Event Codes

SP1Access Manager Appliance 4.0 SP1

May 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About NetIQ Corporation 5
About This Book and the Library 7

1 Event Code Overview 9

2 Administration Console (009) 11

3 Identity Server (001) 49

4 Linux Access Gateway Appliance(045) 91

5 Access Gateway Service (046) 93

6 SSL VPN Server (005) 99

7 Policy Engine (008) 103

8 SOAP Policy Enforcement Point (011) 109

9 Backup and Restore (010) 115

10 Novell Modular Authentication Class (012) 121

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

About This Book and the Library

The *Event Codes Guide* is intended to help you understand and resolve any issues with the event codes that are displayed on error pages or logged in files.

- Chapter 1, "Event Code Overview," on page 9
- Chapter 2, "Administration Console (009)," on page 11
- Chapter 3, "Identity Server (001)," on page 49
- Chapter 4, "Linux Access Gateway Appliance(045)," on page 91
- Chapter 5, "Access Gateway Service (046)," on page 93
- Chapter 6, "SSL VPN Server (005)," on page 99
- Chapter 7, "Policy Engine (008)," on page 103
- Chapter 8, "SOAP Policy Enforcement Point (011)," on page 109
- Chapter 9, "Backup and Restore (010)," on page 115
- Chapter 10, "Novell Modular Authentication Class (012)," on page 121

Intended Audience

This book is intended for Access Manager Appliance administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

- Extensible Markup Language (XML)
- Simple Object Access Protocol (SOAP)
- Security Assertion Markup Language (SAML)
- Public Key Infrastructure (PKI) digital signature concepts and Internet security
- Secure Socket Layer/Transport Layer Security (SSL/TLS)
- Hypertext Transfer Protocol (HTTP and HTTPS)
- Uniform Resource Identifiers (URIs)
- Domain Name System (DNS)
- Web Services Description Language (WSDL)

Other Information in the Library

The library provides the following information resources:

- *NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide*
- *NetIQ Access Manager Appliance 4.0 Identity Server Guide*
- *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*
- *NetIQ Access Manager Appliance 4.0 SP1 Policy Guide*
- *NetIQ Access Manager Appliance 4.0 Setup Guide*

NOTE: Contact namsdk@netiq.com for any query related to Access Manager SDK.

1 Event Code Overview

Event codes for Access Manager Appliance consist of 4 fields that describe the type of code and the module that produced it:

- Severity (1 digit)
  - 1 = severe - Describes problems that needs to be resolved in order for the system to run correctly.
  - 2 = error - Describes that a failure occurred, but the system is operational.
  - 3 = warn - Describes a situation that may exist that the administrator should be aware of and may need to address. The system is currently running properly
  - 4 = config - Describes configuration related information.
  - 5 = info - Describes events that occur.
  - 6 = debug - Describes execution points within the software.
  - 9 = internal - Describes an error that is for internal use only. This error code will not be documented in any public documentation.
- Component issuing the error code (3 digits)
- Sub-grouping for further classification within a component (2 digits)
- Event code (three digits)

0	000	00	000
Severity	**Component field**	**Sub-grouping**	**Event Code**

The following sections divide the event codes by component, then describe them:

- Chapter 1, “Event Code Overview,” on page 9
- Chapter 2, “Administration Console (009),” on page 11
- Chapter 3, “Identity Server (001),” on page 49
- Chapter 4, “Linux Access Gateway Appliance(045),” on page 91
- Chapter 5, “Access Gateway Service (046),” on page 93
- Chapter 7, “Policy Engine (008),” on page 103
- Chapter 8, “SOAP Policy Enforcement Point (011),” on page 109
- Chapter 9, “Backup and Restore (010),” on page 115
- Chapter 10, “Novell Modular Authentication Class (012),” on page 121

2 Administration Console (009)

Component 009

- Subgroup 01: Certificate Manager
- Subgroup 02: Application
- Subgroup 03: Platform
- Subgroup 04: Web UI
- Subgroup 05: Roma Application
- Subgroup 06: Policy

Event Code	*Description*	**Remedy**
	Application	
100901001	Error getting web manager.	**Cause:** The Administration Console was not installed correctly or has become corrupt. **Action:** Verify installation.
100901002	Error in initializing the dirCerts APIs.	**Cause:** The Administration Console was not installed correctly or has become corrupt. Specifically, the PKI and/or certificate management jars may be missing or have mismatched versions. **Action:** Verify that the `certmgr.jar` file is contained in the `/var/opt/novell/tomcat4/webapps/roma/WEB-INF/lib` directory and that PKI has been installed. Verify that the Java command line contains the following: `-Djava.library.path=/opt/novell/lib` Verify that `npki.jar` is in the classpath.
100901003	Error in init.	**Cause:** The Administration Console was not installed correctly or has become corrupt. **Action:** Verify installation.
100901004	Error in CertHandler.getMultipartParamValue.	**Cause:** Servlet error when retrieving data from a multipart form. **Action:** Submit log to Novell Support for analysis and resolution.

Event Code	*Description*	**Remedy**
100901008	Could not remove certificate with the given alias from the keystore.	**Cause:** The keystore that contains the certificate might not exist or might have become corrupt. **Action:** View the configuration store and find the keystore object and check that the certificate is no longer in the key list. If it is there, manually remove it. Also, find the keystore on the file system of the device and remove the key manually, using the Java keytool program for JKS keystores.
100901010	Error In CertHandler.doGetSigningCertDN.	**Cause:** Unable to retrieve the DN of the signing cert. **Cause:** The signing cert does not exist. **Cause:** The signing keystore does not exist. **Action:** View the Identity Server Configuration's Signing keystore to verify that it exists and contains a certificate. If the signing keystore does not exist, there has been an error during the import of an Identity Server or during the creation of an Identity Server Configuration. Check to make sure that there are no corrupt Identity Server configurations. If the signing keystore does exist, add or replace a certificate.
100901011	Error in creating or configuring one or more of the Identity Server Configuration cluster keystores.	**Cause:** Test certificates might have been accidentally deleted from the file system. **Cause:** Error communicating with the Identity Server(s) while pushing down the test certificates. **Action:** Use the exception stack trace to discover a more detailed description of the error. Go to the Certificates tab and verify that the test-connector, test-signing, test-encryption, test-provider, test-consumer certificates have not been deleted. Also verify they still exist on the file system. Go to the Trusted Roots tab and verify that the configCA trusted root has not been deleted and that it exists in the configuration store. These test certificates are pushed down to each Identity Server during the creation of an Identity Server configuration. You can delete the Identity Server configuration and create a new one and add the Identity Servers back into the new configuration.

Event Code	*Description*	**Remedy**
100901012	keystore already exists.	**Cause:** You are trying to create a keystore that already exists on the device. **Action:** Use the existing keystore.
100901013	Error in init (using reflection to call a method has failed in init).	**Cause:** The java class is unable to locate another java class through reflection. **Action:** Submit log to Novell Support for analysis and resolution.
700901014	Cannot add non-existent key to keystore.	**Cause:** The certificate you are trying to add to a keystore does not exist. **Action:** Specify a valid key to be added to the keystore.
700901015	Cannot add key to non-existent keystore.	**Cause:** The keystore does not exist. **Action:** Specify a valid keystore or create the keystore.
700901016	Could not add key to keystore because the alias was too long.	**Cause:** Some platforms and keystore formats only support a limited number of characters in the alias name. **Action:** Use a shorter alias.
700901017	Could not add key to keystore because the maximum number of keys has been reached.	**Cause:** Many keystores allow only one key to be contained in it because the keystore has a specific purpose in Access Manager Appliance. **Action:** Remove unused keys from the keystore and try again.
700901020	Cannot remove non-existent key from keystore.	**Cause:** The key no longer exists in Access Manager Appliance. **Action:** View the configuration store and find the keystore object and manually remove the key from the key list.
700901021	Cannot remove key from non-existent keystore.	**Cause:** The keystore does not exist. **Action:** Specify a valid keystore.
100901023	CertHandler.doGetCertFromServer: Could not connect to server IP and port.	**Cause:** The server IP or DNS name and port combination is not reachable. **Action:** Verify that the IP address or DNS name exists and that the port is correct. You can try connecting to it with a web browser or other utility.

Event Code	*Description*	**Remedy**
100901024	CertHandler.doGetCertFromServer: certificate was not obtained from server IP and port.	**Cause:** The server IP or DNS name and port combination had no certificate to be presented. **Action:** Verify that the IP address or DNS name exists and that the port is correct. Verify that the server you are attempting to import the certificate from has a certificate. You can try connecting to it with a web browser or other utility.
100901025	Error in handleException.	**Cause:** The exception reported has no details associated with it. **Action:** Scroll up in the log to see if there is a stack trace immediately above this error, determine what steps you had taken to create this error condition, and submit the log and steps to Novell Support.
100901026	The node keystore does not exist. Cannot add cluster keys to a non-existent keystore.	**Cause:** The grouping of Identity Servers (Identity Server Configuration) or Access Gateways is trying to locate a keystore on one of the Identity Server or Access Gateway devices but the keystore cannot be found. **Action:** Verify that the Identity Servers and Access Gateway devices had no errors during import to the Administration Console. Try to re-import the devices.
100901027	Error in CertHandler.getNIDPDeviceKeystoreName (The name of the device's keystore was not found).	**Cause:** The cluster keystore representation object was not found. **Cause:** The cluster keystore representation did not have a device type specified. **Action:** Delete and recreate the Identity Server Configuration or Access Gateway Group that is causing the problem and then re-add the members.
100901028	Error in CertHandler.isTomcatCert (Unable to determine if the specified certificate is the one being used by Tomcat).	**Cause:** The certificate representation has missing or invalid attributes. **Action:** Delete this certificate and re-import it.
100901030	Error in CertHandler.getNodeKeystoreNames (The cluster object was not found in the configuration store, or the cluster server list was empty).	**Cause:** The cluster object was not found in the configuration store, the type of the cluster could not be determined, or the cluster server list was empty. **Action:** No action needed unless your devices are unable to communicate. If you are having problems with communication, delete and recreate the Identity Server configuration or Access Gateway cluster that is causing the problem.

Event Code	*Description*	**Remedy**
100901031	Error in CertHandler.getClusterDisplayName (The cluster object was not found in the configuration store).	**Action:** Delete and recreate the Identity Server configuration or Access Gateway cluster that is causing the problem and then re-add the members.
100901032	The device does not exist but the certificate is in a keystore assigned to that device.	**Cause:** It's possible the device is in a partially-imported state. **Action:** Delete the keystore, if possible, and re-import the device.
100901033	The device does not exist but the keystore is assigned to that device.	**Cause:** It's possible the device is in a partially-imported state. **Action:** Delete the keystore, if possible, and re-import the device.
100901034	Unable to retrieve the primary member of the group.	**Cause:** The group is corrupt. **Action:** Delete the group, re-create it, and re-add the members.
100901035	Unable to remove the node keystore setting off the Access Gateway group device.	**Cause:** Could not locate the keystore object in the configuration store. **Action:** No action required.
700901036	Unable to set the Update Servers status.	**Cause:** Communication error. **Action:** Manually restart or update the device.
700901037	Unable to remove all keys from keystore.	**Cause:** The keystore doesn't exist. **Cause:** There is a corrupt key in the keystore. **Action:** Manually remove each certificate from the keystore.
700901038	Unable to reinitialize keystore contents for a particular device in a group or configuration.	**Cause:** One of the device keystores does not exist. **Action:** Re-create the keystore or delete and recreate the group or configuration and then re-add the devices to it. **Cause:** There was an error either removing all certificates from a keystore. **Action:** Manually remove all certificates from the keystore and then remove and re-add that device to the group/configuration. **Cause:** There was an error adding the test certificates to a keystore. **Action:** Verify that the test certificates exist (see error 1.009.01.011 for more detail). Manually add the test certificates to the keystore. Or remove the device from the group/configuration and re-add it.

