local host's name.

System action: The request has been halted.

Administrator response: Add the pdt-host-name property and its value to the properties file and retry the command.

CTGVS1530E Exception occurred while trying to contact the policy manager.

Explanation: A communications error occurred while trying to contact the policy manager.

System action: The request has been halted.

Administrator response: Check the policy manager's name and port number. Ensure that the registration service is running on the policy manager's application server instance.

CTGVS1531E Failed to read the register properties file.

Explanation: Failed to read the properties file.

System action: No action taken.

Administrator response: Check that the application server instance is running using the same id that was used while registering the policy distribution target. If there is a mismatch, use system commands to make the id the same as what the application server instance is using and restart the application server.

CTGVS1532E Failed to delete the register properties file.

Explanation: Failed to delete the properties file.

System action: No action taken.

Administrator response: Check that the ID used to run the application server instance has write authority on the register properties file in the configuration directory. If not use system commands to grant that authority and restart the application server.

CTGVS1533W Security policy manager not configured. Please register the policy distribution target and copy the register properties file to the configuration directory and restart the application server.

Explanation: Policy distribution target not yet configured. The location of the security policy manager is missing.

System action: None

Administrator response: Create a register properties file by using the registration client and copy the properties file to the configuration directory. Restart the application server.

CTGVS1534W A registration property: *missing_prop* was missing from the registration file: reg.props, Registration aborted.

Explanation: A required registration property was missing from the registration file.

System action: No action taken.

Administrator response: Run the registration client again and fill in all parameters that are not optional. Copy the reg.props file to the configuration directory and restart the Websphere server.

CTGVS1538E Can not use both and

Explanation: The two options are incompatible. Use either one or the other.

System action: No action taken.

Administrator response: Determine which option is to be used and eliminate the other. Retry the operation with only one of the options.

CTGVS1539E The required argument *missing_property* is missing from the registration input properties file.

Explanation: A required property that is needed for this operation is missing.

System action: The request has been halted.

Administrator response: Add the missing property to the input properties file and retry the command.

CTGVS1540E The registration program version *reg_ver* does not match the version recorded in the properties file: *reg_ver*.

Explanation: A version mismatch between the properties file and the registration program was detected.

System action: The request has been halted.

Administrator response: Ensure that the correct properties template file was used to create the properties file and that the version in the file matches that reported by the registration program. Once corrected, retry the command.

CTGVS1541E The Policy Distribution Target (PDT) type defined in the properties file was not numeric.

Explanation: The PDT type when parsed was not numeric.

System action: The request has been halted.

Administrator response: Correct the PDT type and make it one of the valid integers as defined in the properties file comments. Retry the command.

CTGVS1542E The property value of *property_value* is not applicable for the *property* property.

Explanation: A required property does not have a valid value.

System action: The request has been halted.

Administrator response: See the properties template for comments on that property and the valid property values. Change the property's value and retry the command.

CTGVS1543W The Policy Distribution Target (PDT) was already unregistered.

Explanation: The policy manager's certificate was already deleted from the truststore.

System action: The request has been halted.

Administrator response: Correct the PDT type and make it one of the valid integers as defined in the properties file comments. Retry the command.

CTGVS1544W The user: *tspm_usere* could not be created in the registry. Not added to the *admin_group* group.

Explanation: The Bind distinguished name of the registry might not have write authority to the underlying registry or the user has already been created. This Policy Distribution Target (PDT) will not work correctly unless this user is created and added to the pdt-admin-group.

System action: No action taken.

Administrator response: Either configure the application server registry with a Bind distinguished name that has write access and retry the registration command or add the name manually to the registry and make it a member of the pdt-admin-group.

CTGVS1545W The user:*tspm_usere* could not be added to the pdt-admin-group: *admin_group*.

Explanation: The pdt-admin-group is defined during PDT install. The name of the group is a require property of a type 1 or 2 Policy Distribution Target (PDT) for registration. Another factor that would cause this error would be if the bind distinguished name of the registry does not have write authority to the underlying registry. This PDT will not work correctly unless the user is added to the pdt-admin-group.

System action: No action taken.

Administrator response: Check that the name defined in the PDT registration properties file is fully defined and matches the one that was created in the registry. The fully defined name may be viewed using the application server's console panel and selecting groups. The unique name would be the one that must match the property in the registration properties file. If the bind distinguishing name defined in the application server registry definition does not have write access, the name would have to be added using appropriate registry tools.

CTGVS1546W Members of group: ***group_name*** **not found.**

Explanation: Could not find the members of this group. The group may have been deleted.

System action: No action taken.

Administrator response: Reinstall the Tivoli runtime security service or create the group in the application server's registry exactly how it was defined during Tivoli runtime security service install.

CTGVS1547E An error was detected while trying to run a remote command on the web server.

Explanation: Suspect problems with the program setup or web server instance.

System action: No action taken.

Administrator response: Ensure that the bat or script that runs this program has not been changed. Check that all required jars mentioned in the bat or script exist in the locations that are defined in the file. Make sure that the application server which the program is trying to contact is running.

CTGVS1548W User ***group_name*** **not in group** *group_name*

Explanation: Suspect problems with the program setup or web server instance.

System action: No action taken.

Administrator response: Ensure that the bat or script that runs this program has not been changed. Check that all required jars mentioned in the bat or script exist in the locations that are defined in the file. Make sure that the application server which the program is trying to contact is running.

CTGVS1549W Could not setup command handler to the application server.

Explanation: The command handler is used to execute administration commands during registration.

System action: No action taken.

Administrator response: Ensure that the web server is setup and running correctly and retry the operation.

CTGVS1550W Could not delete Policy Distribution Target (PDT) certificate alias: ***alias*** **from the keystore:** ***keystore*** **during the unregister operation.**

Explanation: The deletion operation returned an error.

System action: No action taken.

Administrator response: Certificate might have been deleted already. Check the keystore to verify that the file has already been deleted.

CTGVS1551W Exception occurred during SSL port creation or deletion for pdt.

Explanation: Error occurred while trying to create or delete a SSLProf, transportchain, and alias for a Policy Distribution Target (PDT) SSL port.

System action: No action taken.

Administrator response: Create or delete the port manually using the keystore. Make sure the transport certificate uses the SSL port template. Enable certificate authentication in the QoS option of the SSLConf definition.

CTGVS1552W Error occurred while writing the registration properties file.

Explanation: A write error occurred while trying to write out the registration properties.

System action: No action taken.

Administrator response: This error might be due to a user's write authority. Check the system settings for this user, alter the settings if necessary, and retry the command.

CTGVS1553E No data was returned from server for the policy update.

Explanation: The policy update did not contain the WS-MetadataExchange Metadata element.

System action: The request has been halted.

Administrator response: Investigate the policy update request. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS1554E Could not determine local cell by looking for Node in the directory tree under ***dir_name*****.**

Explanation: Could not determine the local Cell name.

System action: The request has been halted.

Administrator response: Check the websphere-install-path and websphere-profile in the register tool's input file. These values are used to derive the local cell name. Using incorrect values could result in the local cell not being found.

CTGVS1555E The properties file passed to the register tool ***prop_file*** **was not found.**

Explanation: The properties file could not be located.

System action: The request has been halted.

Administrator response: Correct the file path and name and retry the operation.

CTGVS1556E An error has occurred that was not expected.

Explanation: An unanticipated error has occurred.

System action: The request has been halted.

Administrator response: Please run trace and/or debug. Examine the logs for advice on why this error occurred and suggestions for fixing it.

CTGVS1559W The user could not be created. If the Federated Repository is not used on the application server instance, then the id will have to be created manually in the user account repository.

Explanation: User IDs can only be created when the application is using the Federated repositories as its user account repository.

System action: None

Administrator response: Either switch the user account repository to the Federated repositories and retry the operation, or create the user ID tspm manually in the current user account repository.

CTGVS1562E An error occurred parsing the XML string for notifications. The XML input received is: *xmlString* **.**

Explanation: The string is not valid XML.

System action: Parsing halted.

Administrator response: Examine the system log, and ensure the XML being parsed is correct.

CTGVS1563E An error occurred validating the AdminCommand for policy updates. The command is missing the required command parameter PolicyDistributionEvents.

Explanation: The NOTIFYUPDATE AdminCommand expects a parameter called PolicyDistributionEvents.

System action: Parsing halted.

Administrator response: Pass in the XML string for the PolicyDistributionEvents to the AdminCommand web-service.

CTGVS1564E Incorrect Policy Distribution Target type specified.

Explanation: The Policy Distribution Target type is invalid or unknown.

System action: Execution halted

Administrator response: Provide a valid Policy Distribution Target type.

CTGVS1565E The supplied keystore: *keystorefile* **does not existor could not be read, verify the password, integrity of the file and keystore type.**

Explanation: The command was unable to find the suplied keystore file or it could not be read due to wrong passwords or file corruption.

System action: Execution halted

Administrator response: Provide a valid keystore and password.

CTGVS1566E A connection to the WebSphere server could not be established. Check the supplied properties.

Explanation: The command was unable to connect to WebSphere due to bad connection properties.

System action: Execution halted

Administrator response: Correct the connection properties that were supplied.

CTGVS1569E A reload configuration command cannot be completed due to initialization failures in the cluster.

Explanation: A reload configuration command was received but initialization failures prevented its completion.

System action: Execution halted

Administrator response: Verify the cluster configuration and the state of the nodes. Examine any logs or incident streams for information that might explain the initialization failure and correct them.

CTGVS1571W The user *user* **could not be removed from the target server registry.**

Explanation: A user for the policy distribution target could not be removed in the registry of the target WebSphere Application Server. The user should be manually removed.

System action: The operation was not performed. Processing continues.

Administrator response: Ensure that the administrator name and password are correct in the input properties If necessary, manually remove the registry user.

CTGVS1572W The user *user* could not be created in the target server registry.

Explanation: A user for the policy distribution target could not be created in the registry of the target WebSphere Application Server. This may occur if the user already exists.

System action: The operation was not performed. Processing continues.

Administrator response: Ensure that the administrator name and password are correct in the input properties and that the user does not already exist in the registry. If necessary, manually create the registry user.

CTGVS1573E The name for the policy manager server user could not be determined or was not provided.

Explanation: An attempt is made to create a user in the local registry for the policy manager server, but the user name is unknown. The user name is determined from the policy manager server public certificate.

System action: The operation was not performed. Processing does not continue

Administrator response: The certificate may be corrupt or the registration process may have encountered other errors. Check the application and system logs for the policy manager server for additional information.

CTGVS1576E The policy distribution target certificate with alias *alias* was not found in the store. The certificate could not be exported.

Explanation: An attempt to export the public certificate for the policy distribution target failed because the certificate could not be found in the key store.

System action: The save is not performed. Processing continues.

Administrator response: Manually export the certificate from the policy distribution target key store. If the auto generate option is enabled, the certificate can be found in they keystore with the alias name matching the name of the policy distribution target appended with _public.

CTGVS1577W Unable to download certificate from the remote authorization server. The certificate from endpoint URL *URL* could not be retrieved.

Explanation: An attempt to download a public certificate from the remote authorization servers SSL port failed.

System action: The operation was not performed. Processing continues.

Administrator response: Either verify the HTTPS URL for the remote authorization service in the input properties and retry the operation, or manually import the certificate into the policy distribution target key store.

CTGVS1578W An HTTPS protocol is not specified for the remote authorization server. Certificate downloading is skipped. An HTTPS port must be used.

Explanation: In a remote mode configuration if the URL for the remote authorization service uses an HTTP protocol, an attempt is made to automatically add the certificate to the policy distribution target key store.

System action: The operation was not performed. Processing continues.

Administrator response: Change the protocol for the authorization service to HTTPS URL in the input properties or the current configuration, and retry the operation.

CTGVS1579W The certificate for the remote authorization service could not be retrieved. The certificate could not be retrieved from *url* .

Explanation: In a remote mode configuration an attempt to download the public certificate of the remote authorization service into the certificate to the policy distribution target key store failed.

System action: The operation was not performed. Processing continues.

Administrator response: Ensure the that the remote server is running and that the HTTPS port is available, or manually import the certificate into the policy distribution target key store.

CTGVS1580E An unknown RTSS component *name* was specified in the input properties. The property *propertyname* must be either *rtsscomp* or *rtssclientcomp* .

Explanation: An incorrect value was set in the registration input properties.

System action: The operation was not performed. Processing does not continue.

Administrator response: Correct the input properties and retry the operation.

CTGVS1581E The runtime security services configuration file *filename* could not be loaded.

Explanation: The runtime security services configuration file could not be read.

System action: The operation was not performed. Processing does not continue.

Administrator response: Check the file permissions and path name of the input properties file and retry the operation.

CTGVS1583E The remote authorization service could not be contacted. Ensure the target server is running and available. *filename* .

Explanation: The appliation is attempting to verify that the remote runtime security server is running. The remote server could not be contacted.

System action: Processing does not continue.

Administrator response: Ensure the target server is running and available.

CTGVS2001E An error occurred while loading the policy with identifier *policy_id* .

Explanation: The policy specified by policy_id could not be loaded.

System action: The request fails with an error.

Administrator response: Investigate the policy identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2002E The policy identified by identifier *policy_id* was not found.

Explanation: The policy might not exist.

System action: The request fails with an error.

Administrator response: Investigate the policy identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2003E An error occurred while loading the policy identified by policy identifier *policy_id* .

Explanation: The policy specified by policy_id could not be loaded.

System action: The request fails with an error.

Administrator response: Investigate the policy identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2004E The policy set identified by identifier *policy_id* was not found.

Explanation: The policy set specified by policy_id was not found.

System action: The request fails with an error.

Administrator response: Investigate the policy set identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2005E The policy set identified by identifier *policy_id* was not found.

Explanation: The policy set specified by policy_id was not found.

System action: The request fails with an error.

Administrator response: Investigate the policy set identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2006E The policy version specified for identifier *policy_id* was not found.

Explanation: The policy version specified for policy_id was not found.

System action: The request fails with an error.

Administrator response: Investigate the policy identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2007E The version for identifier *identifier_id* was not found.

Explanation: The identifier version for the identifier specified by identifier_id was not found.

System action: The request fails with an error.

Administrator response: Investigate the identifier specified. Enable the finest level of logging and retry. Review the log files. Make changes as needed and retry the request.

CTGVS2008E An error occurred while trying to serialize a request object to XML.

Explanation: While trying to serializing an eXtensible Access Control Markup Language (XACML) request object to XML an error occurred.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed and retry the request.

CTGVS2009E An error occurred while creating a response object from the received XML.

Explanation: While trying to create an eXtensible Access Control Markup Language (XACML) request object from received XML data, an error occurred.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed and retry the request.

CTGVS2010E The expected eXtensible Access Control Markup Language (XACML) response data was not found in the returned message.

Explanation: While evaluating the returned message, eXtensible Access Control Markup Language (XACML) response data was expected to exist but was not found.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed and retry the request.

CTGVS2011W HTTP authentication was specified but could not complete because the required username and/or password were not specified.

Explanation: HTTP authentication was specified which requires a username and a password to be specified. However, the username and / or the password were not specified.

System action: The request fails with an error.

Administrator response: When using HTTP authentication specify a username and a password. Alternatively, consider not using HTTP authentication. Retry the operation with the necessary changes.

CTGVS2012E The Security Assertion Markup Language (SAML) is not at the required version *version_info* **.**

Explanation: The Security Assertion Markup Language (SAML) version was found to not the required version. The SAML data exchange cannot complete.

System action: The request fails with an error.

Administrator response: Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2013E The Required Security Assertion Markup Language (SAML) element *SAML_ELEMENT* **was not found, instead found** *WRONG_SAML_ELEMENT* **SAML element.**

Explanation: The Security Assertion Markup Language (SAML) element was not the required element. The data exchange could not complete.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2014E The incoming eXtensible Access Control Markup Language (XACML) request has no context specified and no default context was configured.

Explanation: The incoming XACML request does not have a context specified and there is no default context configured for the environment. The request can not be processed.

System action: The request fails with an error.

Administrator response: Specify a default context property or reconfigure the incoming request to contain a default context. Review the operating environment. Retry the operation after making the necessary changes.

CTGVS2015E An error occurred while evaluating the eXtensible Access Control Markup Language (XACML) request.

Explanation: While evaluating the incoming eXtensible Access Control Markup Language (XACML) request an error occurred. The request can not be processed.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2016E The Security Assertions Markup Language (SAML) request cannot complete due to an unfound token handler for namespace *NAMESPACE_URI* **.**

Explanation: The token handler for namespace NAMESPACE_URI could not be found. The SAML request cannot complete.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2017E An error occurred while evaluating the eXtensible Access Control Markup Language (XACML) request.

Explanation: While evaluating the incoming eXtensible Access Control Markup Language (XACML) request an error occurred. The request can not be processed.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2018E No eXtensible Access Control Markup Language (XACML) request found in Security Assertion Markup Language (SAML) request.

Explanation: Could not find XACML request in the incoming SAML query. The request can not be processed.

System action: The request fails with an error.

Administrator response: Investigate the failure by enabling the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2019E Response object's 'InResponseTo' ID *in_responseTo_id* **does not match the expected ID** *send_id* **.**

Explanation: The received ID must match the sent ID.

System action: The request fails with an error.

Administrator response: Ensure that the request is a valid request. Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2020W Response object's 'InResponseTo' Id was not found in the response.

Explanation: The Response object's 'InReponseTo' ID is missing.

System action: No action taken

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS2021W The found Security Assertion Markup Language (SAML) statement is not of the type *statement_type* **.**

Explanation: The SAML statement does not contain an XACML response.

System action: No action taken.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2022W The Security Assertion Markup Language (SAML) statement is not found in the SAML assertion

Explanation: The Security Assertion Markup Language (SAML) statement is missing from the SAML assertion.

System action: No action taken.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2023W The Security Assertion Markup Language (SAML) statement is not found in the SAML assertion

Explanation: The Security Assertion Markup Language (SAML) statement is missing from the SAML assertion.

System action: No action taken.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2024W The Security Assertion Markup Language (SAML) statement is not found in the SAML response.

Explanation: The Security Assertion Markup Language (SAML) statement is missing from the SAML response.

System action: No action taken.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2025W An error occurred while initializing the External Rule system.

Explanation: An exception was thrown while initializing the External Rule system. All External Rule functions will be disabled.

System action: External rules are disabled.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2026E The External Rule with the identifier *identifier* could not be found.

Explanation: No External Rules with the given identifier has been defined in the RTSS configuration.

System action: An exception is thrown, the result for the authorization decision is indeterminate.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2027W The External Rule with name *name* could not be loaded.

Explanation: An error occurred during while loading the External Rule with the given name. This External Rule has been disabled.

System action: The External Rule is registered. References to this External Rule at runtime will cause an error.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2028E Could not get an instance of the OSGi Extension Registry.

Explanation: A reference to the OSGi Extension Registry could not be obtained. External Rule plugins cannot be loaded.

System action: No External Rules could be loaded. References to External Rules in the policy are not resolved.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2029E The External Rule extension point *name* could not be found.

Explanation: A reference to the OSGi Extension Point for External Rules could not be obtained. External rule plug-ins cannot be loaded.

System action: External Rule plug-ins could not be loaded. References to External Rules in the policy are not resolved.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2030E The External Rule implementation with plugin identifier *id* could not be found.

Explanation: An External Rule implementation with the given plug-in identifier could not be found. This External Rule configuration cannot be loaded.

System action: This External Rule implementation is not loaded.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2031E An error occurred while instantiating the External Rule implementation *class*.

Explanation: The External Rule implementation could not be created as an exception was thrown.

System action: The External Rule implementation is not loaded.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2032W Could not create the External Rule with id *id* as one or more required configuration parameters are missing.

Explanation: The RTSS configuration does not contain one or more configuration parameters that the plug-in identified has declared as required.

System action: This External Rule will not be loaded.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2033E The required property *paramName* was not found in the configuration.

Explanation: The configuration does not contain the specified configuration parameter that the External Rule plug-in has declared as required.

System action: This External Rule will not be loaded.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2034E An invalid configuration was provided for an IdAS attribute finder. The mandatory property value *sourceProp*. was missing or not valid.

Explanation: Ensure the property value was configured. The error log contains details.

System action: Startup has been halted.

User response: Add the missing mandatory property value to the attribute finder's configuration.

CTGVS2035E The IdAS attribute finder property value for *propertyName* not correctly formated to RFC 2732 specifications.

Explanation: RFC 2732 places restrictions on the format of URI values. The provided value does not conform to these restrictions.

System action: Startup had been halted.

User response: Update the IdAS attribute finder property value to conform to RFC 2732.

CTGVS2036E The IdAS registry has not been configured to run. Thus the IdAS attribute finder is unable to use the IdAS Context Provider *contextProvider* and is unable to initialize.

Explanation: The IdAS registry must be configured in order for the IdAS attribute finders to operate.

System action: The Authorization Runtime Service startup had been aborted.

User response: Configure the IdAS registry before using IdAS attribute finders.

CTGVS2037E The IdAS registry does not recognize the context provider *propertyName*= *contextProvider*. The IdAS Attribute Finder is unable to initialize.

Explanation: The IdAS registry must have available the context provider ID in order for the IdAS Attribute Finders to operate.

System action: Startup as been halted.

User response: Update the IdAS Attribute Finder idas.context.provider property value to match a valid entry in the IdAS registry.

CTGVS2038W An unexpected error was generated while searching the IdAS context for the entity containing the attribute for the policy evaluation. The key used for the search was *keyValueString*.

Explanation: The IdAS registry generated an error that was assumed could not occur when it searched for the entity containing the policy attribute.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the IdAS registry is functioning correctly.

CTGVS2039W Multiple entities matched the key value *keyValueString*. in a search of the IdAS context. All of the entities will be ignored.

Explanation: The IdAS registry search for the entity containing the key value resulted in multiple matching entries. Only one is permitted.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the entity key values are unique to each entity.

CTGVS2040W The IdAS context reported a error while attempting to authenticate.

Explanation: IdAS Authentication provided caused an error while searching for an attribute for policy evaluation.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the configured authentication is correct in both the IdAS Attribute Finder configuration and the IdAS Registry configuration.

CTGVS2041W No entity was located using the key value *keyValueString*. during a search of the IdAS context.

Explanation: The IdAS registry search for the entity containing the key value did not produce a result.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the entity key value maps to an entity in the IdAS Context.