Event Code	*Description*	**Remedy**
700901039	Unable to assess whether the keystore contains a tomcat connector certificate.	**Cause:** The cluster keystore representation does not exist or is corrupt. **Cause:** Unable to locate the devices in the group/configuration. **Action:** Delete and recreate the group/ configuration and re-add the devices to it.
700901040	Error adding a key to keystore during the renew certificate process.	**Cause:** The original certIficate information could not be located. **Action:** Manually create a new certificate and place it into all the keystores which previously held the certificate being renewed.
100901041	Unable to extract the public key from a key during the auto-import public certificate process.	**Cause:** The source keystore does not exist. **Action:** Select a valid keystore. **Cause:** The specified source key does not exist. **Action:** Verify that the key you have specified to export the public certificate from exists.
100901042	Unable to set up the initial keys for the cluster.	**Cause:** When trying to locate the cluster keystores so that their contents can be initialized, one or more of those keystore representations could not be found. **Action:** Delete and recreate the Identity Server configuration or Access Gateway cluster.
100901043	The source keystore does not exist. Cannot push keys from a non-existent keystore.	**Cause:** The source keystore does not exist. **Action:** Usually the source keystore is a cluster keystore representation. Try deleting and recreating the Identity Server configuration or Access Gateway cluster to ensure those cluster keystore representations get created.
	Application	
100902001	Error - Exception thrown in eventOccurred of vcdn.application.sc.alert.AlertEventListener	**Cause:** Cannot post alert to internal subsystem. **Action:** Non-fatal error. No action required.
100902002	Error - Exception thrown in eventOccurred of vcdn.application.sc.alert.AlertEventListener.	**Cause:** Cannot post alert to internal subsystem. **Action:** Submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902003	Error - Exception thrown in logAlert of vcdn.application.sc.alert.AlertLogger.	**Cause:** Problem occurred update the Identity Server Alert count. **Action:** Non-fatal error. May be a symptom of a more serious condition. Submit the `app_sc.0.log` file for resolution.
100902004	Error - Exception thrown in the execute method of vcdn.application.sc.alert.CertUpdateWork.	**Cause:** Could not update or read the list of trusted server certificates. **Action:** Be sure the `/var/opt/novell/novlwww/devman.cacerts` file exists, is a valid Java keystore, and is not corrupted. To check its status, enter the following command: `/opt/novell/java/bin/keytool -v -list -keystore devman.cacerts` Otherwise, be sure the config store is running and functioning properly.
100902005	Error - (The specified device) has not been imported. Failed to start device.	**Cause:** The Identity Server was not properly imported. **Action:** Go to Access Gateway Server List and click *Repair Import.* (The repair import. functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902006	Error importing device (with the specified ID).	**Cause:** The Server was not properly imported. **Action:** Go to Access Gateway Server List and click *Repair Import.* (The repair import. functionality works for any server type.) If this fails, reinstall the server component.
100902007	Error - Import failed. Retrying.	**Cause:** Unable to communicate with the Server being imported. **Action:** Be sure the firewall is allowing port 1443 traffic. Otherwise allow the system to retry for several minutes. If the server does not appear in the Server List, click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902008	Error auto importing. Retry.	**Cause:** Unable to communicate with the Server being imported. **Action:** Be sure the firewall is allowing port 1443 traffic. Otherwise allow the system to retry for several minutes. If the server does not appear in the Server List, click *Repair Import.* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902009	Error - Could not create subcontext: cn=(The specified Context)	**Cause:** Error creating Server object in config store during import. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902010	Error - (The given ESP) does not exist!	**Cause:** There was a error during the Administration Console installation. **Action:** Reinstall the Administration Console.
100902011	Error - Exception reading (the given ESP)	**Cause:** The file required during the import process could not be read. **Action:** Be sure the indicated file can be read by the novlwww user.
100902012	Error - Could not import LDIF.	**Cause:** The error occurred while creating the configuration for the Embedded Service Provider. **Action:** Go to Access Gateway Server List and click *Repair Import.* (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902013	Error - Could not find (the specified DN)	**Cause:** Error connecting to the config store while importing the Embedded Service Provider. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution. You might need to restart the Administration Console.
100902014	Error - ESP Configuration was not found, so auto-import failed.	**Cause:** Could not find the configuration for the imported Embedded Service Provider. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902015	Error - Exception thrown in importDevice of vcdn.application.sc.alert.RegisterCommand.	**Cause:** Error during import of server component. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902016	Error - ImportThread null member vars.	**Cause:** Internal error occurred during import. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902017	Error - Could not connect to eDir for certs.	**Cause:** Either the primary Administration Console is down (if this is a secondary console), or the config store is down. **Action:** Be sure the config store is operating properly and that port 554 is not blocked by a firewall.
100902018	Error during execution.	**Cause:** Error executing an external program during import process. **Action:** Go to Access Gateway Server List and click *Repair Import*. (The repair import functionality works for any server type.) Otherwise, submit the `app_sc.0.log` file for resolution.
100902019	Error - Could not get (the given number of) bytes of payload data.	**Cause:** An error occurred while trying to read data for a command. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902020	Error - VException thrown while executing command in vcdn.application.sc.alert.AlertCommandHandler.	**Cause:** Problem executing a command from a server component. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902021	Error - VCDNException thrown in performConfiguration of vcdn.application.sc.config.AGApplyWork	**Cause:** Problem occurred while sending configuration to Access Gateway server. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902022	Error - VCDNException thrown in responseReceived method of vcdn.application.sc.config.AGApplyWork	**Cause:** Error occurred in processing the response from an Access Gateway server. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902023	Error - VCDNException thrown in performConfiguration method of vcdn.application.sc.config.AGConfigWork	**Cause:** Error occurred while sending configuration to Access Gateway server. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902024	Error - VCDNException thrown in responseReceived method of vcdn.application.sc.config.AGConfigWork	**Cause:** Error occurred in processing the response from an Access Gateway server. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902025	Error - Exception thrown in processAGResponse method of vcdn.application.sc.config.AGConfigWork	**Cause:** Error occurred in processing the response from an Access Gateway server. **Action:** Ensure the server component is operating properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902031	Error - SchedulerException thrown in configureDeviceNow method of vcdn.application.sc.config.ConfigManager	**Cause:** Error occurred while scheduling an immediate apply of the current configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902032	Error - Exception thrown in the execute method of vcdn.application.sc.config.ConfigWork	**Cause:** Error occurred while performing pending actions. **Action:** Submit the `app_sc.0.log` file for resolution.
100902033	Error setting LDAP attribute in performPendingActions of vcdn.application.sc.config.ConfigWork	**Cause:** Pending actions could not be completed because of a problem communicating with the config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902034	Error invoking method in performPendingActions of vcdn.application.sc.config.ConfigWork	**Cause:** Problem occurred while invoking a method during a pending action. **Action:** Submit the `app_sc.0.log` file for resolution.
100902035	Error executing pending action (name) in performPendingActions of vcdn.application.sc.config.ConfigWork	**Cause:** Problem occurred while displaying a pending dialog message. **Action:** This is a non-fatal error. If the problem persists, submit the `app_sc.0.log` file for resolution.
100902036	Error - Exception thrown in getConfigXML of vcdn.application.sc.config.ConfigWork	**Cause:** Error occurred while retrieving XML data from the config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902037	Error - VException thrown in saveInDB method of vcdn.application.sc.config.ConfigWork	**Cause:** Error occurred while saving the applied configuration in the config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902038	Error - VException thrown in configFinished method of vcdn.application.sc.config.DeviceConfigApplyWork	**Cause:** Error occurred while sending the Audit event for a changed configuration. **Action:** Ensure the Audit server and the config store are functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902039	Error - VException thrown in configFinished method of vcdn.application.sc.config.DeviceConfigWork	**Cause:** Error occurred while sending the Audit event for a changed configuration. **Action:** Ensure the Audit server and the config store are functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902040	Error - Exception thrown in processConfigDiff method of vcdn.application.sc.config.DeviceGroupConfigWork	**Cause:** Error occurred while parsing the XML for a group configuration. **Action:** Error occurred while sending the Audit event for a changed configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902041	Error - Exception thrown in memberConfigFinished method of vcdn.application.sc.config.DeviceGroupConfigWork	**Cause:** Error occurred while processing a group member configuration apply response. **Action:** Ensure the server component is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902042	Error - Exception thrown in removePendingFromFailedList method of vcdn.application.sc.config.DeviceGroupConfigWork	**Cause:** Error occurred while re-applying a server configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902043	Error - SchedulerException thrown in scheduleMultiDeviceWorks method of vcdn.application.sc.config.DeviceGroupConfigWork	**Cause:** Error occurred while scheduling a group configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902044	Error - Exception thrown in the execute method of vcdn.application.sc.config.DeviceGroupConfigWork	**Cause:** Error occurred while scheduling a group configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902045	Error - VException thrown in performWork method of vcdn.application.sc.config.MultiDeviceConfigWork	**Cause:** Error occurred while applying configuration to a group member. **Action:** Ensure the server component is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902046	Error - Exception thrown in performWork method of vcdn.application.sc.config.MultiDeviceConfigWork	**Cause:** Error occurred while applying configuration to a group member. **Action:** Ensure the server component is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902047	Error - SchedulerException thrown in getDeviceGroupConfigWork method of vcdn.application.sc.config.MultiDeviceConfigWork	**Cause:** Error occurred while trying to get the scheduled configuration. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902048	Error - VException thrown in configFinished method of vcdn.application.sc.config.MultiDeviceConfigWork	**Cause:** Error occurred while importing status from a group member. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902049	Error - VCDNException thrown in the execute method of vcdn.application.sc.command.AGCommandWork	**Cause:** Error occurred while sending a command to an Access Gateway server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902050	Error - Exception thrown in the sendCommand method of vcdn.application.sc.command.AGCommandWork	**Cause:** Error occurred while sending a command to an Access Gateway server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902051	Error - Exception thrown in the processAGResponse method of vcdn.application.sc.command.AGCommandWork	**Cause:** Error occurred while processing a command response from an Access Gateway server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902055	Error - IOException thrown in the addCommand method of vcdn.application.sc.command.CertCommand	**Cause:** Error generating certificate command. **Action:** Submit the `app_sc.0.log` file for resolution.
100902056	Error - IOException thrown in the generateCmd method of vcdn.application.sc.command.CertCommand	**Cause:** Error generating certificate command. **Action:** Submit the `app_sc.0.log` file for resolution.
100902057	Error - IOException thrown in the setCertChainData method of vcdn.application.sc.command.CertCommand	**Cause:** Error generating chained certificate command. **Action:** Submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902058	Error - VCDNException thrown in the execute method of vcdn.application.sc.command.IDPCommandWork	**Cause:** Error occurred while sending a command to an Identity Server ESP server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902059	Error - VCDNException thrown in the sendCommand method of vcdn.application.sc.command.IDPCommandWork	**Cause:** Error occurred while sending a command to an Identity Server or ESP server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902060	Error - NamingException thrown in the updateNIDPCommandStatus method of vcdn.application.sc.command.IDPCommandWork	**Cause:** Error occurred while processing a command response from an Identity Server or ESP. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
010090261	Error - VException thrown in the updateNIDPCommandStatus method of vcdn.application.sc.command.IDPCommandWork	**Cause:** Error occurred while processing a command response from an Identity Server or ESP. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902062	Error - Exception thrown in the processIDPResponse method of vcdn.application.sc.command.IDPCommandWork	**Cause:** Error occurred while processing a command response from an Identity Server or ESP. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902063	Error - VCDNException thrown in the execute method of vcdn.application.sc.command.JCCCommandWork	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902064	Error - Exception thrown in the sendCommand method of vcdn.application.sc.command.JCCCommandWork	**Cause:** Error occurred while sending a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902065	Error - Exception thrown in the processResponse method of vcdn.application.sc.command.JCCCommandWork	**Cause:** Error occurred while processing a response from a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902066	Error - VCDNException thrown in the execute method of vcdn.application.sc.command.SSLVPNCommandWork	**Cause:** Error occurred while sending an SSLVPN server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902067	Error - Exception thrown in the sendCommand method of vcdn.application.sc.command.SSLVPNCommandWork	**Cause:** Error occurred while sending an SSLVPN server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902068	Error - Exception thrown in the processSSLVPNResponse method of vcdn.application.sc.command.SSLVPNCommandWork	**Cause:** Error occurred while processing a command response from an SSLVPN Server. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
300902069	Exception changing factory LocalAddress.	**Cause:** Error occurred while changing factory XML during configuration import. **Action:** Submit the `app_sc.0.log` file for resolution.
100902070	Error - ConverterException thrown in the getCurrentDeviceXML method of vcdn.application.sc.core.AGDevice	**Cause:** Error occurred during translation of NetWare Access Gateway configuration. **Action:** Submit the `app_sc.0.log` file for resolution.
100902071	Error - NamingException thrown in the importDevice method of vcdn.application.sc.core.AGDevice	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902072	Error - VException thrown in the importDevice method of vcdn.application.sc.core.AGDevice	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902073	Error - Exception thrown in the importDevice method of vcdn.application.sc.core.AGDevice	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902074	Error - NamingException thrown in the vcdn.application.sc.core.AuditManager constructor.	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902075	Error - JDOMException thrown in the processDocument method of vcdn.application.sc.core.AuditManager	**Cause:** Audit XML data could not be parsed. **Action:** Submit the `app_sc.0.log` file for resolution.
100902076	Error - Exception thrown in the processDocument method of vcdn.application.sc.core.AuditManager	**Cause:** Invalid data format. **Action:** Attempt the operation again. Otherwise, submit the `app_sc.0.log` file for resolution.
100902077	Error - Exception thrown in the setDefaultServer method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902078	Error - VException thrown in the writeConfig method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902079	Error - NamingException thrown in the writeConfig method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902080	Error - Exception thrown in the writeConfig method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902081	Error - SException thrown in the getIDPConfigObject method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902082	Error - NamingException thrown in the getIDPConfigObject method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902083	Error - Exception thrown in the getIDPConfigObject method of vcdn.application.sc.core.AuditManager	**Cause:** Config store could not be accessed or an internal error occurred. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902084	Error - NullPointerException thrown in the logEvent method of vcdn.application.sc.core.AuditManager	**Cause:** Error logging Novell Audit event. **Action:** Ensure the Novell Audit server is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902085	Error - Exception thrown in the creatElement method of vcdn.application.sc.core.DeviceConfig	**Cause:** Internal XML error. **Action:** Submit the `app_sc.0.log` file for resolution.
100902086	Error - Exception thrown in the setLastModified method of vcdn.application.sc.core.DeviceConfig	**Cause:** Internal XML error. **Action:** Submit the `app_sc.0.log` file for resolution.
300902087	Warning - Exception thrown in the getLastScheduledWorkID method of vcdn.application.sc.core.DeviceGroupManager	**Cause:** The last executed command status ID could not be read. **Action:** Non-fatal error.
100902088	Error - Could not get version from device. Make sure it is running properly.	**Cause:** Could not get version from device. **Action:** Make sure the server component is running properly, then click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902089	Error - NamingException thrown in the importDevice method of vcdn.application.sc.core.DeviceManager	**Cause:** Error importing device. **Action:** Make sure the server component is running properly, then click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902090	Error - VException thrown in the importDevice method of vcdn.application.sc.core.DeviceManager	**Cause:** Error importing device. **Action:** Make sure the server component is running properly, then click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902091	Error - InvocationTargetException thrown in the importDevice method of vcdn.application.sc.core.DeviceManager	**Cause:** Error importing device. **Action:** Make sure the server component is running properly, then click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902092	Error - Exception thrown in the importDevice method of vcdn.application.sc.core.DeviceManager	**Cause:** Error importing device. **Action:** Make sure the server component is running properly, then click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902093	Error - Could not find esp cfg SCC to remove in cluster container.	**Cause:** Error deleting improperly imported server. **Action:** Non-fatal error.

Event Code	*Description*	**Remedy**
100902094	Error deleting the trusted IDP entry for ESP.	**Cause:** Error accessing config store. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902095	Error - NamingException thrown in the setHealthCheck method of vcdn.application.sc.core.DeviceManager	**Cause:** Error saving health status in config store. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902096	Error - Could not find the DN specified.	**Cause:** Error saving health status in config store. **Action:** Ensure the server component imported correctly and the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902097	Error - Exception thrown in the deleteDevice method of vcdn.application.sc.core.DeviceManager	**Cause:** Error occurred while deleting the server objects. **Action:** Ensure the config store is functioning properly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902098	Error - Exception thrown in the setHealthCheck method of vcdn.application.sc.core.DeviceManager	**Cause:** Error updating the version following an upgrade of a server component. **Action:** Allow the operation to try again. Otherwise, submit the `app_sc.0.log` file for resolution.
300902099	Warning - Exception thrown in the getLastScheduledWorkID method of vcdn.application.sc.core.DeviceManager	**Cause:** The last executed command status ID could not be read. **Action:** Non-fatal error.
300902100	Device is not imported.	**Cause:** Server component is sending health to Administration console that does not recognize the server. **Action:** Click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
300902101	Identity configuration not found for device.	**Cause:** Identity server configuration not found in config store. **Action:** Non-fatal error.