CTGVS2042W An unexpected error was generated while searching the IdAS context for the entity containing the attribute for the policy evaluation. The key value used for the search was *keyValueString*.

Explanation: The IdAS registry generated an unexpected error when searched for the entity containing the policy attribute.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the IdAS registry is functioning correctly. Examine the log for details of the IdASException to assist in determining the cause.

CTGVS2043W An unexpected error was generated while extracting the policy attribute from the IdAS entity. The key value used for the search was *keyValueString*.

Explanation: The IdAS registry generated an unexpected error when extracting the attribute for policy evaluation from the IdAS entity.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the IdAS registry is functioning correctly. Examine the log for details of the IdASException to assist in determining the cause.

CTGVS2044W The IdAS Context, *contextId*, either did not get created or did not open. Ensure that the hostname, port and login information is correct for the target server.

Explanation: The server or registry could not be opened or contacted, meaning the policy attribute could not be located.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the IdAS registry is functioning correctly. Examine the log for details of the exception to assist in determining the cause. Check to make sure the host name and port for the registry is correct. If using authentication, ensure the user name and password are correct.

CTGVS2045W An unexpected error was generated while processing the policy attribute from the IdAS entity. The IdAS attribute name is *returnAttributeName*.

Explanation: An unexpected error occurred when extracting the attribute for policy evaluation from the IdAS entity.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the IdAS registry is functioning correctly. Examine the log for details of the IdASException to assist in determining the cause.

CTGVS2046W An unexpected error was generated while closing the context *contextId*.

Explanation: The IdAS context generated an unexpected error when closing.

System action: Ignored.

User response: Ensure the IdAS registry is functioning correctly. Examine the log for details of the IdASException to assist in determining the cause.

CTGVS2047W The XACML return attribute type *dataType* configured for option *propertyName* is not supported.

Explanation: The IdAS attribute finder only supports a limited set of XACML Attribute types. The one configured is not one of them.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Use one of the supported XACML Attribute types.

CTGVS2048W Unable to convert the attribute value, *value* , returned from the IdAS context into the XACML data type, *dataType*.

Explanation: The IdAS attribute finder was unable to parse the value into an XACML attribute.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the configured XACML data type is correct for the IdAS attribute being returned.

CTGVS2049E Unable to configure the IdAS Registry from the file *directory/file*.

Explanation: The IdAS registry failed to configure from the supplied file.

System action: Startup has been halted.

User response: Check the file exists as specified. Check the file contains valid IdAS Registry XML configuration. Examine the logged IdAS Exception for additional details on the failure.

CTGVS2050E Unable to configure the IdAS Registry from the string supplied, *string*.

Explanation: The IdAS registry failed to configure from the supplied string.

System action: Startup has been halted.

User response: Check the string contains valid IdAS Registry XML configuration. Examine the logged IdAS Exception for additional information on the cause.

CTGVS2051E Unable to convert the IdAS registry configuration stored in the storage service into a XML String. The location of the configuration in the storage service was *serviceName*, *dialect*, *identifier*.

Explanation: The IdAS configuration extracted from the storage service must be converted into a form the IdAS registry can consume. This does not modify the data, rather transforms the form in which it is passed within the programs memory.

System action: Startup has been halted.

User response: Check the storage service entry contains valid IdAS registry XML configuration. Ensure the correct location is configured. Examine the logged exception for additional information on the cause.

CTGVS2052E An error was returned from the External Rule with name *name*.

Explanation: The XACML policy specified that an External Rule should be invoked, but the External Rule returned an error. Please consult the relevant logs for the external service to determine the cause of the error.

System action: Threw an XACMLProcessingException.

User response: Examine the logs of the external system and take action as appropriate.

CTGVS2053E Invalid arguments for the function *function* were found. At least one argument, of type *type* must be specified.

Explanation: The XACML policy specified that an External Rule should be invoked, but the required arguments were not found in the policy.

System action: This function has been marked as not valid.

User response: Ensure the required arguments for this function are specified in the policy.

CTGVS2054E The directory *directory* which was specified in the property *property* does not exist and could not be created.

Explanation: The configuration specified a directory that was not found and could not be created.

System action: The initialization operation fails.

User response: Ensure the directory specified exists and is writable by the current user.

CTGVS2055E An error occurred while deploying the XMT file that specifies the custom XACML functions for the External Rule functionality.

Explanation: A file is required in order to use custom functions for the External Rules. This file could not be automatically deployed to the file system.

System action: The initialization operation fails.

User response: Ensure the directory specified exists and is writable by the current user.

CTGVS2056E An error occurred while loading the XMT file that specifies the custom XACML functions for the External Rule functionality.

Explanation: A file is required in order to use custom functions for the External Rules. This file could not be read.

System action: The initialization operation fails.

User response: Ensure the directory specified exists and is writable by the current user.

CTGVS2057E An error occurred while registering Policy Information Point (PIP) entry *pipName*.

Explanation: The configuration information for the (PIP) entry might be not valid or does not exist.

System action: The initialization operation fails.

User response: Ensure that the configuration file contains the correct information. Make sure all the required properties are set correctly for the PIP. Enable the finest level of logging and retry the request. Review the log files. Make changes as needed and retry the request.

CTGVS2058E A URL for the remote authorization service was not provided.

Explanation: The configuration value for the authz.http.url property has not been set.

System action: The initialization operation fails. Remote authorization requests will not function properly.

User response: Set the authz.http.url property to a valid authorization service URL.

CTGVS2059W HTTP authentication has been enabled, but a user name was not provided.

Explanation: The configuration value for the authz.http.user property has not been set.

System action: Basic authentication for remote authorization requests is disabled. Remote authorization requests will not function properly if application security has been enabled.

User response: Set the authz.http.user property to a valid user ID.

CTGVS2060W HTTP authentication has been enabled, but a password was not provided.

Explanation: The configuration value for the authz.http.password property has not been set.

System action: Basic authentication for remote authorization requests is disabled. Remote authorization requests will not function properly if application security has been enabled.

User response: Set the authz.http.password property to a valid user password.

CTGVS2061E An XACML Response is expected but not found in the response message.

Explanation: A remote authorization request returned an unexpected response. The authorization request fails.

System action: The authorization request fails with a SOAP exception.

User response: Set the authz.http.url property to a valid IBM Runtime Security Service authorization service URL.

CTGVS2062E Both ldapsearch.prefix and ldapsearch.baseDn must be specified, but only one of the attributes was found for attribute finder *pipName*.

Explanation: Both ldapsearch.prefix and ldapsearch.baseDn must be specified, but only one of the attributes was found in the configuration.

System action: The attribute finder did not load.

User response: Configure either bot ldapsearch.prefix and ldapsearch.baseDnh or neither.

CTGVS2063E Unable to dynamically create an IdAS JNDI Context for attribute finder *pipName*. The error reported was *causeText*.

Explanation: A problem occurred while dynamically adding an IdAS JNDI context provider configuration into the IdAS Registry.

System action: The attribute finder failed to load.

User response: Examine the cause error for possible causes. Also check the configuration for the attribute finder is correct.

CTGVS2064E Substring match (*) is not supported in search filters for Attribute Finder *pipName*.

Explanation: Limitations in the LDAP implementation do not allow for substring matching.

System action: No attributes will be returned from the search.

User response: Reformulate the LDAP search filter to remove any substring (*) usage.

CTGVS2065E Approximate match (~=) is not supported in search filters for attribute finder *pipName*.

Explanation: Limitations in the LDAP implementation do not allow for approximate matching.

System action: No attributes will be returned from the search.

User response: Reformulate the LDAP search filter to remove any approximate match (~=) usage.

CTGVS2066E Extensible matches are not supported in search filters for attribute finder *pipName*.

Explanation: Limitations in the LDAP implementation do not allow for extensible matching.

System action: No attributes will be returned from the search.

User response: Reformulate the LDAP search filter to remove any extensible match usage.

CTGVS2067E An unknown element type *filterComponentType* was encountered in the search filter for attribute finder *pipName*.

Explanation: An unsupported LDAP operator was specified in the LDAP search filter.

System action: No attributes will be returned from the search.

User response: Reformulate the LDAP search filter to avoid the problem.

CTGVS2068E getEvaluationTarget() method not supported by RTSSProviderImpl class.

Explanation: An unsupported method was invoked. This is an internal coding error.

System action: No action taken.

User response: Investigate the logs to determine if another error caused this error.

CTGVS2069E A thread already has a lock on this repository.

Explanation: The policy repository cannot satisfy a policy retrieval request.

System action: No action taken.

User response: If the problem persists, restart the application.

CTGVS2070E The thread does not have a lock on this repository to release.

Explanation: The policy repository cannot complete a policy retrieval request.

System action: No action taken.

User response: If the problem persists, restart the application.

CTGVS2071E A configuration that is not valid was supplied to the STS attribute finder. A request type URI, and either an issuer or a appliesTo or both must be specified to be able to construct a valid STS request.

Explanation: Add the request type, issuer and/or appliesTo to the STS attribute configuration.

System action: Startup has been halted.

User response: Add the missing required property value to the configuration for the attribute finder.

CTGVS2072E A configuration that is not valid was supplied to the STS attribute finder. The required attribute *attribute* is missing.

Explanation: Add the required attribute to the configuration for the attribute finder.

System action: Startup has been halted.

User response: Add the missing required property value to the configuration for the attribute finder.

CTGVS2073E Unable to parse the security token from the XACML request. No attributes will be returned from the search.

Explanation: An error occurred while parsing the security token from the XACML request. The security token is used as part of the STS request that is sent to the STS for attribute retrieval.

System action: No attributes will be returned from the search.

User response: Investigate the logs to determine if another error caused this error.

CTGVS2074E An error occurred when calling the STS from the attribute finder.

Explanation: Check the STSConfigurations to make sure the STS configuration is setup correctly. Either the STS could not be contacted due to a configuration problem or the chain was not found on the STS server.

System action: No attributes will be returned from the search.

User response: Check the logs to determine the configuration problem.

CTGVS2075E The STS response status indicates that it is not valid. The response returned is *response*.

Explanation: Check the STS response to determine why the status is not valid.

System action: No attributes will be returned from the search.

User response: Check the logs for more information.

CTGVS2076E A protocol violation occurred parsing the SAML token.

Explanation: The SAML token is not in the expected format as described by the Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1.

System action: No attributes will be returned from the search.

User response: Check the logs for more information on why the token did not parse as expected.

CTGVS2077W Unable to convert the attribute value, *value* **into the XACML data type,** *dataType* **, as specified in the policy.**

Explanation: The STS attribute finder was unable to parse the value into an XACML attribute.

System action: The attribute for the policy evaluation will be assumed to be missing.

User response: Ensure the configured XACML data type is correct in the policy for the STS attribute.

CTGVS2078E Could not get an instance of the OSGi Extension Registry.

Explanation: A reference to the OSGi Extension Registry could not be obtained. Custom Attribute Finder plug-ins cannot be loaded.

System action: No Custom Attribute Finders could be loaded. References to Custom Attribute Finders in the policy will not be resolved.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2079E The Custom Attribute Finder extension point *name* **could not be found.**

Explanation: A reference to the OSGi Extension Point for Custom Attribute Finders could not be obtained. Custom Attribute Finder plug-ins cannot be loaded.

System action: No Custom Attribute Finders could be loaded. References to Custom Attribute Finders in the policy will not be resolved.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2080E The Custom Attribute Finder implementation with plug-in identifier *id* **could not be found.**

Explanation: A Custom Attribute Finder implementation with the given plug-in identifier could not be found. This Custom Attribute Finder configuration cannot be loaded.

System action: This Custom Attribute Finder implementation is not loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2081E An error occurred while instantiating the Custom Attribute Finder implementation *class***.**

Explanation: The Custom Attribute Finder implementation could not be created as an exception was thrown.

System action: The Custom Attribute Finder implementation is not loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2082W Could not create the Custom Attribute Finder with ID *id* **because one or more required configuration parameters are missing.**

Explanation: The runtime security services configuration does not contain one or more configuration parameters that the identified plug-in has declared as required.

System action: This Custom Attribute Finder will not be loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2083E The required property *paramName* was not found in the configuration.

Explanation: The runtime security services configuration does not contain the specified configuration parameter that the Custom Attribute Finder plug-in has declared as required.

System action: This Custom Attribute Finder will not be loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2084E The data type supplied for attribute instantiation was null.

Explanation: When creating an attribute, a data type parameter must be sent from the plug-in to the AttributeFactory. If this parameter is null, the attribute cannot be created.

System action: The attribute cannot be created.

Administrator response: Identify the plug-in that has failed to create an attribute. Examine its implementation and ensure the parameters it uses to instantiate attributes are valid.

CTGVS2085E The supplied data type *paramName* is not a supported attribute type.

Explanation: The data type supplied for creating an attribute is not a supported attribute type.

System action: The attribute will not be created.

Administrator response: Identify the plug-in that has failed to create an Attribute. Examine its implementation and ensure the parameters it uses to instantiate Attributes are valid.

CTGVS2086E Both search prefix and base DN must be specified, but only one of the pair was found.

Explanation: Ensure the search prefix and the base DN are configued in the properties. The error log contains details.

System action: The query for the external attribute is not performed. The operation is aborted with a denied access decision.

User response: Verify that the configuration for the external attribute query is correct.

CTGVS2087E An error occurred while connecting to the LDAP server at host *hostName*. Ensure the address and authentication credentials are correct.

Explanation: Ensure the address and authentication credentials are correct. The error log contains details.

System action: The query for the external attribute is not performed. The operation is aborted with a denied access decision.

User response: Verify that the configuration for the external attribute query is correct.

CTGVS2088E An invalid configuration was provided for an LDAP attribute finder. The mandatory attribute *sourceProp*. was missing or invalid.

Explanation: Ensure the property value was configured. The error log contains details.

System action: The query for the external attribute is not performed. The operation is aborted with a denied access decision.

User response: Verify that the configuration for the external attribute query is correct.

CTGVS2089E The search string *filter* was not found on server *hostName* with base context *baseDN* for the finder with Issuer *issuer*.

Explanation: No value was returned by the query. The error log contains details.

System action: The query for the external attribute is not performed. The operation is aborted with a denied access decision.

User response: Verify that the configuration for the external attribute query is correct.

CTGVS2090E An error occurred while retrieving AttributeId *attributeID* with Issuer*issuer*.

Explanation: No value was returned by the query. The error log contains details.

System action: The query for the external attribute is not performed. The operation is aborted with a denied access decision.

User response: Verify that the configuration for the external attribute query is correct.

CTGVS2091E Cannot get an instance of the OSGi Extension Registry.

Explanation: A reference to the OSGi Extension Registry cannot be obtained.

System action: No action was taken.

Administrator response: Enable the most granular level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Make necessary changes and retry the operation.

CTGVS2092E Cannot find the Obligation Handler extension point *name*.

Explanation: Cannot obtain a reference to the OSGi Extension Point for the Obligation Handler.

System action: No action was taken.

Administrator response: Enable the most granular level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Make necessary changes and retry the operation.

CTGVS2093E Cannot find the Obligation Handler implementation with plugin identifier *id*.

Explanation: Cannot find an Obligation Handler implementation with the specified plug-in identifier. The Obligation Handler configuration cannot be loaded.

System action: The Obligation Handler configuration is not loaded.

Administrator response: Ensure that the Obligation Handler configuration is correctly defined in the security-services.xmi configuration file. Enable the most granular level of logging and retry the operation. Review the log files. Make necessary changes and retry the operation.

CTGVS2094E An error occurred while instantiating the Obligation Handler implementation *class*.

Explanation: Cannot create the Obligation Handler implementation because an error occurred.

System action: The Obligation Handler implementation is not loaded.

Administrator response: Ensure that the Obligation Handler configuration is correctly defined in the security-services.xmi configuration file. Enable the most granular level of logging and retry the operation. Review the log files. Make necessary changes and retry the operation.

CTGVS2095W Cannot create the Obligation Handler with ID *id* because one or more required configuration parameters are missing.

Explanation: The RTSS configuration does not contain one or more configuration parameters that the specified plug-in requires.

System action: This Obligation Handler will not be loaded.

Administrator response: Ensure that the Obligation Handler configuration is correctly defined in the security-services.xmi configuration file. Enable the most granular level of logging and retry the operation. Review the log files. Make necessary changes and retry the operation.

CTGVS2096W Cannot load the Obligation Handler with name *name*.

Explanation: An error occurred while loading the Obligation Handler with the specified name. This Obligation Handler has been disabled.

System action: The Obligation Handler is not registered. References to this Obligation Handler at runtime will cause an error.

Administrator response: Ensure that the Obligation Handler configuration is correctly defined in the security-services.xmi configuration file. Enable the most granular level of logging and retry the operation. Review the log files. Make necessary changes and retry the operation.

CTGVS2097E The required property *paramName* was not found in the configuration.

Explanation: The configuration specified by the plug-in does not contain the configuration parameter that the plug-in requires.

System action: The obligation handler plug-in is not loaded.

Administrator response: Ensure that the plug-in configuration parameters declared in the plugin.xml file are correctly defined in the security-services.xmi configuration file. Enable the most granular level of logging and try the operation again. Review the log files. Make necessary changes and try the operation again.

CTGVS2098W Obligation Handler with ID *obligationId* returned the following error - *errorFromHandler*

Explanation: The configured Obligation Handler with the specified ID returned an error.

System action: For an authorization decision an INDETERMINATE response will be sent to the PEP. For an entitlement request, the particular entitlement that triggered the Obligation Handler will be removed from the response.

Administrator response: The configured Obligation Handler returned an error. Enable the most granular level of logging and retry the operation. Review the log files. Review the operating environment and ensure components are at the required levels. Make necessary changes and retry the operation.

CTGVS2099W The Obligation Handler class *classname* returned a value of FALSE for the passed in obligation ID *obligationId*. The obligation will be returned to the Policy Enforcement Point.

Explanation: The configured Obligation Handler class returned a value of FALSE for the specified obligation string.

System action: No action was taken.

Administrator response: No administrative action is required.

CTGVS2100W The following attribute cannot be converted to a proper format *attributeName*.

Explanation: This attribute will not be sent to the Policy Enforcement Point because there was an error converting it to a proper format.

System action: No action was taken.

Administrator response: Enable the most granular level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Make necessary changes and retry the operation.

CTGVS2101W Obligation ID *obligationId* is already mapped to the Obligation Handler ID *id*. Failed to create a new Obligation Handler because the Obligation Handler with name *name* is configured with an Obligation ID that is already mapped to an existing Handler.

Explanation: An Obligation ID can only be mapped to one Obligation Handler. If the Obligation ID is specified in multiple handlers, then only the first Obligation Handler is registered.

System action: No action was taken.

Administrator response: Make necessary changes to the specified Obligation Handler in the security-services.xmi file. Retry the operation.

CTGVS2200E Failed to load the configuration from the directory *directory path* because the directory does not exist.

Explanation: The configuration was not loaded because the specified directory path is incorrect.

System action: No action was taken.

Administrator response: Specify the correct directory path and try the operation again.

CTGVS2201E Failed to load the configuration from the properties file *file path*.

Explanation: The configuration was not loaded because the specified file does not exist or is not correctly set up.

System action: No action was taken.

Administrator response: Ensure that the specified file exists and is set up correctly. Make necessary changes and try the operation again.

CTGVS2202E Failed to load the configuration because the system property com.ibm.tscc.rtss.dir was not specified.

Explanation: The configuration was not loaded because the required system property was not specified.

System action: No action was taken.

Administrator response: Ensure that the system property specifies the location of the directory where the configuration file exists and is set up correctly. Make necessary changes and try the operation again.

CTGVS2203E Failed to load the configuration because the basic authentication username (authz.http.user property) or the password (authz.http.password property) is not specified in the properties file.

Explanation: The configuration was not loaded because the required system properties were not specified. For the basic authentication method, specify the value for both username and password in the client properties file.

System action: No action was taken.

Administrator response: If basic authentication is used to authenticate the client, ensure that both the username (authz.http.user property) and the password (authz.http.password property) are specified in the configuration file. Make necessary changes and try the operation again.

CTGVS2205E Failed to validate the specified rtssEndpoint URL *url*.

Explanation: The program exited because no valid rtssEndpoint URL was specified.

System action: No action was taken.

Administrator response: Ensure that a valid URL is specified for the rtssEndpoint argument. Make necessary changes and try the operation again.

CTGVS2206E Failed to validate the specified truststore path *trustStorePath*.

Explanation: The program exited because no valid truststore was specified.

System action: No action was taken.

Administrator response: Ensure that a valid file path is specified as the truststore argument. Make necessary changes and try the operation again.

CTGVS2207W A new truststore file will be created because the specified truststore *trustStorePath* does not exist.

Explanation: A new truststore file will be created because the specified truststore does not exist.

System action: No action was taken.

Administrator response: None.

CTGVS2208E Failed to load the specified truststore *trustStorePath*.

Explanation: The specified truststore could not be created or loaded.

System action: No action was taken

Administrator response: Ensure that a valid file path is specified as the value of truststore argument. Make necessary changes and try the operation again.

CTGVS2211E Failed to obtain a server certificate chain from host *host* and port *port* .

Explanation: An attempt to retrieve a certificate from a remote SSL port failed.

System action: The operation was not performed. Program will exit.

Administrator response: Ensure that a valid URL is specified for the rtssEndpoint argument. Make necessary changes and try the operation again. If necessary, manually import the certificate into the truststore.

CTGVS2213E The program failed to import the certificate.

Explanation: Failed to import the server certificate due to some errors.

System action: The operation was not performed. Program will exit.

Administrator response: Review the errors. Make necessary changes and try the operation again.

CTGVS2214W Failed to write the configuration properties file *file path*.

Explanation: The program obfuscates the passwords in the properties file and writes the file to the file system. The program failed to write the specified properties file.

System action: No action was taken.

Administrator response: Ensure that the user that the program is running under has write permissions on the specified file. Make necessary changes and retry the operation.

CTGVS2215W The remote client location information could not be added to the request context.

Explanation: The IP address or host name of a remote client that is making an authorization request could not be determined. Authorization decisions that rely on this information might not yield expected results, and audit records might be incomplete.

System action: The information is not added to the authorization request context. Processing continues.

Administrator response: Check the network environment for possible domain name resolution problems and try the operation again.

CTGVS2216E Could not access the OSGi extension registry.