Event Code	*Description*	**Remedy**
100902102	Error - Exception thrown in the createCertEntry method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to create objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`
100902103	Error - Exception thrown in the deleteCertEntry method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to delete objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`
100902104	Error - Exception thrown in the modifyCertEntryXml method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to modify objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`
100902105	Error - Exception thrown in the createKeyStoreEntry method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to create objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`
100902106	Error - Exception thrown in the deleteKeyStoreEntry method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to delete objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`

Event Code	*Description*	**Remedy**
100902107	Error - Exception thrown in the modifyKeyStoreEntryXml method of vcdn.application.sc.core.KeyManager	**Cause:** The config store is not reachable or the user doesn't have rights to modify the config store **Action:** Verify the config store is up and that the user has rights to modify objects in the following container: `ou=KeyContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_root,ou=accessManagerContainer,o=novell`
100902108	Error - Exception thrown in the createElement method of vcdn.application.sc.core.PolicyConfig	**Cause:** Error creating an element in the specified XML document. **Action:** Submit the `app_sc.0.log` file for resolution.
100902109	Error - Exception thrown in the setLastModified method of vcdn.application.sc.core.PolicyConfig	**Cause:** Error setting an attribute value on modified elements. **Action:** Submit the `app_sc.0.log` file for resolution.
100902110	Error - NamingException thrown in the importDevice method of vcdn.application.sc.core.SSLVPNDevice	**Cause:** Error importing device. **Action:** Click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902111	Error - VException thrown in the importDevice method of vcdn.application.sc.core.SSLVPNDevice	**Cause:** Error importing device. **Action:** Click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902112	Error - Exception thrown in the importDevice method of vcdn.application.sc.core.SSLVPNDevice	**Cause:** Error importing device. **Action:** Click *Repair Import* to resolve the issue. Otherwise, submit the `app_sc.0.log` file for resolution.
100902113	Error - Exception thrown in the sendData method of vcdn.application.sc.core.work.DeleteDeviceWork	**Cause:** Error communicating with component. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902114	Error - Exception thrown in the execute method of vcdn.application.sc.core.work.ReimportDeviceWork	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902115	Error - Exception thrown in the getHealth method of vcdn.application.sc.health.HealthCheck	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100902116	Error - Inner Exception thrown in the execute method of vcdn.application.sc.health.HealthCheck	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902117	Error - Outer Exception thrown in the execute method of vcdn.application.sc.health.HealthCheck	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902118	Error - VException thrown in the eventOccurred method of vcdn.application.sc.health.HealthEventListener	**Cause:** Error occurred while receiving/logging a health event. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902119	Error getting Health Module or Service	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100902120	Error - Exception thrown in the execute method of vcdn.application.sc.health.HealthUpdateWork	**Cause:** Error occurred while executing a server command. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
	Platform	
100903001	Error - Unable to find a trusted client certificate.	**Cause:** There was a problem during the import of the device. **Action:** Consult the documentation to re-import the device into the Administration Console.
100903002	Error building delayed response.	**Cause:** Error occurred while processing a request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903003	Error setting return code in HttpServletResponse.	**Cause:** Error occurred while processing a request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100903004	Error - DelayedResponseListener thread failed to start.	**Cause:** Error occurred while processing a delayed response. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903005	Error in the ResponseHandler thread of the DelayedResponseListener.	**Cause:** Error occurred while processing a response. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903006	Error creating XML Element in ResponseBuilder.	**Cause:** Error occurred while editing XML. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903007	Error waiting on mutex in RequestDispatcher.	**Cause:** Error occurred while getting responses. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903008	Error notifying mutex in RequestDispatcher.	**Cause:** Error occurred while receiving a response. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903009	Error receiving in SendInternal of VConnection.	**Cause:** Error occurred while receiving an internal response. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903010	Error getting response code in VConnection.	**Cause:** Error occurred while getting the code. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903011	Error in stopScheduledResponses of VConnection.	**Cause:** Error occurred while attempting to stop scheduled responses. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903012	Error in ConsumeData of VConnection.	**Cause:** Error occurred while reading data. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100903013	Error in sendData of VConnection.	**Cause:** Error occurred while sending data. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903014	Error in getHeaders of VConnection.	**Cause:** Error occurred while getting headers. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100903015	Error in receive of VConnection.	**Cause:** Error occurred while receiving a response. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
	Web UI	
100904001	Error reading manager data in UIManager.	**Cause:** Error occurred while reading data. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904002	Error during auto authentication in WebApplicaitonFilter.	**Cause:** Error occurred while authenticating. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904003	Error - Exception thrown in doFilter of WebApplicationFilter.	**Cause:** Error getting panel data. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904004	Error - Exception thrown in logout of WebApplicationFilter.	**Cause:** Error occurred while logging out. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904005	Error - VException thrown in getUserInfo of WebManager.	**Cause:** Error occurred while getting user information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904006	Error - Exception thrown in getDeviceInfo of WebManager.	**Cause:** Error occurred while getting device information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904007	Error - Exception thrown in getPolicyInfo of WebManager.	**Cause:** Error occurred while getting policy information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904008	Error - Exception thrown in getTypeSpecificationInfo of WebManager.	**Cause:** Error occurred while getting policy type specification information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904009	Error - Exception thrown in getDeviceConfig of WebManager.	**Cause:** Error occurred while getting device configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904010	Error - Exception thrown in getPolicyConfig of WebManager.	**Cause:** Error occurred while getting device configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904011	Error - Exception thrown in getTypeSpecificationConfig of WebManager.	**Cause:** Error occurred while getting policy type specification configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904012	Error - Exception thrown in parameterMapToString of WebManager.	**Cause:** Error occurred while getting parameter information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904013	Error while logging out user {0}.	**Cause:** Error occurred while logging out NDS user object. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904014	Error - Exception thrown in getSelectionCriteria of WebPanel.	**Cause:** Error occurred while getting selection criteria. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904015	Error - Exception thrown in getPanelVersion of WebPanel.	**Cause:** Error occurred while getting panel version. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904016	Error - Group Config failed.	**Cause:** Error occurred while applying group configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904017	Error - Schedule Group Config failed.	**Cause:** Error occurred while scheduling group configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904018	Error - Update XML and Device Config failed.	**Cause:** Error occurred while updating configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904019	Error - Unlock Config failed.	**Cause:** Error occurred while unlocking the configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904020	Error - Exception thrown in do_cancelPendingConfig of ConfigWorkDispatcher.	**Cause:** Error occurred while canceling a pending configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904021	Error - Exception thrown in do_cancelPendingConfig of ConfigWorkDispatcher.	**Cause:** Error occurred while canceling a pending configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904022	Error - Exception thrown in do_reapplyPendingConfig of ConfigWorkDispatcher.	**Cause:** Error occurred while reapplying a pending configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904023	Error - Exception thrown in do_deviceConfig of ConfigWorkDispatcher.	**Cause:** Error occurred while applying configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904024	Error - Exception thrown in do_scheduleDeviceConfig of ConfigWorkDispatcher.	**Cause:** Error occurred while scheduling configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200904025	Error - XML VALIDATION FAILED. PLEASE CHECK APP_SC LOG.	**Cause:** XML created by GUI does not match the XML schema and fails validation. **Action:** Cancel the changes that were made and try again. In any case, submit the `app_sc.0.log` file for resolution.
100904026	Error applying settings in ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while applying configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904027	Error - Exception thrown in do_save of ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while saving configuration. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904028	Error - Exception thrown in do_cancel of ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while canceling configuration changes. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904029	Error - Exception thrown in do_refreshConfig of ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while refreshing configuration manager panel. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904030	Error - Exception thrown in setLastModParams of ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while setting an XML attribute. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904031	Error - IOException thrown in getXPathMap of ConfigXmlUpdateDispatcher.	**Cause:** Error occurred while xpath mapping on the current panel. **Action:** Ensure the server component is functioning correctly. Cancel changes on the current panel, return, and try again. Otherwise, submit the `app_sc.0.log` file for resolution.
100904032	Error decoding: {0}.	**Cause:** Error occurred while xpath mapping on the current panel. **Action:** Ensure the server component is functioning correctly. Cancel changes on the current panel, return, and try again. Otherwise, submit the `app_sc.0.log` file for resolution.
100904033	Error - Exception thrown in processRequest of ExceptionDispatcher.	**Cause:** Error occurred while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904034	Error - Exception thrown in the service method of ServletDispatcher.	**Cause:** Error occurred while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904035	Error - Exception thrown in ServletDispatcher.	**Cause:** Error occurred while inserting dispatchers. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904036	Error - Exception thrown in processRequest of DeviceCommandHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904037	Error - VException thrown in setNIDPCommandState of DeviceCommandHandler.	**Cause:** Error occurred while accessing data store. **Action:** Ensure the data store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904038	Error - NamingException thrown in setNIDPCommandState of DeviceCommandHandler.	**Cause:** Error occurred while accessing data store. **Action:** Ensure the data store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904039	Error - Could not find signing keystore for {0}.	**Cause:** An error occurred during the import of the device. **Action:** Consult the documentation and re-import the device into the Administration Console.
100904040	Error - Could not find encryption keystore for {0}.	**Cause:** An error occurred during the import of the device. **Action:** Consult the documentation and re-import the device into the Administration Console.
100904041	Error - Could not find connector keystore for {0}.	**Cause:** An error occurred during the import of the device. **Action:** Consult the documentation and re-import the device into the Administration Console.
100904042	Error - Could not find trust keystore for {0}.	**Cause:** An error occurred during the import of the device. **Action:** Consult the documentation and re-import the device into the Administration Console.
100904043	Error - Could not find OCSP trust keystore for {0}.	**Cause:** An error occurred during the import of the device. **Action:** Consult the documentation and re-import the device into the Administration Console.
100904044	Error - No keys were assigned to keystore: {0}.	**Cause:** The keystore does not have any certificates in it. This may or may not be a bad condition. For instance, the OCSP trust store can be empty and that should not cause a problem. The signing, encryption, connector, provider, and consumer keystores should have one certificate in them. If it is empty, either the device import failed or the user manually removed the certificate from the keystore. **Action:** Check the keystore using the UI. If the keystore shows that it has a certificate, then the device import probably failed. Consult the documentation and re-import the device and also try deleting and re-creating the NIDP configuration. Also, try replacing the certificate in the keystore through the UI.
100904045	Error - Exception thrown in processRequest of UpgradeDeviceGroupHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100904046	Error - Exception thrown in processRequest of UpgradeDeviceHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100904047	Error - Exception thrown in getUpgradeInfo of UpgradeDeviceHandler.	**Cause:** Error occurred while getting update information. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
	Application Handlers	
100905001	Error during repair import.	**Cause:** Error occurred while attempting to repair import. **Action:** Delete the server from the list and reinstall. Otherwise, submit the `app_sc.0.log` file for resolution.
100905002	Error - Failed to remove server.	**Cause:** Error occurred while attempting to remove server. **Action:** Submit the `app_sc.0.log` file for resolution.
100905003	Error setting device groups.	**Cause:** Error occurred while attempting to mark a server as a member of a group. **Action:** Delete the server from the group and retry or delete the group and recreate. Otherwise, submit the `app_sc.0.log` file for resolution.
100905004	Error setting device admin.	**Cause:** Error occurred while attempting to give an Administrator access to a server. **Action:** Submit the `app_sc.0.log` file for resolution.
100905005	Error - Exception thrown while importing appliance.	**Cause:** Error occurred while importing a server. **Action:** Delete the server from the list and reinstall. Otherwise, submit the `app_sc.0.log` file for resolution.
100905006	Error getting health info.	**Cause:** Error occurred while getting health information for a server. **Action:** Ensure the server component and the config store are functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905007	Error canceling appliance creation.	**Cause:** Internal error. **Action:** Submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905008	Error creating new CDN.	**Cause:** Internal error. **Action:** Submit the `app_sc.0.log` file for resolution.
100905009	Error removing CDN.	**Cause:** Internal error. **Action:** Submit the `app_sc.0.log` file for resolution.
100905010	Error creating new Admin.	**Cause:** Internal error. **Action:** Submit the `app_sc.0.log` file for resolution.
100905011	Error while changing the cached device port.	**Cause:** Internal error while processing request. **Action:** Ensure the Management IP Address is correct or edit as needed. Otherwise, submit the `app_sc.0.log` file for resolution.
100905012	Error while changing the cached device password.	**Cause:** Internal error while processing request. **Action:** Ensure the Management Password is correct or edit as needed. Otherwise, submit the `app_sc.0.log` file for resolution.
100905013	Error - Exception thrown while processing request in EditApplianceHandler	**Cause:** Internal error while processing request. **Action:** Ensure all values on the Server Details Edit page are correct and edit as needed. Otherwise, submit the `app_sc.0.log` file for resolution.
100905014	Error - Exception thrown while modifying device handler in EditDeviceHandler.	**Cause:** Error occurred while processing a request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905015	Error - Exception thrown while changing password in EditDeviceHandler.	**Cause:** Error occurred while processing a request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905016	Error - Exception thrown while editing CDN in EditPublisherHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905017	Error - Exception thrown while updating CDN in EditPublisherHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
200905018	Error - Failed to update the device groups for this user.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905019	Error - Failed to update the devices for this user.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905020	Error - Failed to update the cdns for this user.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905021	Error - Failed to update user data.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905022	Error processing client certs in GenericPipeHandler.	**Cause:** Internal error while processing request. **Action:** Ensure the server component is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905023	Error accessing XML data item in generic pipe: {0}	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905024	Error parsing XML data item in generic pipe: {0}	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
200905025	Error processing XML data item in generic pipe: {0}	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905026	Error - Exception thrown in processRequest of GenericPipeHandler: {0}	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905027	Error occurred while creating group {0} : {1}.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete the group and recreate it. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905028	Error getting device manager in doGroupRemove of GroupCreateHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete the group again. Otherwise, submit the `app_sc.0.log` file for resolution.
100905029	Error occurred while removing group {0} : {1}.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete the group again. Otherwise, submit the `app_sc.0.log` file for resolution.
100905030	Error occurred while getting device manager in doGroupAlertStatus of GroupCreateHandler.	**Cause:** Unable to get alert status for the group. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905031	Error occurred while setting alert status for group {0} : {1}.	**Cause:** Unable to set alert status for the group. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905032	Error occurred while updating group {0} : {1}.	**Cause:** Unable to make updates to the group. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905033	Error occurred while removing devices from group {0} : {1}.	**Cause:** Unable to remove servers from the group. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905034	Error - Naming Exception thrown in removeDeviceFromCluster of GroupCreateHandler.	**Cause:** Unable to remove servers from the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905035	Error - Exception thrown in removeDeviceFromCluster of GroupCreateHandler.	**Cause:** Error occurred while removing servers from the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905036	Error - Exception thrown in removeDeviceFromCluster of GroupCreateHandler.	**Cause:** Error occurred while removing servers from the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905037	Error occurred while adding devices to group {0} : {1}.	**Cause:** Error occurred while adding servers to the group. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905038	Error - Naming Exception thrown in addDeviceToCluster of GroupCreateHandler.	**Cause:** Error occurred while adding servers to the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905039	Error - Exception thrown in addDeviceToCluster of GroupCreateHandler.	**Cause:** Error occurred while adding servers to the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905040	Error - Exception thrown in addDeviceToCluster of GroupCreateHandler.	**Cause:** Error occurred while adding servers to the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905041	Error occurred while adding devices to group {0} : {1}.	**Cause:** Error occurred while adding servers to the cluster. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905042	Error - VCDNException thrown in processRequest of SyncHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905043	Error - Exception thrown in processRequest of SyncHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905044	Error - Exception thrown in modifySystemSync of SyncHandler.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905045	Error - WSException thrown in isAssignedUser of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905046	Error - WSException thrown in isAssignedDevice of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905047	Error - WSException thrown in getApplianceByUrl of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905048	Error - WSException thrown in generateMembershipList of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905049	Error - WSException thrown in getAppGroupByName of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905050	Error - WSException thrown in getDescForThisGroup of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905051	Error - Exception thrown in getDescForThisGroup of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905052	Error - WSException thrown in getLastModifiedDate of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905053	Error - Get appliance groups failed in GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete group and recreate it. Otherwise, submit the `app_sc.0.log` file for resolution.
100905054	Error - WSException thrown in hasAMembershipIn of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete group and recreate it. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905055	Error - Get appliances failed in GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly or delete group and recreate it. Otherwise, submit the `app_sc.0.log` file for resolution.
100905056	Error - Get admins failed in GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905057	Error - WSException thrown in getPerDeviceProperties of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905058	Error - WSException thrown in getPerUserProperties of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905059	Error - WSException thrown in getDeviceGroupProperties of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905060	Error - NamingException thrown in setDeviceClusterConfig of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905061	Error - Exception thrown in setDeviceClusterConfig of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905062	Error - VException thrown in clusterServers of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905063	Error - Exception thrown in clusterServers of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905064	Error - VException thrown in getAdminList of GroupCreateBean.	**Cause:** Internal error. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905065	Error - Exception thrown in callRestartESP of SPConfigHandler.	**Cause:** Error occurred while restarting Embedded Service Provider. **Action:** Ensure the server component and ESP are functioning correctly or restart ESP again. Otherwise, submit the `app_sc.0.log` file for resolution.
100905066	Error restarting {0}.	**Cause:** Error occurred while restarting Embedded Service Provider. **Action:** Ensure the server component and ESP are functioning correctly or restart ESP again. Otherwise, submit the `app_sc.0.log` file for resolution.
100905067	Error - Could not lookup {0}.	**Cause:** Error occurred while looking up DN in config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905068	{0}.	**Cause:** Error occurred while accessing config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905069	Error - Exception thrown in createTrustedIDP of SPConfigHandler.	**Cause:** Error occurred while accessing config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905070	Error getting the esp trusted IDP.	**Cause:** Error occurred while accessing config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905071	espTrustAccessDN not set.	**Cause:** Error occurred while accessing config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905072	Error deleting trusted IDP config.	**Cause:** Error occurred while accessing config store. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905073	Error - VCDNException thrown in processRequest of ScheduleHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905074	Error - Exception thrown in processRequest of ScheduleHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905075	Error - Exception thrown in setEnable of ScheduleHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905076	Error - Exception thrown while removing scheduled work in ScheduleHandler.	**Cause:** Error occurred while processing request. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905077	Error - Exception thrown while releasing config lock in ScheduleHandler.	**Cause:** Error occurred while unlocking configuration. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905078	Error - Exception thrown in modify method of ScheduleHandler.	**Cause:** Error occurred while modifying scheduled work. **Action:** Ensure the config store is functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905079	Error - Exception thrown in executeNow method of ScheduleHandler.	**Cause:** Error occurred while scheduling work. **Action:** Ensure the config store and server component are functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905080	Error - ParamNotFoundException thrown in createSchedule method of ScheduleHandler.	**Cause:** Error occurred while scheduling work. **Action:** Ensure the config store and server component are functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.

Event Code	*Description*	**Remedy**
100905081	Error - Can not forward the request to return page. Nothing can be done.	**Cause:** Internal error. **Action:** Ensure server component is functioning correctly and attempt to navigate to desired panels. Otherwise, submit the `app_sc.0.log` file for resolution.
100905082	Error - Exception thrown in create method of ScheduleHandler.	**Cause:** Error occurred while scheduling work. **Action:** Ensure the config store and server component are functioning correctly. Otherwise, submit the `app_sc.0.log` file for resolution.
100905083	Config store Error	**Cause:** The connection to the config store is experiencing problems. **Action:** To diagnose time synchronization issues with multiple Administration Consoles, run the following command on the primary server command-line: `/opt/novell/eDirectory/bin/ndsrepair -T` This will check the overall time synchronization status. If the time is not in sync, then you might want to consider configuring NTP on each server.
	Policy	
100906000	Cannot set update status for NULL policy extension.	**Cause:** The composite ID of the extension specified cannot be resolved to an extension ID. **Action:** On the device that is not receiving an Update status, make a configuration change to force the Update link to become active.
100906001	Cannot retrieve policy collection info object for the extension.	**Cause:** The extension ID specified cannot be found in the configuration store. **Action:** If you see a problem with your extensions, note this error in the log and call support.
100906002	Cannot retrieve device info object for a device	**Cause:** When trying to set the Update status on devices which use an extension, the device info was unable to be located in the configuration store. **Action:** On the device that is not receiving an Update status, make a configuration change to force the Update link to become active.

Event Code	*Description*	**Remedy**
500906000	Attempting to update policy status on devices because the policy extension changed.	**Cause:** Informational message. **Action:** No action necessary.
500906001	Setting update policy status for device.	**Cause:** Informational message. **Action:** No action necessary.

3 Identity Server (001)

Component 001

- Subgroup 01: End user events
- Subgroup 02: Web Service Framework (WSF)
- Subgroup 03: Web Service Consumer (WSC)
- Subgroup 04: User Authentication

Event Code	Message	Remedy
100100001		Type: SEVERE:NIDP:INITIALIZE:001
100100002		Type: SEVERE:NIDP:INITIALIZE:002
100101001	No binding available or set for profile.	Type: SEVERE:NIDP:USERMSG:001 **Cause:** An action using Liberty or SAML protocols could not be completed because the server and trusted provider are not compatibly configured to interact to complete the action. **Action:** Set the desired protocol profiles in the administration tool to match those supported at the trusted provider.
100101043	IDP is unable to load ESP metadata.	Type: SEVERE:NIDP:USERMSG:043 **Cause:** The IDP cannot connect to the metadata URL for the ESP. The IDP may not be able to resolve the domain name for the ESP or if HTTPS is being used, the IDP may not trust the SSL certificate for the ESP. The ESP might also not be running. **Action:** Make sure that certificates for ESP are imported and trusted into IDP configuration. Check the metadata URL for the ESP and make sure the metadata can be retrieved from a browser: http://<DNS_name>/nesp/idff/metadata If you are seeing this error after changing the IP address of the Access Gateway, restart Tomcat on the Identity Server. **Cause:** The IDP needs to have access to the internet to resolve and reach the CRL and OCSP URLs for ESP certificate validation. **Action:** Make sure the internet access is enabled, else the IDP will not trust the ESP certificate even if it has the signing and intermediary certificates.

Event Code	Message	Remedy
100101044	ESP is unable to load IDP metadata	Type: SEVERE:NIDP:USERMSG:044 **Cause:** The ESP cannot connect to the metadata URL for the IDP. The ESP may not be able to resolve the domain name for the IDP or if HTTPS is being used, the ESP may not trust the SSL certificate for the IDP. The IDP may also not be running **Action:** Make sure the IDP is running and that all certificates are imported and trusted. Check the metadata URL for the IDP and make sure the metadata can be retrieved from a browser: http://<DNS_name>/nidp/idff/metadata A common cause is the base URL on the IDP is set incorrectly. For additional help, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.
100101045	An error happened while the request was being sent to the correct cluster member for processing.	Type: SEVERE:NIDP:USERMSG:045 **Cause:** The target cluster member may be unavailable. **Action:** Ensure that all cluster devices are operating correctly.
100102001	Incomplete web service configuration.	Type: SEVERE:NIDP:WSF:001 **Cause:** The web service instance type (attribute nidsWsfServiceInstanceType on the nidsWsfService object) is not available in the service definition. **Action:** Delete the associated web service definition and recreate it.
100102002	Invalid web service configuration.	Type: SEVERE:NIDP:WSF:002 **Cause:** The web service configuration XML (attribute nidsConfigXML on the nidsWsfService object) has invalid XML. **Action:** Delete the associated web service definition and recreate it.
100102003	Unable to instantiate the web service provider authority class. This class will be com.novell.nidp.liberty.wsf.config.authority.ldap.WSFConfigAuthorityLdap.	Type: SEVERE:NIDP:WSF:003 **Cause:** Some Java error (probably a classpath issue) is causing the main authority class to not instantiate. **Action:** Review how the Access Manager product was installed and attempt to determine if Java class files are being accessed from an unexpected source.
100102004	Unable to load web services.	Type: SEVERE:NIDP:WSF:004 **Cause:** This error catches all failures encountered while trying to load all web services. The reason will be different depending on where the error happened. **Action:** Try to delete and recreate the web services.

Event Code	Message	Remedy
100102005	Unable to access Novell Secret Store.	Type: SEVERE:NIDP:WSF:005 **Cause:** The LDAP connection between the IDP and the User Store must be secure LDAP if Novell Secret Store is to be used as the back end storage for Credential Profile. **Action:** Go to the associated user store and change the connection type to secure LDAP.
100102006	Unable to create user profile object.	Type: SEVERE:NIDP:WSF:006 **Cause:** A Liberty User Profile Object did not exist for the current user, so an attempt was made to create one. That attempt failed! **Action:** Determine if the named container exists and that the administrator user has rights to create objects there.
100102007	Unable to instantiate password callback class.	Type: SEVERE:NIDP:WSF:007 **Cause:** Could not find the password callback class in the classpath. **Action:** Make sure the password callback class to check UsernameToken that decrypts an encrypted message in WSS is in the classpath.
100102008	Unable to convert XML into Document.	Type: SEVERE:NIDP:WSF:008 **Cause:** This error occurred when converting XML to Document in WSS (Receiver side). It may happen due to incorrect WSC requests. **Action:** Check the WSC (Sender side) request and resend it.
100102009	Unable to process WSSecurity (WSS) message.	Type:SEVERE:NIDP:WSF:009 **Cause:** This error occurred when processing WSS headers (Receiver side). It may happen due to incorrect WSS headers in WSC requests. **Action:** Check the WSS headers in WSC (Sender side) request and resent it.
100102010	No WSS header found	Type: SEVERE:NIDP:WSF:010 **Cause:** This error occurred when processing WSS headers (Receiver side). It may happen due to no WSS headers in WSC requests. **Action:** Check the WSS headers in WSC (Sender side) request and resend it.

Event Code	Message	Remedy
100102011	No processed WSS header found	Type: SEVERE:NIDP:WSF:011 **Cause:** This error occurred after processing WSS headers (Receiver side). It may happen due to incorrect or no WSS headers in WSC requests. **Action:** Check the WSS headers in WSC (Sender side) request and resend it.
100102012	WSS untrusted certificate	Type: SEVERE:NIDP:WSF:012 **Cause:** This error occurred when validating signature on WSS headers (Receiver side). The certificate used for the signature is not trusted. **Action:** Check the certificate used to sign the message. The certificate is trusted if either it itself or the certificate of the issuer is installed in the trust store.
100102013		Type: SEVERE:NIDP:WSF:013
100102014		Type: SEVERE:NIDP:WSF:014
100102015		Type: SEVERE:NIDP:WSF:015
100102016		Type: SEVERE:NIDP:WSF:016
100102017		Type: SEVERE:NIDP:WSF:017
100102018		Type: SEVERE:NIDP:WSF:018
100102019		Type: SEVERE:NIDP:WSF:019
100102020		Type: SEVERE:NIDP:WSF:020
100102021		Type: SEVERE:NIDP:WSF:021
100102022		Type: SEVERE:NIDP:WSF:022
100102023		Type: SEVERE:NIDP:WSF:023
100102024		Type: SEVERE:NIDP:WSF:024
100102025	The Service Discovery Service has not been initialized.	Type: SEVERE:NIDP:WSF:025 **Cause:** The Discovery Service has not been enabled or created. **Action:** Create and enable a Liberty Discovery Service using the Access Manager Appliance administration utility.
100102026		Type: SEVERE:NIDP:WSF:026
100102027		Type: SEVERE:NIDP:WSF:027
100102028		Type: SEVERE:NIDP:WSF:028
100102029		Type: SEVERE:NIDP:WSF:029
100102030		Type: SEVERE:NIDP:WSF:030
100102031		Type: SEVERE:NIDP:WSF:031
100102032		Type: SEVERE:NIDP:WSF:032