Explanation: A reference to the OSGi extension registry could not be obtained. External rule, custom policy information point, or obligation handler plug-ins cannot be loaded.

System action: A reference to the internal OSGi extension registry could not be obtained. References to external rule, policy information point, or obligation handler plug-ins are not loaded.

Administrator response: Enable the most granular level of logging and try the operation again. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Make the necessary and try the operation again.

CTGVS2217E The extension point *name* could not be found.

Explanation: A reference to an OSGi extension point could not be obtained. The plug-in is not loaded.

System action: The code extension is not loaded. The extension could be a reference to a custom external rule, policy information point, or obligation handler plug-in. References to unresolved external rules in the policy are not resolved and might yield unexpected authorization decision results.

Administrator response: Enable the most granular level of logging and try the operation again. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Make the necessary and try the operation again.

CTGVS2218W Failed to obfuscate the password in configuration properties file *file path*.

Explanation: The program obfuscates the passwords in the properties file and writes the file to the file system. The program failed to obfuscate the password in the specified properties file.

System action: No action was taken.

Administrator response: Ensure that the user has the write permissions on the specified properties file. Make necessary changes and retry the operation.

CTGVS2503E The audit service encountered an error while creating audit event.

Explanation: The audit service encountered a failure while creating an audit event record. This failure does not constitute a failure in other aspects of the product. The audit record in question, and subsequent audit records, may be lost. In order to prevent further audit system errors, take action before continuing to use the system.

System action: No action taken.

Administrator response: Check the audit service parameters and ensure that the device capturing audit records is available and healthy.

CTGVS2504E The audit service encountered an error while writing an audit record.

Explanation: The audit service encountered a failure while logging an audit event record. This failure does not constitute a failure in other aspects of the product. The audit record in question, and subsequent audit records, may be lost. In order to prevent further audit system errors, take action before continuing to use the system.

System action: No action taken.

Administrator response: Check the audit service parameters and ensure that the device capturing audit records is available and healthy.

CTGVS2505W The audit log configuration parameter *identifier* is missing.

Explanation: The audit service was unable to locate the specified configuration parameter used to configure the logging of audit event records to a file. File logging will be disabled until this problem is corrected. In order to prevent loss of audit data, take action before continuing to use the system. This failure does not constitute a failure in other aspects of the product.

System action: No action taken.

Administrator response: Check the audit service configuration and ensure that all configuration parameters are present and set to valid values.

CTGVS2506W The audit log configuration parameter *identifier* is set to an incorrect value.

Explanation: The setting of the specified configuration parameter used to configure the logging of audit event records to a file is not valid. When correcting this, please check the Administration Guide for the valid range of values for this parameter.

System action: File logging will be disabled until this problem is corrected.

Administrator response: In order to prevent loss of audit data, take action before continuing to use the system. Check the audit service configuration and ensure that all configuration parameters are present and set to valid values.

CTGVS2508W Audit file logging directory could not be created.

Explanation: The directory location configured to contain audit log files could not be created. File logging will be disabled until this problem is corrected. In order to prevent loss of audit data, take action before continuing to use the system. This failure does not constitute a failure in other aspects of the product.

System action: No action taken.

Administrator response: If the specified location already exists, verify that it is a directory and is writeable. If the specified directory does not exist, verify that file system permissions allow it to be created.

CTGVS2509E The file handler used for writing audit records to log files could not be created.

Explanation: An exception was thrown while creating the file handler. File logging will be disabled until this problem is corrected. In order to prevent loss of audit data, take action before continuing to use the system. This may indicate a system environment problem that could affect other aspects of the product.

System action: No action taken.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2510E The file handler used for writing audit records to log files threw an exception.

Explanation: An exception was thrown by the file handler when writing to audit log files. In order to prevent loss of audit data, take action before continuing to use the system. This may indicate a system environment problem that could affect other aspects of the product.

System action: No action taken.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2512W The audit log configuration could not be located.

Explanation: The audit service was unable to locate the specified configuration used to configure the logging of audit event records to a file. File logging will be disabled until this problem is corrected. In order to prevent loss of audit data, take action before continuing to use the system. This failure does not constitute a failure in other aspects of the product.

System action: No action taken.

Administrator response: Check the audit service configuration and ensure that all configuration parameters are present and set to valid values.

CTGVS2513E The audit log configuration could not be written to the configuration file.

Explanation: The audit service was unable to write the specified audit configuration to the configuration file. Audit logging will be disabled until this problem is corrected. In order to prevent loss of audit data, take action before continuing to use the system. This may indicate a system environment problem that could affect other aspects of the product.

System action: No action taken.

Administrator response: Another exception or message was created with details of the error. Enable the finest level of logging and retry the operation. Review the log files and make changes as needed. Review the operating environment and ensure components are at the required levels. Review the configuration settings and ensure they are all present and correct. Retry the operation after making the necessary changes if desired.

CTGVS2656E The ISAM Syslog handler could not be created.

Explanation: The syslog audit event handler could not be created. Audit events will not be routed to a remote syslog daemon.

System action: The audit service started, but the syslog audit event handler could not be created. The default file-based event handler will be used.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2657E Could not get an instance of the OSGi extension registry.

Explanation: A reference to the OSGi extension registry could not be obtained. External audit event handler plugins cannot be loaded.

System action: A define audit event handler could not be loaded. The default file-based event handler will be used.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2658E Multiple extensions found for the audit event handler. Only one will be used.

Explanation: The audit service supports only a single event handler for capturing audit events. Multiple event handler extensions were detected on service start-up. The first event handler provided by the OSGi framework is used.

System action: The audit service will use the first available audit handler service provided by the OSGi registry. Other handler plug-ins are ignored. The handler selected by the OSGi registry is arbitrary and may may change between restarts.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2659E The audit event handler extension could not be created.

Explanation: The audit handler extension class could not be instantiated. The default file-based handler will be used to capture audit events.

System action: The audit handler extension class could not be instantiated. The default file-based handler is used to capture audit events.

Administrator response: Consult the provider of the audit handler plug-in. Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2660E The auditing service could not be started. Auditing is disabled.

Explanation: An error occured while trying to start the auditing service.

System action: The audit service could not be started. Auditing is disabled. Access and administrative events are not recorded.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS2661E The event handler extension point *name* could not be found.

Explanation: A reference to an OSGi extension point could not be obtained. Audit event handler plug-ins cannot be loaded.

System action: Audit event handler plug-ins are not loaded. The default file-based handler will be used to capture audit events.

Administrator response: Enable the finest level of logging and retrying the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes if desired.

CTGVS3501E The base storage directory *directory* was not created.

Explanation: An attempt to create a directory in the file system for the policy repository failed.

System action: No action taken.

Administrator response: Ensure that the file system permissions are adequate for the services runtime directory in the configuration repository and restart the application.

CTGVS3502W The default policy for the administrative services might not have been added.

Explanation: At application startup a check made to ensure that default policy for the runtime services agent application is populated. A system error occurred either during the check or while the default policy was being deployed.

System action: No action taken.

Administrator response: If web services enforcement point is preventing policy distribution updates from completing, Ensure that the file system permissions are adequate for the services runtime directory in the configuration repository and restart the application.

CTGVS3503E The policy for file *file* could not be added to the policy repository.

Explanation: An attempt to add policy to the repository failed.

System action: No action taken.

Administrator response: Ensure that the file system permissions are adequate for the services runtime directory in the configuration repository and restart the application.

CTGVS3504E The policy for file *file* could not be parsed.

Explanation: An attempt to load policy from an XML source failed.

System action: No action taken.

Administrator response: Ensure that the source is a valid policy file and retry the operation.

CTGVS3505E The policy for identifier *identifier* of dialect *dialect* in service *service* was not added.

Explanation: An attempt to save policy with the named identifiers from an XML source failed.

System action: No action taken.

Administrator response: Ensure that the source file is a valid policy file that the file system permissions are adequate and retry the operation.

CTGVS3506E The directory *directory* does not exist and could not be created.

Explanation: An attempt to create a directory on the local file system failed.

System action: No action taken.

Administrator response: Ensure that the file system permissions are adequate create the directory tree and retry the operation.

CTGVS3507E The file *file* could not be created.

Explanation: An attempt to a file on the local file system failed.

System action: No action taken.

Administrator response: Ensure that the file system permissions are adequate create the file retry the operation.

CTGVS3508E The index file in directory *directory* could not be read.

Explanation: An attempt to a locate a file in the policy repository failed. The index file containing the location of the target file either does not exist or could not be read. The policy repository might be corrupted.

System action: No action taken.

Administrator response: Ensure that the directory and index file exists and have proper permissions for reading. If the target policy file does not exist redistribute the policy and retry the operation.

CTGVS3509E The index file in directory *directory* could not be saved.

Explanation: An attempt to a save a file to the policy repository failed. The index file containing the location of the target file could not be created.

System action: No action taken.

Administrator response: Ensure that the directory and index file exists and have proper permissions for writing. If the target policy file does not exist redistribute the policy and retry the operation.

CTGVS3510E The database-backed policy storage service has been enabled but no DataSource property has been configured under the components Storage, subComponents Database, items Connection.

Explanation: The database-backed policy storage service has not been completely configured and is missing the DataSource property.

System action: The policy storage service will not be started.

Administrator response: Add the DataSource property to the security-services.xmi file.

CTGVS3511E An error occurred while establishing a connection to the DataSource with JNDI name *dataSourceName*.

Explanation: Unable to lookup the specified DataSource.

System action: The policy storage service will not be started.

Administrator response: Ensure the correct value for the DataSource property is in security-services.xmi.

CTGVS3512E An error occurred while verifying the existence of the database table *_databaseTable*.

Explanation: The startup will determine if the table exists in the database using the SQL query SELECT NAME FROM SYSIBM.SYSTABLES WHERE NAME=?. The table was not found. Note that the table does not need to exist as the program will attempt to create it if it is not present.

System action: The error will be ignored.

Administrator response: If a table property was explicitly supplied in security-services.xmi, ensure that is a valid value. If this property is not explicitly specified it will default to the value RTSS_POLICY.

CTGVS3513E An error occured while creating database table *_databaseTable*.

Explanation: The startup will determine if the table exists in the database using the SQL query SELECT NAME FROM SYSIBM.SYSTABLES WHERE NAME=?. The table was not found. Note that the table need not exist as the program will attempt to create it if it is not present.

System action: The error will be ignored.

Administrator response: If a table property was explicitly supplied in security-services.xmi, ensure that is a valid value. If this property is not explicitly specified it will default to the value RTSS_POLICY.

CTGVS3514E An error occurred while adding policy with identifier *identifier* for service *serviceName* of dialect *dialect* to the database.

Explanation: An error occurred while adding policy to the database.

System action: The error will be ignored and the policy will not be added.

Administrator response: Examine the error to determine the cause and correct this. You may then need to reinvoke the operation that caused the policy to be added as the last attempt failed.

CTGVS3515E An error occurred while removing policy version *version* with identifier *identifier* for service *serviceName* of dialect *dialect* from the database.

Explanation: An error occurred while attempting to delete the policy from the database.

System action: The error will be ignored and the policy, if it existed, will not be removed.

Administrator response: Examine the error to determine the cause and correct this. You may then need to reinvoke the operation that caused the policy to be removed as the last attempt failed.