Event Code	Message	Remedy
100102033		Type: SEVERE:NIDP:WSF:033
100103001	Web Service Consumer XML Configuration Parse Exception.	Type: SEVERE:NIDP:WSC:001 **Cause:** The nidsConfigXML attribute on the nidsWsf object has invalid XML. **Action:** Delete the nidsConfigXML attribute and reconfigure WSC.
100103002		Type: SEVERE:NIDP:WSC:002
100103003		Type: SEVERE:NIDP:WSC:003
100103004		Type: SEVERE:NIDP:WSC:004
100103005		Type: SEVERE:NIDP:WSC:005
100103006		Type: SEVERE:NIDP:WSC:006
100103007		Type: SEVERE:NIDP:WSC:007
100103008		Type: SEVERE:NIDP:WSC:008
100103009		Type: SEVERE:NIDP:WSC:009
100103010		Type: SEVERE:NIDP:WSC:010
100103011		Type: SEVERE:NIDP:WSC:011
100103012		Type: SEVERE:NIDP:WSC:012
100103013		Type: SEVERE:NIDP:WSC:013
100103014		Type: SEVERE:NIDP:WSC:014
100103015		Type: SEVERE:NIDP:WSC:015
100103016		Type: SEVERE:NIDP:WSC:016
100103017		Type: SEVERE:NIDP:WSC:017
100104105	Could not initialize Kerberos/ GSS	Type: SEVERE:NIDP:USERAUTH:105 **Cause:** Failure at GSS-API **Action:** Check the following according the details of the error message: Keytab file - validity, presently only understands DES; Service Principal Name (SPN)
100104107	Kerberos Configuration is not properly initialized	Type: SEVERE:NIDP:USERAUTH:107 **Cause:** Kerberos Configuration is not properly initialized in the admin user interface **Action:** Make sure all the required configuration setting are properly specified in admin UI

Event Code	Message	Remedy
100104108	SPNEGO/Kerberos method not implemented	Type: SEVERE:NIDP:USERAUTH:108 **Cause:** SPNEGO/Kerberos NegTokenInit not implemented. **Action:** NegTokenInit token not implemented as the server side does not need to generate it new. No Action needed.
100105001	An error happened while forwarding a request to a cluster member.	Type: SEVERE:NIDP:APP:001 **Cause:** An internal error occurred. **Action:** Evaluate the error and take appropriate action.
100105002	Failed to initialize JNDI connections.	Type: SEVERE:NIDP:APP:002 **Cause:** NIDP attempts to create JNDI connections to each user store replica during NIDP startup. In this case, NIDP was unable to establish connections with the indicated host. **Action:** Ensure that the host is available and that the configuration information for the replica is correct.
100105003	Error obtaining SOAP response.	Type: SEVERE:NIDP:APP:003 **Cause:** A SOAP request was made and a response was expected, but an error happened retrieving the response. **Action:** Evaluate the indicated reason and take appropriate action.
100105004	Error in SOAP response format.	Type: SEVERE:NIDP:APP:004 **Cause:** A SOAP request was made and a response was expected, the response was obtained but the format of it was unexpected. **Action:** Evaluate the indicated reason and take appropriate action.
100105005	Error executing Login Policy Check LDAP Extension for user on user store	Type: SEVERE:NIDP:APP:005 **Cause:** User authenticated using X509. An additional check of the directory's user login policy needs to be made using an LDAP method extension. This check was successfully done using an LDAP extension. However, after the LDAP extension is called, it must be called a second time to update the user account with a success or failure. This second call to the extension failed, so directory user account status may be erroneous. **Action:** Check with eDirectory documentation for LDAP extension with OID 2.16.840.1.113719.1.39.42.100.25
100105006		Type: SEVERE:NIDP:APP:006
100105007		Type: SEVERE:NIDP:APP:007

Event Code	Message	Remedy
100105008	The audit logging system is not operational.	Type: SEVERE:NIDP:APP:008 **Cause:** The audit logging system can, in rare circumstances, become non-operational. **Action:** Examine the error description supplied and take appropriate action.
100106001		Type: SEVERE:NIDP:IDFF:001
200102001	Invalid access code found for web service specific user interaction query policy.	Type: ERROR:NIDP:WSF:001 **Cause:** The web service definition has a service level user interaction policy that is not ALWAYS or NEVER. Disallowed values are NO and ONCE. **Action:** Using Access Manager Appliance management tools, edit the policy associated with the web service.
200102002	Invalid access code found for web service specific user interaction modify policy.	Type: ERROR:NIDP:WSF:002 **Cause:** The web service definition has a service level user interaction policy that is not ALWAYS or NEVER. Disallowed values are NO and ONCE. **Action:** Using Access Manager Appliance management tools, edit the policy associated with the web service.
200102003	Unrecognized web service.	Type: ERROR:NIDP:WSF:003 **Cause:** The web service definition has a service type specifier (attribute nidsWsfServiceInstanceType on object nidsWsfService) that is not recognized. **Action:** Using Access Manager Appliance management tools, delete the associated web service and recreate it.
200102004	Error writing user interaction access policy to the data store.	Type: ERROR:NIDP:WSF:004 **Cause:** The IDP received user interaction access policy from the user, but was unable to persist it to the data store. **Action:** Check the Access Manager Appliance Configuration datastore to see if it is available.
200102005	Cannot read or write web service data because zero data locations are specified.	Type: ERROR:NIDP:WSF:005 **Cause:** When an IDSIS web service is reading or writing data it follows the configured data locations to know where to perform its operations. If the administrator has not set up any data locations then the operation must fail. **Action:** Add at least one data location the web service.

Event Code	Message	Remedy
200102006	Cannot read or write web service data because the first data location is unknown.	Type: ERROR:NIDP:WSF:006 **Cause:** When an IDSIS web service is reading or writing data it follows the configured data locations to know where to perform its operations. **Action:** Delete all data locations from the associated web service and add them back into the list.
200102007	Unexpected error writing data to web service.	Type: ERROR:NIDP:WSF:007 **Cause:** Writing to web services is prone to various unexpected errors. **Action:** Evaluate the reason for the error and take appropriate action.
200102008	Unable to locate the cached NIDPSession object given session id.	Type: ERROR:NIDP:WSF:008 **Cause:** The user session has expired. **Action:** The user must login again.
200102009	Cached NIDPPrincipal object has zero NIDPSubject objects.	Type: ERROR:NIDP:WSF:009 **Cause:** The user session has expired. **Action:** The user must login again.
200102010	No web service authority available.	Type: ERROR:NIDP:WSF:010 **Cause:** A web service of the provided type did not initialize correctly. **Action:** Delete the web service and recreate it.
200102011	No web service available.	Type: ERROR:NIDP:WSF:011 **Cause:** A web service of the provided type does not exist, or is not enabled. **Action:** Create or enable a web service of this type.
200102012	Unable to understand the web service request's XML.	Type: ERROR:NIDP:WSF:012 **Cause:** A web service sent a request to the IDP that cannot be parsed or it is missing data such that the request cannot be understood. **Action:** Notify your system administrator that invalid web service requests are being made to the system.
200102013	Error processing web service query request.	Type: ERROR:NIDP:WSF:013 **Cause:** Processing web service requests may result in a number of unexpected errors. **Action:** Evaluate the reason given in the error message, and take appropriate action.

Event Code	Message	Remedy
200102014	Error processing web service modify request.	Type: ERROR:NIDP:WSF:014 **Cause:** Processing web service requests may result in a number of unexpected errors. **Action:** Evaluate the reason given in the error message, and take appropriate action.
200102015	Unable to locate the user's local identifier in the resource id.	Type: ERROR:NIDP:WSF:015 **Cause:** The web service resource id, an identifier indicating what user the request is destined for, did not contain the information required to identify the user. **Action:** Notify your system administrator that invalid web service requests are being made to the system.
200102016	Unable to locate a cached NIDPPrincipal object given the local id.	Type: ERROR:NIDP:WSF:016 **Cause:** The user session has expired. **Action:** The user must login again.
200102017	Unable to locate a NIDPIdentity object given the local id.	Type: ERROR:NIDP:WSF:017 **Cause:** The user session has expired. **Action:** The user must login again.
200103001	The indicated web service is not available or it has been disabled! An attempt was made to access this service to operate on the indicated data.	Type: ERROR:NIDP:WSC:001 **Cause:** The Web Service Consumer received a request and one of the data tokens referenced a data item that is not available in any of the services known to the Access Manager Appliance. **Action:** The system has encountered an invalid configuration and should be restarted by the system administrator.
200103002	Cannot make web service request because there are zero web service resource offerings available.	Type: ERROR:NIDP:WSC:002 **Cause:** The Web Service Consumer received a request but there were zero service resource offerings provided. So, the web service has no destination service to which a request can be made. **Action:** The user must login again.
200103003	Unable to locate an identity id from the authentications available in the provided NIDPSession.	Type: ERROR:NIDP:WSC:003 **Cause:** The user session has expired. **Action:** The user must login again.
200104001	Could not get client certificate.	Type: ERROR:NIDP:USERAUTH:001 **Cause:** Could not get user certificate from the client browser **Action:** Install user X509 certificate on the client browser and try again.

Event Code	Message	Remedy
200104003	Could not read configuration	Type: ERROR:NIDP:USERAUTH:003 **Cause:** Could not read configuration out of file **Action:** Make sure the X509 config properties file is present.
200104004	User Certificate Authentication Failed	Type: ERROR:NIDP:USERAUTH:004 **Cause:** User Certificate Authentication Failed due to the reasons in detailed message **Action:** Take appropriate action as per the reasons in the detailed message
200104005	No matching Principal found.	Type: ERROR:NIDP:USERAUTH:005 **Cause:** No Principal from X509Certificate found in User store **Action:** Check the X509Class Method and it's attribute mapping profile as defined using administration tool. Also, make sure the matched user exists in the User store.
200104006	More than one Principal matched.	Type: ERROR:NIDP:USERAUTH:006 **Cause:** Principal from X509Certificate Multiple users found in User store which matched Principal from X509Certificate based on X509Class attribute mapping profile.\ **Action:** Check the X509Class Method and it's attribute mapping profile as defined using administrator tool. Also, check if multiple user exists in the User store(s).
200104008	Error loading Trust store	Type: ERROR:NIDP:USERAUTH:008
200104009	Client certificate not yet valid.	Type: ERROR:NIDP:USERAUTH:009 **Cause:** X509 certificate is valid in the future **Action:** Use a valid certificate
200104010	Client certificate no longer valid.	Type: ERROR:NIDP:USERAUTH:010 **Cause:** X509 certificate is expired **Action:** Use a valid certificate
200104011	The Certificate has been revoked.	Type: ERROR:NIDP:USERAUTH:011 **Cause:** The Certificate has been revoked **Action:** Use a valid certificate which is not revoked.
200104012	Error Parsing Certificate.	Type: ERROR:NIDP:USERAUTH:012 **Cause:** Error Parsing Certificate when performing certificate validations **Action:** Use a valid X509 certificate.

Event Code	Message	Remedy
200104017	Error getting CRL/OCSP.	Type: ERROR:NIDP:USERAUTH:017 **Cause:** Could not get to the CRL/OCSP URL for validations. **Action:** Make sure the CRL/OCSP URLs are accessible Or disable validations in administration. Additionally, can define a different CRL/OCSP URL in the administration tool which the X509Class can also use for validations.
200104018	Could not verify CRL signature.	Type: ERROR:NIDP:USERAUTH:018 **Cause:** Could not verify signature on the fetched CRL **Action:** Make sure the CRL server public key/certificate is in NIDP/ESP trust store.
200104019	Could not find Key for this server.	Type: ERROR:NIDP:USERAUTH:019 **Cause:** Could not find Key/Cert for NIDP/ESP server towards authenticating to OCSP server **Action:** Make sure the NIDP/ESP Signing keystore has appropriate Key/Cert in it.
200104020	CRL/OCSP is too old; New version already available.	Type: ERROR:NIDP:USERAUTH:020 **Cause:** During validations, the fetched CRL Or OCSP is stale. Newer version will be available **Action:** In case of CRLs, next attempt to fetch CRL should get a fresh CRL after purging the cached one. In case of OCSP, notify the OCSP server administrator.
200104021	No Issuer Certificate found.	Type: ERROR:NIDP:USERAUTH:021 **Cause:** Issuer of user certificate not found which is required for OCSP validations **Action:** Make sure the issuer of user/client certificate is either found in certificate-chain or in NIDP/ESP trust store.
200104022	Error getting OCSP Response.	Type: ERROR:NIDP:USERAUTH:022 **Cause:** Could not get OCSP Response from the OCSP server **Action:** Make sure its going to the right OCSP server.
200104023	Error processing OCSP Response.	Type: ERROR:NIDP:USERAUTH:023 **Cause:** OCSP response could not be processed **Action:** Make sure its going to the right OCSP server and that it is operating correctly.

Event Code	Message	Remedy
200104024	At least one parameter of OCSPProcessor was uninitialized.	Type: ERROR:NIDP:USERAUTH:024 **Cause:** At least one parameter of OCSPProcessor was uninitialized during OCSP validations **Action:** Make sure the NIDP/ESP Signing keystore has appropriate Key/Cert in it. Also, that the NIDP/ESP OCSP trust store has the valid public-key/certificate of OCSP server.
200104025	Request was already generated.	Type: ERROR:NIDP:USERAUTH:025 **Cause:** OCSP request was already generated for certificate(s) **Action:** Check the client certificate chain.
200104026	OCSP response was already processed	Type: ERROR:NIDP:USERAUTH:026
200104027	Internal error occurred in the OCSP Server.	Type: ERROR:NIDP:USERAUTH:027 **Cause:** OCSP server responded to the request with an internal error. **Action:** Contact OCSP server administrator.
200104028	Your request did not fit the RFC 2560 syntax.	Type: ERROR:NIDP:USERAUTH:028 **Cause:** OCSP server responded to the request with malformed request message. **Action:** Contact OCSP administrator and check the request.
200104029	Your request was not signed.	Type: ERROR:NIDP:USERAUTH:029 **Cause:** Request to OCSP server needs to be signed. **Action:** Enable signing of OCSP requests in X509Class administration.
200104030	The server was too busy to answer you.	Type: ERROR:NIDP:USERAUTH:030 **Cause:** OCSP server is too busy to respond to requests. **Action:** Contact OCSP server administrator.
200104031	The server could not authenticate you.	Type: ERROR:NIDP:USERAUTH:031 **Cause:** OCSP server could not authenticate Novell Identity server. **Action:** Make sure Signing of OCSP requests is enabled and NIDP signing keystore has appropriate key in it. Also, make sure the OCSP server trusts Nidp server.

Event Code	Message	Remedy
200104032	Unknown OCSPResponse status code.	Type: ERROR:NIDP:USERAUTH:032 **Cause:** OCSP server responded to the request with unknown status code. **Action:** Contact OCSP server administrator.
200104033	No valid OCSPResponse obtained.	Type: ERROR:NIDP:USERAUTH:033 **Cause:** Invalid OCSP response obtained. **Action:** Check the OCSP server response version and contact administrator.
200104034	Response was generated in the future.	Type: ERROR:NIDP:USERAUTH:034 **Cause:** OCSP response is not yet valid. **Action:** Disable OCSP validations Or Contact OCSP server administrator.
200104035	Error verifying responder certificate.	Type: ERROR:NIDP:USERAUTH:035 **Cause:** This may happen when reading the OCSP trust store during OCSP validations. **Action:** Make sure OCSP trust store exists on NIDP server.
200104036	Response seems to be signed with untrusted certificate.	Type: ERROR:NIDP:USERAUTH:036 **Cause:** OCSP server trusted-root certificate not found in OCSP trust store. **Action:** Import OCSP server trusted root in Nidp's OCSP trust store.
200104037	The received responder id does not match your responder certificate.	Type: ERROR:NIDP:USERAUTH:037 **Cause:** The response ID received in OCSP response does not match. **Action:** Make sure NIDP's OCSP trust store has the right OCSP server public-key certificate.
200104038	Could not verify OCSP server response.	Type: ERROR:NIDP:USERAUTH:038 **Cause:** OCSP server response is incorrect. **Action:** Verify the OCSP server URL. Make sure NIDP's OCSP trust store has the right OCSP server public-key certificate.
200104039	No client certificates inside OCSP response.	Type: ERROR:NIDP:USERAUTH:039 **Cause:** Empty response from OCSP server. **Action:** Verify the OCSP server URL.

Event Code	Message	Remedy
200104040	Number of certificates inside OCSP response does not fit to request.	Type: ERROR:NIDP:USERAUTH:040 **Cause:** OCSP response does not contain the requested number of certificate status. **Action:** Verify the OCSP server URL.
200104041	Certificate was revoked in the future.	Type: ERROR:NIDP:USERAUTH:041 **Cause:** OCSP response not yet valid. **Action:** Verify the OCSP server URL.
200104042	Received certificate twice or one, that was not requested.	Type: ERROR:NIDP:USERAUTH:042 **Cause:** OCSP response does not match request. **Action:** Verify the OCSP server URL.
200104043	Request was not accepted.	Type: ERROR:NIDP:USERAUTH:043 **Cause:** Could not connect to OCSP server. **Action:** Verify the OCSP server URL.
200104044	Wrong response type (not application/ocsp-response).	Type: ERROR:NIDP:USERAUTH:044 **Cause:** Malformed OCSP response. **Action:** Verify the OCSP server URL.
200104045	No OCSPResponse message.	Type: ERROR:NIDP:USERAUTH:045 **Cause:** No OCSPResponse message. **Action:** Verify the OCSP server URL.
200104046	Could not read whole OCSPResponse.	Type: ERROR:NIDP:USERAUTH:046 **Cause:** Malformed OCSP response. **Action:** Verify the connection to OCSP server URL.
200104047	Exception Occurred.	Type: ERROR:NIDP:USERAUTH:047 **Cause:** Error getting CRL. **Action:** Verify the connection to CRL server URL.
200104051	Unsupported critical extension OID(s).	Type: ERROR:NIDP:USERAUTH:051 **Cause:** Some Critical extension OID(s) not understood. **Action:** Check the certificate for unsupported critical extensions. If needed, add the processing of the critical extension in NDPCertPathChecker class.
200104053	Error processing CRL Response.	Type: ERROR:NIDP:USERAUTH:053 **Cause:** Error processing CRL Response. **Action:** Check X509class config and user/client certificate CRL extension.

Event Code	Message	Remedy
200104054	Error processing certificate validations.	Type: ERROR:NIDP:USERAUTH:054 **Cause:** Error processing CRL/OCSP validations. **Action:** Check X509class config and user/client certificate CRL extension.
200104055	Protocol not supported or none specified.	Type: ERROR:NIDP:USERAUTH:055 **Cause:** Transport protocol not supported to fetch CRL. **Action:** Currently, CRLs can be fetched over http and LDAP protocols. Make sure the X509class config and/or user/client certificate CRL extension does not have any other transport protocol specified.
200104057	Unable to do X509 Certificate based authentication over non SSL (HTTP).	Type: ERROR:NIDP:USERAUTH:057 **Cause:** URL protocol is HTTP **Action:** URL protocol needs to be HTTPS
200104058	Overwrite a real or temp user error.	Type: ERROR:NIDP:USERAUTH:058 **Cause:** User is not identified in the authenticated user session. **Action:** Authenticate with a valid authentication contract to identify the user.
200104059	User store connection error.	Type: ERROR:NIDP:USERAUTH:059 **Cause:** LDAP replica connection error **Action:** Check the connectivity from the Identity server to LDAP replicas.
200104060	Problem in fetching password.	Type: ERROR:NIDP:USERAUTH:060 **Cause:** Error while fetching user password **Action:** Check the password policy for the user and verify that admin has permission to retrieve the password for that user.
200104061	Problem in provisioning the user.	Type: ERROR:NIDP:USERAUTH:061 **Cause:** Error while auto User provisioning for password fetch class. **Action:** Check whether admin has permission to create user and modify user's attributes in the LDAP store.
200104062	Auto provisioning successful.	Type: INFO:NIDP:USERAUTH:062 **Scenario:** Password fetch class was successful in auto provisioning user.

Event Code	Message	Remedy
200104063	Universal password retrieval error.	Type: ERROR:NIDP:USERAUTH:063 **Cause:** Universal password retrieval error with password fetch class. **Action:** Check the universal password policy for the user and verify that admin has permission to retrieve the password for that user.
200104064	Simple password retrieval error.	Type: ERROR:NIDP:USERAUTH:064 **Cause:** Simple password retrieval error with password fetch class. **Action:** Check the simple password policy for the user and verify that admin has permission to retrieve the password for that user.
200104065	User lookup failed.	Type: ERROR:NIDP:USERAUTH:065 **Cause:** User lookup failed for the Distinguished Name (DN) with password fetch class. **Action:** Create a user DN in the eDirectory from which the user password is retrieved.
200104066	Client Integrity Check (CIC) failed.	Type: ERROR:NIDP:USERAUTH:066 **Cause:** CIC failed. **Action:** Check if the required software is available on the system. Check the CIC class is configured properly. Check the logs on java console on the system.
200104100	Error processing Authorization header	Type: ERROR:NIDP:USERAUTH:100 **Cause:** Could not process HTTP Authorization header **Action:** Try with correct authorization header with base64 encoded SPNEGO token
200104101	Error processing SPNEGO/ Kerberos	Type: ERROR:NIDP:USERAUTH:101 **Cause:** Error processing SPNEGO/Kerberos. The cause is included in detailed message **Action:** Take action as per the detailed error message
200104102	No Kerberos Principal found in the token	Type: ERROR:NIDP:USERAUTH:102 **Cause:** Failure at GSS-API **Action:** Make sure the Kerberos keytab file is generated correctly by KDC
200104103	No SPNEGO Token found	Type: ERROR:NIDP:USERAUTH:103 **Cause:** No SPNEGO Token found in the request **Action:** Include the SPNEGO token in the request to use this authentication

Event Code	Message	Remedy
200104104	GSS Context already established	Type: ERROR:NIDP:USERAUTH:104 **Cause:** GSS Context already established **Action:** Close the browser and try again
200104106	Unrecognized SPNEGO Token	Type: ERROR:NIDP:USERAUTH:106 **Cause:** Unrecognized SPNEGO Token **Action:** Include the correct SPNEGO token in the request to use this authentication
200104109	Malformed SPNEGO NegTokenInit	Type: ERROR:NIDP:USERAUTH:109 **Cause:** Malformed token NegTokenInit **Action:** Try again with correct NegTokenInit token
200104110	Malformed SPNEGO Token field	Type: ERROR:NIDP:USERAUTH:110 **Cause:** Malformed SPNEGO Token field **Action:** Try again with correct NegTokenInit token
200104111	Multiple users matched in the user stores	Type: ERROR:NIDP:USERAUTH:111 **Cause:** Multiple users matched in the user stores **Action:** Make sure the users are unique in user stores
200104112	No user matched in the user stores	Type: ERROR:NIDP:USERAUTH:112 **Cause:** No user found in the user stores **Action:** Make sure the user attribute (as defined in admin UI) is populated in correct format.
200107005	Error building certificate chain during validations.	Type: ERROR:NIDP::005 **Cause:** This could occur when all the CDPs are unreachable. **Action:** Change the Certificate with correct CDPs or make sure CDP is up and able to serve.
300101002	An authenticated subject is required.	Type: WARN:NIDP:USERMSG:002 **Cause:** An action that can only be performed by an authenticated user was attempted. **Action:** Provide proper user credentials and retry desired action.
300101003	An authentication principal is required.	Type: WARN:NIDP:USERMSG:003 **Cause:** An action that can only be performed by an authenticated user was attempted. **Action:** User must be authenticated to perform operation.

Event Code	Message	Remedy
300101004	Identity does not exist or is not specified.	Type: WARN:NIDP:USERMSG:004 **Cause:** An action was attempted that requires a federated identity to exist. **Action:** Create a federated link prior to performing the action.
300101005	Invalid or no provider is specified.	Type: WARN:NIDP:USERMSG:005 **Cause:** An action was requested related to a trusted provider that does not exist. **Action:** Add the desired provider as a trusted entity or check for invalid access to system.
300101006	An authenticated session is required.	Type: WARN:NIDP:USERMSG:006 **Cause:** An action that can only be performed by an authenticated user was attempted. **Action:** Provide proper user credentials and retry desired action.
300101007	Invalid artifact.	Type: WARN:NIDP:USERMSG:007 **Cause:** An artifact was received from an identity provider that is invalid or has not been used within a reasonable time frame. **Action:** Make sure that the provider sending the artifact is trusted or check for possible security intrusions.

Event Code	Message	Remedy
300101008	No assertion returned in response. No authentication context specified message in the assertion.	Type: WARN:NIDP:USERMSG:008 **Cause:** Assertions will not be returned in a response whenever authentication at the identity provider fails. The cause for this can include invalid configurations and canceling the authentication process at the identity provider. This response is also returned when a user has reached the maximum number of sessions and then attempts to access a protected resource that requires authentication. **Action:** Make sure that both the identity and service providers are configured correctly to trust each other. Provide proper credentials during the authentication process at the identity provider. **Cause:** Protected resources are configured to access using external contracts, which are being executed at the external identity provider. These contracts are not configured to be satisfied by any of the external identity provider. **Action1:** Verify the external identity provider satisfiable contract list at the service provider and ensure that these external contracts are configured under the satisfiable list. **Action 2:** Verify the external contract definition at the identity provider and make sure that this contract definition with the matching allowable class or URI is available. **NOTE:** URI specifies a value that uniquely identifies the contract from all other contracts.
300101009	Invalid issuer.	Type: WARN:NIDP:USERMSG:009 **Cause:** A response was received from a provider that is not trusted. **Action:** Make sure intended provider is trusted or check for possible intrusions.
300101010	Response does not match request.	Type: WARN:NIDP:USERMSG:010 **Cause:** A response was received for a request that was not issued. **Action:** Retry action and check for possible intrusion.
300101011	Assertion is being replayed.	Type: WARN:NIDP:USERMSG:011 **Cause:** An assertion has been received that was already used to authenticate a user at the service provider. **Action:** This is a security mechanism that if persists may require some investigation to determine who is trying to replay the assertion. Assertions are only good for single use.

Event Code	Message	Remedy
300101012	Assertion does not contain an authentication statement.	Type: WARN:NIDP:USERMSG:012 **Cause:** An identity provider has sent an assertion that is not complete. **Action:** Check with administrator of trusted provider to determine why statement is not being sent.
300101013	Unable to validate the subject of the assertion.	Type: WARN:NIDP:USERMSG:013 **Cause:** A subject may not have been sent in the assertion or was not valid. This check protects from certain assertion attacks. If the time is not in sync between the identity provider and the service provider, the subject is invalid because of the timestamp sent with the subject. **Action:** If persistent, check the protocol message sent for a time discrepancy between the providers or a missing subject, then notify the administrator of the trusted site. For more information, see "Federation with External SAML 2.0 Partner Gives 300101013 Error" (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3903427&sliceId=2&docTypeID=DT_TID_1_1&dialogID=69860557&stateId=0%200%2069862016).
300101014	Assertion not yet valid.	Type: WARN:NIDP:USERMSG:014 **Cause:** An assertion was received that is not valid until sometime in the future. **Action:** Check server's clock for accuracy. Attempt to validate the clock accuracy of the computer generating the assertion.
300101015	Assertion no longer valid.	Type: WARN:NIDP:USERMSG:015 **Cause:** An assertion was received that had a time validity period that is in the past. **Action:** Check server's clock for accuracy. Attempt to validate the clock accuracy of the computer generating the assertion. Try to authenticate again.
300101016	No matching audience.	Type: WARN:NIDP:USERMSG:016 **Cause:** An assertion was received that was not intended for your server. **Action:** Determine the origin of the assertion and make sure that you want to accept assertions from it. For more information, see "Access Manager 300101016 Error - No Matching Audience" (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3260366&sliceId=2&docTypeID=DT_TID_1_1&dialogID=69860436&stateId=0%200%2069856899).