CTGVS3516E An error occurred while removing policy with identifier *identifier* for service *serviceName* of dialect *dialect* from the database.

Explanation: An error occurred while attempting to delete the policy from the database.

System action: The error will be ignored and the policy, if it existed, will not be removed.

Administrator response: Examine the error to determine the cause and correct this. You may then need to reinvoke the operation that caused the policy to be removed as the last attempt failed.

CTGVS3517E An error occurred while removing policy for service *serviceName* of dialect *dialect* from the database.

Explanation: >An error occurred while attempting to delete the policy from the database.

System action: The error will be ignored and the policy, if it existed, will not be removed.

Administrator response: Examine the error to determine the cause and correct this. You may then need to reinvoke the operation that caused the policy to be removed as the last attempt failed.

CTGVS3518E An error occurred while retrieving the latest version of policy with identifier *identifier* for service *serviceName* of dialect *dialect* from the database.

Explanation: The specified policy may not exist in the database.

System action: The error will be ignored and the policy will be assumed not to exist.

Administrator response: Examine the error to determine the cause and correct this.

CTGVS3519E An error occurred while performing the SQL query *query*.

Explanation: An attempt to query information from the database used to store the policy failed.

System action: The error will be ignored and the query will be assumed to have returned no matching entries.

Administrator response: Examine the error to determine the cause and correct this error.

CTGVS3520E An error occurred while reading policy from storage file *storageFile*.

Explanation: Unable to read or parse the policy in the storage file

System action: The error will be ignored and the policy will be assumed to not exist.

Administrator response: Examine the error to determine the cause and correct this.

CTGVS3521E An error occurred while reading policy from storage file *storageFile*.

Explanation: Unable to read or parse the policy in the storage file

System action: The error will be ignored and the policy will be assumed to not exist.

Administrator response: Examine the error to determine the cause and correct this.

CTGVS3522E Unable to commit policy update changes to the configuration repository. The causal error message is *localizedMessage*.

Explanation: The changes required to make a policy update (remove, add) are collected and sent as one transaction to the configuration repository. The single repository update request failed and will not be retried.

System action: A runtime exception will be thrown and the operation will not be completed.

Administrator response: This error might be caused by simultaneous updates with other policy updates. Reduce the number of simultaneous updates and try again.

CTGVS3523E Unable to get a connection to the configuration repository.

Explanation: The application requested a connection to the WebSphere Configuration Repository in which it stores policy. The connection was not available.

System action: A runtime exception will be thrown and the operation will not be completed.

Administrator response: During server startup connections to the deployment manager configuration repository are not usually available. Restart the application once the server has completed the startup sequence to allow the operation to succeed.

CTGVS3524E Unable to list files in the configuration repository directory *pathname*.

Explanation: The application requested a listing of files in the application server's configuration repository where it stores policy. This request failed.

System action: A runtime exception will be thrown and the operation will not be completed.

Administrator response: Examine the error logs for a cause and correct this.

CTGVS3525E Unable to extract the contents of the file *pathname* from the configuration repository.

Explanation: The application requested a listing of files in the application server's configuration repository where it stores policy. This request failed.

System action: A runtime exception will be thrown and the operation will not be completed.

Administrator response: Examine the error logs for a cause and correct it.

CTGVS3526E The received notification contains an unknown update class *className*.

Explanation: This is an implementation problem, an unexpected code path was executed.

System action: A runtime exception will be thrown and the operation will not be completed.

Administrator response: Examine the error logs for a cause and correct this.

CTGVS4001E The parameter list for command *command* is not valid.

Explanation: The required parameter is missing for the specified command or the specified parameter contains a value that is not valid.

System action: The request failed.

Administrator response: Investigate the specified and related settings. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS4003E The list configuration command for *compType* failed.

Explanation: The configuration file might not be valid or does not exist.

System action: The request failed.

Administrator response: Ensure that the configuration file exists and contains valid data. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS4005E The component *compItem* could not be retrieved from the configuration file.

Explanation: The configuration file or the requested component might not be valid or does not exist.

System action: The request failed.

Administrator response: Ensure that the configuration file exists and contains valid data. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS4006E The configuration component *comp* could not be deleted from the configuration file.

Explanation: The configuration file or the requested components might not be valid or do not exist.

System action: The request failed.

Administrator response: Ensure that the configuration file exists and contains valid data. Make changes as needed and retry the request. Enable the finest level of logging and retry. Review the log files.

CTGVS4007E Unable to retrieve the product information.

Explanation: The product information is not available.

System action: The request failed.

Administrator response: Enable the finest level of logging and retry. Review the log files.

CTGVS5501E An error occurred when accessing the Trust Service. Verify that the Trust Service configuration is correct.

Explanation: An error occurred accessing the Trust Service or the Trust Service returned an error response.

Administrator response: Check the logs and ensure the configuration is correct.

CTGVS5502E The STS runtime provider plugin with id *pluginId* could not be loaded.

Explanation: An error occurred loading the STS plugin.

Administrator response: Check the STS configuration for the plugin in the security-services.xmi file to ensure the plugin id is correct.

CTGVS5503E Could not get an instance of the OSGi Extension Registry.

Explanation: A reference to the OSGi Extension Registry could not be obtained. STS runtime provider plugins cannot be loaded.

System action: STS runtime provider plugins could be loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5504E The STS runtime provider extension point *name* could not be found.

Explanation: A reference to the OSGi Extension Point for the STS runtime provider could not be obtained. STS runtime provider plug-ins cannot be loaded.

System action: STS runtime provider could not be loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5505E The STS runtime provider implementation with plugin identifier *id* could not be found.

Explanation: An STS runtime provider implementation with the given plug-in identifier could not be found. This STS configuration cannot be loaded.

System action: This STS runtime provider implementation is not loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5506E An error occurred while instantiating the Security Token Service (STS) runtime provider implementation *class* .

Explanation: The STS runtime provider implementation could not be created and an exception was thrown.

System action: The STS runtime provider implementation is not loaded.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5507E An error occurred while parsing the WS-TRUST Security Token Service (STS) response.

Explanation: The Security Token Service (STS) response could not be parsed and an exception was thrown.

System action: The call to the STS failed and processing halted.

Administrator response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5508E An STS runtime provider could not be located with the configuration ID of *configId*

Explanation: An attempt was made to retrieve an STS plugin with a given configuration ID. The plugin was not found. This means that either the configuration identifier passed in is not valid or the plugin failed to load during startup.

System action: An STS runtime provider is not available.

User response: Enable the finest level of logging and retry the operation. Review the log files. Make changes as needed. Review the operating environment and ensure components are at the required levels. Retry the operation after making the necessary changes.

CTGVS5509E The SOAP endpoint passed in the SOAP client is not valid. The passed-in value was *parameter* .

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Make sure that the correct

SOAP endpoint URL is configured.

CTGVS5510E An error occurred in initializing SSL with the SOAP endpoint.

Explanation: The server might not be enabled for SSL. The SSL parameters passed in might not be valid.

System action: The request will be halted.

Administrator response: Validate the SSL configuration of the partner for the SOAP back channel.

CTGVS5511E The TrustStore identifier passed in SOAPClientImpl is null. The SSL connection with the endpoint *parameter* **cannot be initialized.**

Explanation: The current request is not valid.

System action: The request will be halted.

Administrator response: Validate the SSL configuration of the partner for the SOAP back channel.

CTGVS5512E The trust store cannot be initialized from the passed in identifier *parameter* **.**

Explanation: The trust store parameter passed in is not valid.

System action: The request will be halted.

Administrator response: Validate the SSL configuration of the partner for the SOAP back channel.

CTGVS5513E The SOAP client is unable to parse the response SOAP message.

Explanation: The SOAP client was unable to parse the incoming response SOAP message.

System action: The request will be halted.

Administrator response: Validate the Access Control List configuration in the destination endpoint.

CTGVS5514E The Client keystore cannot be initialized from the passed in identifier *parameter* **.**

Explanation: The client keystore parameter passed in is not valid.

System action: The request will be halted.

Administrator response: Validate the SSL configuration of the partner for the SOAP back channel.

CTGVS5515E The SOAP client is unable to send the request SOAP message.

Explanation: The SOAP client was unable to send the outgoing request SOAP message.

System action: The request will be halted.

Administrator response: Validate the Access Control List configuration in the destination endpoint.

CTGVS5516E Unobfuscation of the basic authentication password for SOAP client authentication failed.

Explanation: Unobfuscation of the basic authentication password for SOAP client authentication failed.

System action: The request will be halted.

Administrator response: Check the logs for a runtime exception.

CTGVS5517E Unable to construct a SOAP fault because the required parameter *parameter* **was null.**

Explanation: A constructor of a SOAP fault attempted to build it without the required parameter.

System action: The SOAP fault will not be built.

Administrator response: Check the logs for a runtime exception.

CTGVS5518E An error was returned from the Trust Service: *parameter*

Explanation: The Trust Service returned a SOAP fault in the response.

System action: An exception is returned from the Trust Service client and processing is halted.

Administrator response: Check the logs for a runtime exception.

CTGVT1584E The key store *name* **could not be loaded.**

Explanation: The specified key store for the policy distribution target could not be created or loaded.

System action: Processing halts.

Administrator response: Check the input properties. Ensure all path names are correct and retry the operation.

CTGVT1585E A key store with with path *name* **could not be opened.**

Explanation: An attempt was made to open a key store with a specified path and password.

System action: Processing halts. The operation was not performed.

Administrator response: Check the input properties. Ensure all path names are correct and retry the operation.

CTGVT1586E Unable to remove alias *alias* from key store *keystore* .

Explanation: A certificate with a specified alias could not be removed from a key store.

System action: Processing halts. The operation was not performed.

Administrator response: Check the input properties. Ensure all path names are correct and retry the operation.

CTGVT1587E An incorrect value for the authorization client mode was specified (*property* = *value*). If specified the value must be one of localremote or configuration .

Explanation: An unrecognized value for the the authorization service mode was specified in the input properties.

System action: Processing halts. The operation was not performed.

Administrator response: Check the input properties. Ensure the value is one of 'local', 'remote', or 'configuration'.

CTGVT1588E A mandatory parameter was not specified.

Explanation: A malformed administrative command was submitted.

System action: Processing halts. The operation was not performed.

Administrator response: If the administrative command was submitted by the policy management server, ensure that all components are at the same version. Check logs for any errors or warnings prior to this error.

CTGVT1589E Authorization failed for *name* . User not in specified role: *role*

Explanation: The named user is not mapping to the property security role.

System action: Processing halts. The operation was not performed.

Administrator response: Change the user and group to role mapping for the application to allow access.

CTGVT1590E Authorization failed for Insufficient configuration specified. Required parameter *parameter* was either null or not provided.

Explanation: A required parameter for the method was either empty or null.

System action: Processing halts. The operation was not performed.

Administrator response: Correct the input data and retry the operation.

CTGVT1591E Insufficient policy identification data was specified. A required parameter was either null or not provided.

Explanation: A required parameter for the method was either empty or null.

System action: Processing halts. The operation was not performed.

Administrator response: Correct the input data and retry the operation.

Chapter 5. Risk-based Access Messages

These messages are provided by the Risk-based Access component.

FBTRBA001E A database error occurred.

Explanation: An unrecoverable database error occurred.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA008E Creation of database connection failed. Check the database configuration and network connectivity to the database server.