Event Code	Message	Remedy
300101017	Missing or invalid signature on assertion.	Type: WARN:NIDP:USERMSG:017 **Cause:** The identity provider did not sign. **Action:** Check with provider of assertion to determine why assertion is not signed.
300101018	Missing or invalid signature on request/response.	Type: WARN:NIDP:USERMSG:018
300101020	Digital signature is required.	Type: WARN:NIDP:USERMSG:020 **Cause:** A protocol message was received that was expected to be digitally signed, but was not. **Action:** It may be necessary to contact the trusted provider administrator to determine why the message is not signed. Make sure authentication request signing settings match those for the trusted provider.
300101021	Signature validation failed.	Type: WARN:NIDP:USERMSG:021 **Cause:** The digital signature of a protocol message could not be verified using the public key obtained in the metadata of a trusted provider. **Action:** Update the metadata of trusted provider. This should ensure you have the latest signing certificate.
300101022	An undetermined problem in the message format has occurred.	Type: WARN:NIDP:USERMSG:022 **Cause:** An error was detected in the exchange of either a Liberty or SAML protocol message. **Action:** Turn logging/tracing on to print out the message that is problematic. It may be necessary to contact Novell Technical Services in this case.
300101023	User lookup failed.	Type: WARN:NIDP:USERMSG:023 **Cause:** An attempt to identify a user failed while attempting to complete a federation at the server. **Action:** Check the configuration for identifying users for the trusted provider and ensure the specified method can resolve to a single user in your directory.
300101024	Failed to load java class.	Type: WARN:NIDP:USERMSG:024 **Cause:** A Java class failed to be loaded during program execution. **Action:** Check the logs to determine the class that is failing to load. Make sure the class being loaded is in the classpath of the JVM.
300101025		Type: WARN:NIDP:USERMSG:025
300101026		Type: WARN:NIDP:USERMSG:026
300101027		Type: WARN:NIDP:USERMSG:027

Event Code	Message	Remedy
300101028	SOAP TLS authorization failed.	Type: WARN:NIDP:USERMSG:028 **Cause:** SSL mutual authentication is being used to authenticate a SOAP back channel session and the credentials cannot be validated. **Action:** Make sure certificates for back channel communications are trusted on each end. For more information, see "Access Manager 300101028 - SOAP TLS Authorization Failed" (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3813149&sliceId=2&docTypeID=DT_TID_1_1&dialogID=69848431&stateId=0%200%2069844751).
300101029		Type: WARN:NIDP:USERMSG:029
300101030	SOAP fault.	Type: WARN:NIDP:USERMSG:030 **Cause:** An error was detected in the transmission of protocols using SOAP. **Action:** Turn tracing on and look for any obvious causes for the problem.
300101031	Received an identity that does not resolve to the current logged in user.	Type: WARN:NIDP:USERMSG:031 **Cause:** This is caused when a user is logged in with one identity and then attempts to authenticate as the identity of another user. For a given session, all authentications must resolve to the same user. **Action:** Log out of the current user and log in again as the desired user.
300101032	Assertion is expired.	Type: WARN:NIDP:USERMSG:032 **Cause:** The use of the assertion to authenticate the server did not occur within the time limits specified by the assertion. **Action:** Try and re-authenticate. Determine if there are any network latencies that may cause the assertion not to arrive in a timely fashion. Look for misuse of the assertion.
300101033	IDP return authentication failure.	Type: WARN:NIDP:USERMSG:033 **Cause:** An IDP's attempt to authenticate the server was unsuccessful. This particular authentication came from the IDP's intersite transfer service and was not requested by the server. **Action:** Check at the IDP for a reason why the authentication was a failure. It may just be necessary to attempt authentication again.

Event Code	Message	Remedy
300101034	No target is defined.	Type: WARN:NIDP:USERMSG:034 **Cause:** A request was made of the server's intersite transfer service without specifying a target resource. **Action:** Requests for the intersite transfer service must include an id of the intended service provider to be authenticated as well as the target resource to be displayed. To avoid this error, provide an &TARGET="value" on the URL.
300101035		Type: WARN:NIDP:USERMSG:035
300101036	Not enough memory to process request.	Type: WARN:NIDP:USERMSG:036 **Cause:** The system does not have enough memory to complete the requested action. **Action:** Wait a few moments for memory to free up and retry request. It may be necessary to add additional memory to the server.
300101037	Server is not in a running state.	Type: WARN:NIDP:USERMSG:037 **Cause:** A request was made of the server that can only be performed when the server is in a running state. **Action:** Start the server.
300101038	JSP file not found.	Type: WARN:NIDP:USERMSG:038 **Cause:** An attempt was made to load a JSP page that does not exist. **Action:** Determine the JSP not loading and make sure it is in the correct location.
300101039	Invalid authentication credentials were provided.	Type: WARN:NIDP:USERMSG:039 **Cause:** A user has attempted to authenticate to the system with credentials that are not valid for the account. **Action:** User needs to enter correct credentials.
300101040	User password has expired.	Type: WARN:NIDP:USERMSG:040 **Cause:** A user has attempted to authenticate to the system with a password that is expired. **Action:** The user needs to create a new password.

Event Code	Message	Remedy
300101041	User account identification failed.	Type: WARN:NIDP:USERMSG:041 **Cause:** Account identification can fail due to: 1. User cancels authentication request 2. User cannot be uniquely identified by Matching Expression 3. Necessary attributes to do user matching or provisioning were not obtained. **Action:** Check Account Identification configuration for the trusted provider and make sure that necessary attributes are available. If using Matching Expressions, make sure that they include attributes that can resolve to a single user. If using Provisioning, make sure required attributes are all available in the defined attribute set for the trusted provider. For more information, see "Access Manager Error 300101041 Provisioning New Users Using SAML2" (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3219302&sliceId=1&docTypeID=DT_TID_1_1&dialogID=69780245&stateId=0%200%2069778277).
300101042	Invalid assertion conditions.	Type: WARN:NIDP:USERMSG:042 **Cause:** A set of conditions that are not understood were sent as part of an assertion. **Action:** Check with the provider of the assertion to determine what these conditions are and why they are being sent.
300101046	Unknown URL host.	Type: WARN:NIDP:USERMSG:046 **Action:** Use logs to determine the problematic host and determine why DNS is failing.
300101047	An untrusted provider is being referenced in a request or a response.	Type: WARN:NIDP:USERMSG:047 **Action:** Use logs to determine the provider that is untrusted and then create a trusted relationship if desired.
300101048	The LDAP servers are too busy to accept more users.	Type: WARN:NIDP:USERMSG:048 **Cause:** There are too many threads waiting to get an available LDAP connection. The LDAP servers are too busy to accept more users. **Action:** Wait a few moments for the LDAP requests to be processed and retry the request. It may be necessary to add additional LDAP servers or upgrade the hardware specifications of the existing LDAP servers.
300101049	The HTTPS protocol was not used to access this authentication card.	Type: WARN:NIDP:USERMSG:049 **Cause:** Accessing the site was done via http, not https. **Action:** Access the site again using https.

Event Code	Message	Remedy
300101050	The Authentication Card specified is not valid.	Type: WARN:NIDP:USERMSG:050 **Cause:** An invalid card identifier was used, most likely due to modifying a url. **Action:** Specify cards to use only by clicking them. Ensure that the PID in the login URL exactly matches the entity ID specified in the metadata.
300101051	The user's session limit has been reached.	Type: WARN:NIDP:USERMSG:051 **Cause:** User has already logged in the maximum allowable times. **Action:** Logout of one or more sessions.
300101052	A response was expected at the url but none was found.	Type: WARN:NIDP:USERMSG:052 **Cause:** The wrong endpoint may be accessed for the operation desired. **Action:** Check the action being performed against the url/endpoint being accessed.
300101053	CardSpace authentication profile failed to load.	Type: WARN:NIDP:USERMSG:053 **Cause:** Trusted provider failed to load (probably due to certificate errors). **Action:** Check the certificates for the trusted provider and make sure they are valid.
300101054	CardSpace authentication fails because a required attribute is not in assertion.	Type: WARN:NIDP:USERMSG:054 **Cause:** A required attribute was not returned in the assertion provided by an STS. **Action:** Check the attribute value at the STS, or make the attribute optional.
300101057	Request to broker an authentication to a target SP denied	Type: WARN:NIDP:USERMSG:057 **Cause:** Request to broker an authentication to a target Service Provider denied, either the Identity Provider or target Service Provider are part of a brokering group, but both does not belong to same group. **Action:** Check the brokering group to verify if the Identity Provider and target Service Provider belong to the same group.
300101058	Request to broker on authentication to a target SP denied	Type: WARN:NIDP:USERMSG:058 **Cause:** Request to broker on authentication to a target Service Provider denied because broker policy evaluation resulted in denying. **Action:** Check the brokering rule and try to access with the valid user.

Event Code	Message	Remedy
300101059	Error in processing the broker request.	Type: WARN:NIDP:USERMSG:059 **Cause:** Could not validate the request to broker on authentication to a target service provider. **Action:** Read the error description supplied and take appropriate action.
300101060	Assertion does not contain valid authentication statement.	Type: WARN:NIDP:USERMSG:060 **Cause:** An assertion has been received, which does not contain valid declaration/class statement. **Action:** Authentication response statement will be validated against the authentication request statement. Check the contract definition in the service provider for the authentication statement received from the Identity Provider. Check if the requested statement matches the response statement or response statement's authentication level is greater than the requested one.
300101061	Failed to obtain consent for the federation.	Type: ERROR:NIDP:USERMSG:061 **Cause:** This is a message to users if they have declined the consent. If it is a valid federation consent, accept the consent in the next attempt, else deny the same. **Action:** In a federated setup using the name identifier as persistent, if you make an Intersite Transfer Service request for the first time federation, users will be asked to provide their consent and they select No.
300101062	An Identity Provider response was received that failed to authenticate this session.	**Cause:** When you configure a policy for a spsend request to SAML 2.0, the user is denied the policy rule, and a message is displayed. **Action:** You are accessing an URL that is not intended for you. Contact your administrator.
300102001	No Discovery Service Configured! Unable to create the requested resource offering!	Type: WARN:NIDP:WSF:001 **Cause:** The system administrator did not create or enable a Discovery service. **Action:** Create or enable a Discovery web service.
300102002	Unable to find user object with identifier.	Type: WARN:NIDP:WSF:002 **Cause:** An LDAP search was performed for a user object with a given identifier. This identifier may be a GUID. The search resulted in zero hits. This usually means that web service data cannot be read or written for the user. **Action:** The user needs to login again.

Event Code	Message	Remedy
300102003	Unrecognized select string for service.	Type: WARN:NIDP:WSF:003 **Cause:** The select string (XPath) is either incorrectly formed or not supported by the web service. **Action:** The system administrator must enable services to support the select string.
300102004	Unable to process web service query request! Select string missing!	Type: WARN:NIDP:WSF:004 **Cause:** The select string (XPath) is not in the web service query request. **Action:** Inform your system administrator that an improperly formatted web service request is being made.
300102005	Unable to perform trusted user interaction service request. Web service authority was not found.	Type: WARN:NIDP:WSF:005 **Cause:** An internal system error. **Action:** The system has encountered an invalid configuration and should be restarted by the system administrator.
300102006	Unable to perform trusted user interaction service request. Unable to obtain trusted user interaction service description from SOAP headers.	Type: WARN:NIDP:WSF:006 **Cause:** The web service making the request did not provide valid or complete information about the trusted user interaction service. **Action:** The system administrator must complete the definition of the trusted interaction service.
300102007	Unable to perform trusted user interaction service request. No trusted user interaction service description provided in SOAP headers.	Type: WARN:NIDP:WSF:007 **Cause:** The web service making the request did not provide valid or complete information about the trusted user interaction service. **Action:** The system administrator must complete the definition of the trusted interaction service.
300102008	Trusted user interaction service failed.	Type: WARN:NIDP:WSF:008 **Cause:** There are various unexpected reasons for the failure of a trusted user interaction service request to fail. **Action:** Evaluate the reason and take the appropriate actions.
300102009	Error creating user interaction redirection request.	Type: WARN:NIDP:WSF:009 **Cause:** There was an error converting the redirect request to an XML DOM. **Action:** Evaluate the reason and take the appropriate actions.

Event Code	Message	Remedy
300102010	Unable to perform user interaction redirection request. User intervention service not found.	Type: WARN:NIDP:WSF:010 **Cause:** There must be an interaction service on the IDP creating the user interaction redirection request. **Action:** If it does not exist, using Access Manager Appliance management tools, create one.
300102011	Error reading data from LDAP data attribute plugin.	Type: WARN:NIDP:WSF:011 **Cause:** If a web service's data locations includes LDAP, then LDAP data attribute plugins are used to read data from the LDAP user store. This error provides descriptions of various errors that can happen while doing this. **Action:** Evaluate the reason and take the appropriate actions.
300102012	Error writing data to LDAP data attribute plugin.	Type: WARN:NIDP:WSF:012 **Cause:** If a web service's data locations includes LDAP, then LDAP data attribute plugins are used to write data to the LDAP user store. This error provides descriptions of various errors that can happen while doing this. **Action:** Evaluate the reason and take the appropriate actions.
300102013	Cannot read/write Credential Profile data because the user's LDAP user store distinguished name is not available.	Type: WARN:NIDP:WSF:013 **Cause:** All Credential Profile reads and writes end up operating on a user object in a user store. If this user object cannot be found, then the operation must fail. This may happen if a temporary identifier is being used for the authentication. **Action:** Use a permanent federation to the service provider if your system allows it.
300102014	A Web Service request was received for a user, but the session for that user is not found.	Type: WARN:NIDP:WSF:014 **Cause:** The user's login has timed out and has been removed from the system. **Action:** The user must login again.
300102015	A Web Service request was received for a user, but the session for that user has insufficient data in it.	Type: WARN:NIDP:WSF:015 **Cause:** An internal error has occurred. **Action:** The user must login again.
300102016	A Web Service request was received for a user, but the Liberty User Profile object for that user is unavailable.	Type: WARN:NIDP:WSF:016 **Cause:** An internal error has occurred. **Action:** Make sure the administrator user has rights to read, write and create Liberty User Profile objects in the configuration data store.

Event Code	Message	Remedy
300102017	A Web Service request was received for a user, and attempt to read the requested attributes from the Liberty User Profile object was made, but an error occurred.	Type: WARN:NIDP:WSF:017 **Cause:** An internal error has occurred. **Action:** Evaluate the reason and take the appropriate actions.
300102018	A Web Service request was received for a user, While reading user data from an LDAP user object, a mismatch occurred because the LDAP attribute is multi-valued, but the Liberty attribute is single-valued.	Type: WARN:NIDP:WSF:018 **Cause:** A multi-valued LDAP attribute has been mapped to a single-valued Liberty attribute. **Action:** Change the attribute mapping.
300102019	The user used an X509 Certificate to authenticate and we tried to put the cert into the SecretStore as a Base64 DER encoded cert, but we got an encoding error from the security layer when trying to get the DER encoded cert. Result is that there will not be a X509 Certificate in Secret Store for this user.	Type: WARN:NIDP:WSF:019 **Cause:** The X509 certificate cannot be encoded. **Action:** Review the type of X509 certificates that are being used for authentication.
300102020	A SAMLAssertion was requested for a given user. While generating the SAMLAssertion an error occurred.	Type: WARN:NIDP:WSF:020 **Cause:** The SAMLAssertion cannot be created. **Action:** Review the reason for the failure and take appropriate actions.
300102021		Type: WARN:NIDP:WSF:021
300102022		Type: WARN:NIDP:WSF:022
300103001	The web service request did not return a response within the protocol timeout limit. Request abandoned.	Type: WARN:NIDP:WSC:001 **Cause:** The web service consumer waited for the web service request to return a response, but it did not during the allowed waiting period. **Action:** This waiting period may be increased by click Access Manager > Identity Servers > Edit > Liberty > Web Service Consumer, and setting the Protocol Timeout to a higher value.
300103002	An unexpected error happened in the web service consumer while processing a web service request.	Type: WARN:NIDP:WSC:002 **Cause:** There are various reasons why a web service request could fail. **Action:** Evaluate the reason and take appropriate actions.