Explanation: The database connection could not be created.

System action: Command execution is halted.

Administrator response: Ensure that the database is configured correctly. Also check that the network connectivity to the database server is available.

FBTRBA0100E The action: *action* failed because the resource [*resource*] was not found.

Explanation: The requested action on the specified resource could not be completed because the resource was not found.

System action: No action necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0101E The import cannot be performed while another import is in progress.

Explanation: The system can only perform one import operation at a time.

System action: The new import operation request was ignored.

Administrator response: Retry the new import operation after the original import operation is completed.

FBTRBA0106E The action *action* failed because the resource ID [*id*] is not valid for a resource of type: [*type*].

Explanation: The requested action on the specified resource could not be completed because the resource ID is invalid.

System action: No action is necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0107E The action *action* failed for resource [] because the request body contains improperly structured JSON.

Explanation: The requested action on the specified resource could not be completed because the request body contains malformed or improperly structured JSON.

System action: No action is necessary.

Administrator response: Ensure that the request body contains the appropriately structured JSON for the requested action.

FBTRBA0108W The update failed because the resource was not found.

Explanation: The requested action on the specified resource could not be completed because the resource was not found.

System action: No action necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0109W The resource already exists.

Explanation: The requested action on the specified resource could not be completed because the resource already exists.

System action: No action necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0111E The user *userID* does not have any registered devices.

Explanation: The requested user does not have any devices registered.

System action: No action necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0113E No devices last used before *timestamp* were found.

Explanation: No devices last used before the requested timestamp were found.

System action: No action necessary.

Administrator response: Ensure that the resource and action requested are valid.

FBTRBA0114E The file export failed.

Explanation: The file export failed. This can occur if the file does not exist, there are access permissions either at the source or destination, or because there was an I/O error.

System action: No action is necessary.

Administrator response: Examine the logs for the cause of the exception. Ensure that the file exists, that access permissions are set properly, and that there is sufficient space to export the file.

FBTRBA0115E The file import failed.

Explanation: The file import failed. This can occur if the file does not exist, there are access permissions either at the source or destination, or because there was an I/O error.

System action: No action is necessary.

Administrator response: Examine the logs for the cause of the exception. Ensure that the file exists, that access permissions are set properly, and that there is sufficient space to import the file.

FBTRBA0116E The filter string is empty.

Explanation: The filter query parameter has an empty value.

System action: No action is necessary.

Administrator response: If filtering is required add valid content to the value of the filter field.

FBTRBA0117E The filter contains unknown java.sql.Types [*filterObj*]. Supported values are *supportedValues*.

Explanation: An unknown or unsupported java.sql.Types type was passed into the filter.

System action: No action is necessary.

Administrator response: If filtering is required use supported java.sql.Types.

FBTRBA0118E The filter format is not valid. Filters should be in the format of *supportedValues*.

Explanation: An invalid filter syntax was used.

System action: No action is necessary.

Administrator response: If filtering is required use supported format.

FBTRBA0119E No matching field name for [*jsonFieldName*] was found.

Explanation: An invalid filter syntax was used.

System action: No action is necessary.

Administrator response: If filtering is required use supported format.

FBTRBA011E The risk-based access deployment failed.

Explanation: An error occurred during risk-based access deployment.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA0120E The filter function: *function* is not valid. Supported functions are: *supportedFunctions* .

Explanation: An invalid filter type was used.

System action: No action is necessary.

Administrator response: If filtering is required use supported format.

FBTRBA0121E The action failed because the policy is contained in one or more policy sets. The policy sets are [*policySetNames*].

Explanation: The action is not allowed when the policy is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy and retry the action.

FBTRBA0122E The action failed because the policy set is attached to one or more resources. The resources are [*policySetName*].

Explanation: The action is not allowed when the policy set is referenced by another resource.

System action: No action necessary.

Administrator response: >Remove references to the policy set and retry the action.

FBTRBA0127E The table type *unsupportedTable* is not supported. Supported types are: *supportedTables*.

Explanation: An unsupported table type was specified.

System action: No action necessary.

Administrator response: Specify a supported table type.

FBTRBA0128E The resource ID *resourceId* does not exist within the table *supportedTables*.

Explanation: A resource relationship was specified with a resource that does not exist.

System action: No action necessary.

Administrator response: Specify an existing resource.

FBTRBA0129E The obligation with the URI *obligationUri* does not exist.

Explanation: The specified obligation URI does not exist.

System action: No action necessary.

Administrator response: Specify an existing obligation URI.

FBTRBA012E The risk-based access deployment failed because it could not determine the directory in which IBM Tivoli Federated Identity Manager is installed.

Explanation: See message.

System action: Command execution is halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA0130E The attribute with the combination of URI: *attrUri*, datatype: *dataType*, and issuer: *issuer* does not exist.

Explanation: The specified combination of URI, datatype and issuer does not exist.

System action: No action necessary.

Administrator response: Specify an existing URI, datatype and issuer combination..

FBTRBA0131E The attribute with the combination of URI: *attrUri*, and datatype: *dataType* does not exist.

Explanation: The specified combination of URI and datatype does not exist.

System action: No action necessary.

Administrator response: Specify an existing URI and datatype combination..

FBTRBA0132E The action failed because the attribute is used in one or more policies. The policies are [*policyNames*].

Explanation: The action is not allowed when the attribute is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the attribute and retry the action.

FBTRBA0134E The action failed because the obligation is used in one or more policies. The policies are [*policyNames*].

Explanation: The action is not allowed when the obligation is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the obligation and retry the action.

FBTRBA0136E No obligation URI associated with the ID: *oblId*.

Explanation: A delete operation of an obligation that does not exist is not allowed.

System action: No action necessary.

Administrator response: Specify a valid obligation ID to delete.

FBTRBA0138E The action failed because the attribute is included in a risk profile or policy. The risk profiles are [*profileNames*]. The policies are [*policyNames*].

Explanation: The action is not allowed when the attribute is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the attribute and retry the action.

FBTRBA0139E The action failed because the attribute is included in one or more risk profiles. The risk profiles are [*profileNames*].

Explanation: The action is not allowed when the attribute is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the attribute and retry the action.

FBTRBA0141E A predefined resource cannot be deleted or modified. The resource is [*resourceName*].

Explanation: Predefined resources cannot be modified or deleted.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA0142E The action failed because the policy is contained in a policy set or attached to a resource. The policy sets are [*policySetNames*]. The resources are [*policyAttachmentNames*].

Explanation: The action is not allowed when the policy is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy and retry the action.

FBTRBA0143E The action failed because the policy is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation: The action is not allowed when the policy is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy and retry the action.

FBTRBA0144E The action failed because the policy set is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation: The action is not allowed when the policy set is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy set and retry the action.

FBTRBA0145W Unable to obtain authenticated user name. Setting user name to: *unauthnUser*.

Explanation: Failed to get a value while attempting to get the authenticated user from the Subject or Principal objects

System action: No action necessary.

Administrator response: Try authenticating with a valid user.

FBTRBA0146E The JavaScript mapping rule that you submitted is not valid. The JavaScript validator reported a syntax error at line *line* and column *column* with the message: *message*.

Explanation: The JavaScript mapping rule that you submitted is not valid. You can only submit a valid JavaScript mapping rule.

System action: The JavaScript mapping rule is rejected.

Administrator response: Submit a valid JavaScript mapping rule.

FBTRBA0147E The data type [*type*] in the XACML policy is not supported. Supported types are: *dataTypes*.

Explanation: The data type passed in is not supported.

System action: The XACML string is rejected.

Administrator response: Submit a valid data type within the XACML string.

FBTRBA0148E A predefined resource cannot be deleted. The resource is [*resourceName*].

Explanation: Predefined resources of this type cannot be deleted.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA0149E The configuration property cannot be modified because it is a read-only property.

Explanation: Read-only configuration cannot be modified.

System action: The modification operation is rejected.

Administrator response: No action necessary.

FBTRBA0150E The data type of the configuration property is not valid. The data type is: *dataType*.

Explanation: The configuration property data type is not supported.

System action: The modification operation is rejected.

Administrator response: No action necessary.

FBTRBA0151E The configuration property value is not valid. Valid values are: ***validValues*****.**

Explanation: The configuration property value is not valid.

System action: The modification operation is rejected.

Administrator response: No action necessary.

FBTRBA0152E The field [***inputFieldName*****] is not valid for sorting. Valid fields are:** ***validFields***

Explanation: An invalid field name was used for sorting.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA0160E A delete cannot be performed while another delete is in progress.

Explanation: The system can perform only one delete operation at a time.

System action: The new delete operation request was ignored.

Administrator response: Retry the new delete operation after the original delete operation is completed.

FBTRBA049E The runtime property ac.request.server is not configured.

Explanation: To make cross-domain AJAX requests, the runtime property ac.request.server must be configured.

System action: The CORS headers are not set in the HTTP response.

Administrator response: Configure the runtime property ac.request.server.

FBTRBA058E The attribute name, ***name*****, is invalid and is not configured.**

Explanation: The attribute validation failed because the attribute is not configured.

System action: Command execution is halted.

Administrator response: Configure the attribute.

FBTRBA069E The type for the attribute ***id*** **is not specified.**

Explanation: An attribute and its type must be specified must be specified before referencing the attribute. Valid types are integer, double, string, time, or date.

System action: Command execution is halted.

Administrator response: Specify the type for the attribute in the XACML rules file.

FBTRBA079E The attribute collection service GET method is not enabled.

Explanation: The property ac.get.attributes.enabled must be set to true in order to use the attribute collection service's GET method.

System action: No attributes were retrieved from the database.

Administrator response: Set the property ac.get.attributes.enabled to true in order to use the attribute collection service's GET method.

FBTRBA080E This client is not allowed to access the attribute collection service's GET method.

Explanation: Only clients listed in the ac.get.attributes.allowed.clients property may access the attribute collection service's GET method.

System action: No attributes were retrieved from the database.

Administrator response: Add this client to the list of allowed clients or reaccess from an allowed client.

FBTRBA085E Line number: ***line number*** **Lines must be formatted as country,region,city,postal code,metro code,start IP,end IP.**

Explanation: An invalid format was found in the custom location data file on the specified line number. Lines must be formatted as country,region,city,postal code,metro code,start IP,end IP.

System action: Custom location data was not loaded.

Administrator response: Fix the custom location file and redeploy.

FBTRBA086E Line number: ***line number*** **Start IP and end IP must be valid IP addresses.**

Explanation: An invalid value was found for start IP or end IP on the specified line number. The value must be a valid IPv4 or IPv6 address.

System action: Custom location data was not loaded.

Administrator response: Fix the custom location file and redeploy.

FBTRBA086W The IP reputation threshold configuration property is not valid. The default value of ***default value*** **will be used in place of the invalid value.**

Explanation: An invalid value was found for the ip.reputation.threshold configuration property. Valid values include any integer from 0 to 100.

System action: The default value was used.

Administrator response: Set the ip.reputation.threshold property to any valid value and reload risk-based access.

FBTRBA087E The update of this resource requires the *field name* field to have an *value type* value present.

Explanation: There was a required value missing in one of the fields. Refer to the exception for which fields and types are missing.

System action: Add the required input to payload.

Administrator response: Add a value of the correct type to the update to request payload.

FBTRBA088E The update of the resource [*name*] failed.

Explanation: During the update operation of the resource, a database exception was encountered.

System action: Ensure that the database is running correctly.

Administrator response: See the exception in the logs for the cause.

FBTRBA089E The delete of the resource failed.

Explanation: During the delete operation of the resource, a database exception was encountered.

System action: Ensure that the database is running correctly.

Administrator response: See the exception in the logs for the cause.

FBTRBA090E The delete failed because the resource cannot be found.

Explanation: During the delete operation, the specified resource was not found.

System action: See the exception in the logs for the cause.

Administrator response: Verify that the resource exists.

FBTRBA091E The retrieval failed because the resource cannot be found.

Explanation: During the get operation, the specified resource was not found.

System action: See the exception in the logs for the cause.

Administrator response: Contact your system administrator regarding the database exception.

FBTRBA092E The retrieval of the [*resourceType*] resources failed.

Explanation: During the retrieval operation, the specified resource was not found.

System action: See the exception in the logs for the cause.

Administrator response: Contact your system administrator regarding the database exception.

FBTRBA093E The creation of the [*resourceType*] resources failed.

Explanation: During the create operation, there was either a key violation or an internal server error.

System action: See the exception in the logs for the cause.

Administrator response: Contact your system administrator regarding the database exception.

FBTRBA094E The generation of an ID from the KEYS table for resource type [*resourceType*] failed.

Explanation: During the creation of the resource ID, there was an internal server error.

System action: See the exception in the logs for the cause.

Administrator response: Contact your system administrator regarding the database exception.

FBTRBA095E The value '*constraintValue*' for [*constraintName*] already exists.

Explanation: The creation or update of the resource failed because a value within your request, that is required to be unique, already exists.

System action: See the exception in the logs for more details.

Administrator response: Specify a different value for the resource constraint.

FBTRBA096E The profile [*nameValue*] is active. Active profiles cannot be deleted.

Explanation: Attempted to delete an active profile. An active profile cannot be deleted.

System action: No action necessary.

Administrator response: Update the profile so that it is not active, and then delete it.

FBTRBA097E The JDBC connection failed. Check the logs for more information.

Explanation: The connection object was null. There might be a data source or database problem.

System action: Check the data source and database configuration. Also, check the help information for your database.

Administrator response: Check the data source and database configuration.

FBTRBA098E The value '*value*' for [*propertyName*] is not valid. Valid values are: *validValues*

Explanation: The specified value is not valid.

System action: No action necessary.

Administrator response: Ensure that you are using the allowed values for this column.

FBTRBA099E The delete of the attribute failed because it is included in one or more risk profiles. The risk profiles are: *profileNames***.**

Explanation: The delete of the attribute failed because it is used by another risk profile.

System action: No action necessary.

Administrator response: To delete this attribute, first remove this attribute from all risk profiles.

FBTRBA102E The geolocation file must be a .zip file.

Explanation: The import only supports .zip files.

System action: The geolocation data in the database was not changed.

Administrator response: Import the geolocation data in a .zip file.

FBTRBA103E The data within the geolocation .zip file is not valid.

Explanation: The .zip file must contain two files. The name of one of the files must contain the word Location. The name of the other file must contain the word Blocks.

System action: The geolocation data in the database was not changed.

Administrator response: Upload a .zip file that contains two properly named files.

FBTRBA153E The update of the resource [*resourceRequestUri*] failed.

Explanation: During the update operation of the resource, a database exception was encountered.

System action: Ensure that the database is running correctly.

Administrator response: See the exception in the logs for the cause.

FBTRBA154E An attribute with the internal ID of [*attrId*] was not found.

Explanation: An attribute with the specified attribute ID does not exist.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA155E The resource request did not include a valid CSRF token or the request CSRF token did not match the server CSRF token.

Explanation: The CSRF token parsed from the request was either null or did not match with the stored version on the server.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA156E An exception was encountered while parsing the CSRF token from the resource request.

Explanation: The resource request did not match the format expected and caused a CSRF parsing error.

System action: No action necessary.

Administrator response: No action necessary.

FBTRBA164E The device *name* **was not removed.**

Explanation: The device could not be deleted.

System action: No devices were deleted.

Administrator response: No action necessary.

FBTRBA166E The device *name* **could not be updated.**

Explanation: The device could not be updated.

System action: No devices were updated.

Administrator response: No action necessary.

FBTRBA168E The HMAC OTP secret key could not be reset.

Explanation: The secret key could not be reset.

System action: The secret key was not reset.

Administrator response: No action necessary.

FBTRBA169E The value [*uri*] is not a valid URI.

Explanation: The requested value is not a valid URI.

System action: The requested action was not performed.

Administrator response: Ensure the requested value is a valid URI.

FBTRBA179E Communication with the policy server failed with the following command error: *cmdErr*.

Explanation: Communication with the policy server failed.

System action: Ensure that all back end servers are running.

Administrator response: The database, policy manager and webseal server(s) could be down.

FBTRBA180E The http method used to submit the request is not valid. The valid method is [*valid HTTP Method*].

Explanation: Submit the request using the supported http method.

System action: The request has been halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA181E The consent to register device process failed..

Explanation: The consent to register device process did not complete.

System action: The request has been halted.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA182E The value '*value*' is not valid.

Explanation: The specified value is not valid.

System action: The requested action was not performed.

Administrator response: Ensure the requested value is a valid.

FBTRBA183E The value '*value*' for [*propertyName*] is not valid.

Explanation: The specified value is not valid.

System action: The requested action was not performed.

Administrator response: Ensure the requested value is valid.

FBTRBA184E The value for '*propertyName*' is missing.

Explanation: A required property value is missing.

System action: No action necessary.

Administrator response: Ensure that the property value is specified

FBTRBA185E A request *method uri* was denied due to the cluster configuration. Write operations are available only on the master node.

Explanation: The requested URL value is not a master node.

System action: The requested URL value is not a master node.

Administrator response: To perform management operations please make requests to the management nodes URL.

FBTRBA186E A device named '*device name*' already exists.

Explanation: Device names must be unique.

System action: No action necessary.

Administrator response: Specify a unique name for the device.

FBTRBA187E The value for [*propertyName*] is too long.

Explanation: The length of the string for the property is too long.

System action: No action necessary.

Administrator response: Specify a shorter length string

FBTRBA188E The value specified for device name is too long.

Explanation: The length of the string for the device name is too long.

System action: No action necessary.

Administrator response: Specify a shorter length string

FBTRBA189E The value [*value*] specified for device name is not valid.

Explanation: The specified value is not valid.

System action: The requested action was not performed.

Administrator response: Ensure the requested value is valid.

FBTRBA190W The device registration process failed for user [*value*];

Explanation: The device registration process did not complete.

System action: The device will not be registered.

Administrator response: Check the server logs for more details to trace the cause of the error.

FBTRBA191E The definition does not exist.

Explanation: The definition does not exist.

System action: No action necessary.

Administrator response: Ensure that the definition exists.

FBTRBA192E The minimum length for the client shared-secret is <*number*> characters.

Explanation: The length of the client shared-secret in the response file does not meet the required length.

System action: No action taken.

Administrator response: Ensure that the client shared-secret meets the minimum length requirement.

FBTRBA193E The value for [*propertyName*] is not valid.

Explanation: The specified value is not valid.

System action: The requested action was not performed.

Administrator response: Ensure the requested value is valid.

FBTRBA194E The policy type [*inputFieldName*] is not valid. Valid types are: *validFields*.

Explanation: The policy type is invalid.

System action: The requested action was not performed.

Administrator response: Ensure the policy type is valid.

FBTRBA195E The action failed because the definition is referenced by a client or attached to a resource. The clients are [*clientNames*]. The resources are [*policyAttachmentNames*].

Explanation: The action is not allowed when the definition is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the definition and retry the action.

FBTRBA196E The action failed because the definition is referenced by one or more clients. The clients are [*clientNames*].

Explanation: The action is not allowed when the definition is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the definition and retry the action.

FBTRBA197E The action failed because the definition is attached to one or more resources. The resources are [*policyAttachmentNames*].

Explanation: The action is not allowed when the definition is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the definition and retry the action.

FBTRBA198E The authorization grant *state_id* could not be updated.

Explanation: The authorization grant could not be updated.

System action: No authorization grants were updated.

Administrator response: No action necessary.

FBTRBA200E The authorization grant *state_id* was not removed.

Explanation: The authorization grant could not be deleted.

System action: No authorization grants were deleted.

Administrator response: No action necessary.

FBTRBA202E The policy information point property *pipProperty* cannot be modified because it is a read-only property.

Explanation: Read-only policy information point property cannot be modified.

System action: The modification operation is rejected.

Administrator response: No action necessary.

FBTRBA203E The action failed because the policy information point is associated with one or more attributes. The attributes are [*attributeNames*].

Explanation: The action is not allowed when the policy information point is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy information point and retry the action.

FBTRBA204E The REST service returned an unexpected error code: [*error code*]

Explanation: An error was received while calling the REST service.

System action: Processing of the attribute was halted.

Administrator response: Verify that the REST service is functioning properly.

FBTRBA205E The attribute finder for attribute [*attribute name*] returned no values.

Explanation: The REST service did not return a value for the requested attribute.

System action: The attribute value was set to the empty string.

Administrator response: Verify that the REST service is functioning properly.

FBTRBA206E The required property [*configuration property*] does not exist in the configuration.

Explanation: The configuration for a required property is missing.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Configure the missing property.

FBTRBA207E The required property [*configuration property*] for instance [*instance name*] contains an HTTP header delimiter, but it is not in the correct format.

Explanation: The format for HTTP headers is incorrect.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Verify the HTTP header configuration.

FBTRBA210E The property [*configuration property*] for instance [*instance name*] contains an unsupported URI scheme.

Explanation: The specified URI scheme is invalid.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Verify the URI scheme in the REST service URL.

FBTRBA211E The property [*configuration property*] for instance [*instance name*] is not a valid URL.

Explanation: A properly formatted URL must be specified for the REST service.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Verify the REST service URL configuration.

FBTRBA212E The property [*configuration property*] for instance [*instance name*] has an invalid value.

Explanation: A property is configured with an invalid value.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Verify the PIP instance configuration.

FBTRBA213E The property [*configuration property*] for instance [*instance name*] has an invalid integer value.

Explanation: The property must be configured to a valid integer value.

System action: PIP initialization could not complete, so the PIP was disabled.

Administrator response: Verify the PIP instance configuration.

FBTRBA214E The policy information point could not be created or updated because the attribute [*attribute*] was not found.

Explanation: The requested action on the policy information point could not be completed because an attribute was not found.

System action: No action necessary.

Administrator response: Ensure that the attribute is valid and exists.

FBTRBA215E The action failed because the policy information point type is associated with one or more policy information points. The policy information points are [*pips*].

Explanation: The action is not allowed when the policy information point type is referenced by another resource.

System action: No action necessary.

Administrator response: Remove references to the policy information point type and retry the action.

FBTRBA216E The policy information point could not be created or updated because the policy information point type [*pipType*] was not found.

Explanation: The requested action on the policy information point could not be completed because a policy information point type was not found.

System action: No action necessary.

Administrator response: Ensure that the policy information point type is valid and exists.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing, or distributing application programs that conform to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Product Number: 5725-L52

Printed in USA

GC27-6210-01