Event Code	Message	Remedy
300103003	Web service consumer request pending data packet id is not available in request.	Type: WARN:NIDP:WSC:003 **Cause:** After user interaction, processing of the original request returns to the web service consumer. A data packet containing information about how to continue the request is cached on the web service consumer. The id of that packet must be passed through all redirections and requests associated with the user interaction. If that id is not available when the web service consumer regains control, then the request cannot continue. **Action:** Submit the request again.
300103004	The Web service consumer request pending data packet with the indicated id is not available in web service consumer's cache.	Type: WARN:NIDP:WSC:004 **Cause:** After user interaction, processing of the original request returns to the web service consumer. A data packet containing information about how to continue the request is cached on the web service consumer. The id of that packet must be passed through all redirections and requests associated with the user interaction. That id will be used to access the pending data packet when the web service consumer regains control. If the pending data packet with the corresponding id is no longer available on the system, then the request cannot continue. The data packet may have timed out. **Action:** Submit the request again.
300104049	Could not find NIDP PKIX Certificate Path Checker Class.	Type: WARN:NIDP:USERAUTH:049 **Cause:** PKIX Certificate Path Checker Class not found. **Action:** Warning message that PKIX Certificate Path Checker Class not found. This optional class is used to process custom certificate extensions. If required, this class needs to be in NIDP classpath. It may not be present on ESP.
300104050	Could not instantiate NIDP PKIX Certificate Path Checker Class.	Type: WARN:NIDP:USERAUTH:050 **Cause:** Incorrect class constructor. **Action:** Make sure the class has the right constructor.
300105001	No user Login Policy Check LDAP Extension method available on user store.	Type: WARN:NIDP:APP:001 **Cause:** User authenticated using X509. An additional check of the directory's user login policy needs to be made using an LDAP method extension. However, the directory indicated does not support the required LDAP extension method. **Action:** Make sure the LDAP extension method with OID 2.16.840.1.113719.1.39.42.100.25 is present in the user store. Versions 8.7.3 and greater of eDirectory should support this method.
300105002		Type: WARN:NIDP:APP:002
300105003		Type: WARN:NIDP:APP:003

Event Code	Message	Remedy
300105004		Type: WARN:NIDP:APP:004
300105005		Type: WARN:NIDP:APP:005
300105006		Type: WARN:NIDP:APP:006
300105007		Type: WARN:NIDP:APP:007
300105008		Type: WARN:NIDP:APP:008
300105009		Type: WARN:NIDP:APP:009
300105010		Type: WARN:NIDP:APP:010
300105011		Type: WARN:NIDP:APP:011
300105012		Type: WARN:NIDP:APP:012
300105013		Type: WARN:NIDP:APP:013
300105014		Type: WARN:NIDP:APP:014
300105015		Type: WARN:NIDP:APP:015
300105016		Type: WARN:NIDP:APP:016
300105017		Type: WARN:NIDP:APP:017
300105018		Type: WARN:NIDP:APP:018
300105019		Type: WARN:NIDP:APP:019
300105020		Type: WARN:NIDP:APP:020
300105021	Unable to delete unneeded Image Pool Image File.	Type: WARN:NIDP:APP:21 **Cause:** On startup, the NIDP Image Pool is synchronized from eDirectory to the file system. This allows HTML pages to access images from a well known file system structure. Part of synchronization process involves deleting from the file system images that no longer exist in eDirectory. Also, the reverse is true, images that are new to eDirectory and do not yet exist on the file system are created in directories that reflect the image set. File system errors may occur during this synchronization process if a file or directory cannot be deleted or created. **Action:** Ensure that no errant files are copied or directories manually created in the file system path [TOMCAT_HOME]/webapps/nidp/images/pool. Make sure the disk is not full.

Event Code	Message	Remedy
300105022	Unable to create a necessary directory for the Image Pool.	Type: WARN:NIDP:APP:22 **Cause:** On startup, the NIDP Image Pool is synchronized from eDirectory to the file system. This allows HTML pages to access images from a well known file system structure. Part of synchronization process involves deleting from the file system images that no longer exist in eDirectory. Also, the reverse is true, images that are new to eDirectory and do not yet exist on the file system are created in directories that reflect the image set. File system errors may occur during this synchronization process if a file or directory cannot be deleted or created. **Action:** Make sure the disk is not full.
300105023	Unable to create a necessary directory for the Image Pool.	Type: WARN:NIDP:APP:23 **Cause:** On startup, the NIDP Image Pool is synchronized from eDirectory to the file system. This allows HTML pages to access images from a well known file system structure. Part of synchronization process involves deleting from the file system images that no longer exist in eDirectory. Also, the reverse is true, images that are new to eDirectory and do not yet exist on the file system are created in directories that reflect the image set. File system errors may occur during this synchronization process if a file or directory cannot be deleted or created. **Action:** Make sure the disk is not full.
300105024	Unable to update the "last used" attribute of an identity object.	Type: WARN:NIDP:APP:24 **Cause:** Each time an identity object is accessed, the "last used" time is updated. This allows the system to track identities that have not been used for a configurable time period so that they may be deleted. **Action:** Make sure the administrator object for the Trust/Config data store has rights to the indicated directory context.
300105025	Unable to auto delete an identity object.	Type: WARN:NIDP:APP:25 **Cause:** Periodically, the IDP attempts to clean up (delete) identity objects that have not been used for a configurable period of time. If an old unused identity is found, an attempt will be made to delete it. If that delete fails, this error will be logged. **Action:** Make sure the administrator object for the Trust/Config data store has rights to the indicated directory context.

Event Code	Message	Remedy
300105027	No Filename specified in System property.	Type: WARN:NIDP:APP:27 **Cause:** Trying to read properties from file which is not specified in System property. **Action:** Make sure the properties file is passed in the appropriate system property.
300105028	Error trying to delete a CardSpace Issued Card Identity Object.	Type: WARN:NIDP:APP:28 **Cause:** When a CardSpace Managed Card that is backed by a Personal Card is issued, an Identity object is created to represent the "Federation" that allows that card to log into the IDP without supplying any additional credentials. For security reasons, the user may delete that Identity object, or that "federation," when the associated card becomes out of date or compromised. However, when the system attempted to delete the Identity object, the indicated error happened. **Action:** Examine the supplied error detail and take applicable actions.
300105029	Cannot load a custom LDAP Store Plugin module.	Type: WARN:NIDP:APP:29 **Cause:** The java.lang.Class.forName() method call failed to load the LDAP Store Plugin class. **Action:** Ensure a valid Java class file is available in Access Manager's class path for the referenced plugin class file.
300105030	Cannot instantiate a custom LDAP Store Plugin module.	Type: WARN:NIDP:APP:30 **Cause:** The java.lang.Class.newInstance() method call failed to instantiate the LDAP Store Plugin class. **Action:** Ensure a valid Java class file is available in Access Manager Appliance's class path for the referenced plugin class file. Also, ensure the LDAP Store Plugin has a zero parameter constructor.
300105031	A user store was configured with an unrecognized directory type.	Type: WARN:NIDP:APP:031 **Cause:** The configuration was manually modified to include an invalid directory type specifier. Or the configuration has been corrupted. Or there was no valid implementation of an LDAP Store Plugin for this directory type. **Action:** Examine the supplied error detail and take applicable actions.
300105036	Office365 assertion NameID value is null, check user <user name> attribute value.	**Cause:** User LDAP attribute value is empty in the user store. **Action:** Check the user attribute in configured user store. If NameID value is null, check user {1} attribute {0} value.
300106001		Type: WARN:NIDP:IDFF:001

Event Code	Message	Remedy
300106002		Type: WARN:NIDP:IDFF:002
300106003		Type: WARN:NIDP:IDFF:003
300106004		Type: WARN:NIDP:IDFF:004
300106005		Type: WARN:NIDP:IDFF:005
500102001	The authentication information for the user was successfully found.	Type: INFO:NIDP:WSF:001 Scenario: A Web Service request was made to query or modify user attributes. The user's authentication information was successfully found. See Also: 600102001
500102002	The Liberty User Profile object for the associated user was found in the configuration datastore.	Type: INFO:NIDP:WSF:002 Scenario: A Web Service request was made to query or modify user attributes. One of the data locations specified for the service is the Liberty User Profile object and that object was successfully found.
500102003	Created new user profile object.	Type: INFO:NIDP:WSF:003 Scenario: A request was made to query or modify user's attributes. A Liberty User Profile object did not yet exist for this user, so one was created.
500102004	Read data from user profile object.	Type: INFO:NIDP:WSF:004 Scenario: A Web Service request was made to query user attributes. One of the data locations specified for the service is the Liberty User Profile object and that object was successfully read. See Also: 600102002
500102005	Attempted to read data from the Liberty User Profile object, but it did not contain the requested data.	Type: INFO:NIDP:WSF:005 Scenario: A Web Service request was made to query user attributes. One of the data locations specified for the service is the Liberty User Profile object. That object was successfully accessed but did not contain the requested data.
500102006	Read data from attributes obtained when a remote authentication source pushed the attributes to the NIDP.	Type: INFO:NIDP:WSF:006 Scenario: When a user authenticates, the authentication entity can push user attributes to the NIDP as part of the response to the authentication. The NIDP remembers these attributes for the life of that user session. If one of the data locations specified for a Web Service is remote, then these attributes may be returned as part of a query. See Also: 600102005

Event Code	Message	Remedy
500102007	Read data by making a call to a remote service made available through a user authentication.	Type: INFO:NIDP:WSF:007 Scenario: A request was made to query a user's attributes. One of the data locations for the Web Service was remote. So, a request was made to a remote service to read attributes. See Also: 600102006
500102008	Completed building composite data that was read from all data locations for user.	Type: INFO:NIDP:WSF:008 Scenario: A request was made to query a user's attributes. If multiple data locations are specified for the Web Service, then attributes may be read from multiple data locations and then aggregated into a composite data structure. See Also: 600102007
500102009	Initiating a user interaction redirect.	Type: INFO:NIDP:WSF:009 Scenario: A request was made to query or modify user's attributes. Policy indicates that the user must be asked if the attribute operation is permitted. The request indicated that a redirect user interaction service should be used to perform user interaction, so redirection is being invoked using the redirection user interaction service protocol.
500102010	Initiating a user interaction call to a trusted user interaction service.	Type: INFO:NIDP:WSF:010 Scenario: A request was made to query or modify user's attributes. Policy indicates that the user must be asked if the attribute operation is permitted. The request indicated that a trusted user interaction service should be used to perform user interaction, so that service is being invoked using the trusted user interaction service protocol.
500102011	Read Credential Profile data from Novell Secret Store.	Type: INFO:NIDP:WSF:011 Scenario: A request was made to query data from a user's Credential Profile. The data was successfully read. See Also: 600102008
500102012	Read Credential Profile data from an extended user authentication object attribute.	Type: INFO:NIDP:WSF:012 Scenario: A request was made to query data from a user's Credential Profile. The data was read from an extended schema attribute on the user's authenticated user object. See Also: 600102010
500102013	Web service data write denied because the LDAP attribute plugin access for the named data item is read only!	Type: INFO:NIDP:WSF:013 Scenario: The system administrator has marked this data item as read only in the LDAP Attribute Plugin.

Event Code	Message	Remedy
500102014	Override not allowed. Cannot override existing data.	Type: INFO:NIDP:WSF:014 Scenario: The data that is being written already exists in the user's profile. Data override is not allowed so this data cannot be written.
500102015	Existing data changed since notChangedSince time.	Type: INFO:NIDP:WSF:015 Scenario: User profile data is marked with the last time the data changed. The query request indicated that it did not want the data written if the current data in the profile has been changed since an indicated time. The system determined that the current data in the profile has been changed since the time provided, so this data cannot be written.
500103001	Filled the user attribute request from data already in the web service consumer cache.	Type: INFO:NIDP:WSC:001 Scenario: When the WSC reads user attributes, it caches the results of each read. In this case, a subsequent request queried attributes already read, so they were provided from the WSC cache.
500103002	Web service consumer request complete.	Type: INFO:NIDP:WSC:002 Scenario: The WSC was asked to query or modify data for a given user. That request is complete.
500103003	Web service consumer request requires user interaction.	Type: INFO:NIDP:WSC:003 Scenario: The WSC was asked to query or modify data for a given user. The entity called to perform the operation indicated that the user must be asked if the attribute operation is acceptable.
500103004	User interaction policy and data values received.	Type: INFO:NIDP:WSC:004 Scenario: A Web Service request was made to query or modify user attributes. It was determined that the user must be asked if the attribute operation is acceptable. The user's answers have been returned to the NIDP.
500104002	Getting properties from file (informational)	Type: INFO:NIDP:USERAUTH:002 Scenario: Getting properties from file
500104007	X509 Authentication matched principal (informational)	Type: INFO:NIDP:USERAUTH:007 Scenario: X509 Authentication matched principal
500104013	No CRL/OCSP defined by the administrator	Type: INFO:NIDP:USERAUTH:013 Cause: No CRL/OCSP defined by the administrator
500104014	No CRL/OCSP found in the certificate.	Type: INFO:NIDP:USERAUTH:014 **Cause:** No CRL/OCSP found in the certificate **Action:** CRL/OCSP validations are enabled but no CRL/OCSP responder URL was defined by the administrator. CRL/OCSP URLs may be defined if needed.

Event Code	Message	Remedy
500104016	Could not fetch CRL from the local cache (informational)	Type: INFO:NIDP:USERAUTH:016 Scenario: Could not fetch CRL from the local cache, getting it from the CDP
500104048	Successfully loaded NIDP PKIX Certificate Path Checker Class (informational)	Type: INFO:NIDP:USERAUTH:048 Scenario: Successfully loaded NIDP PKIX Certificate Path Checker Class
500104113	Kerberos Principal match found in the user store (informational)	Type: INFO:NIDP:USERAUTH:113 Scenario: Kerberos Principal found in the user store
500105001	Forwarding HTTP request to cluster member.	Type: INFO:NIDP:APP:001 Scenario: A request was received on a cluster member that does not own the authentication information for the associated user. The request must be processed on the cluster member that does own the user authentication information, so the request is being forwarded to that cluster member.
500105002	Successfully initialized JNDI connections.	Type: INFO:NIDP:APP:002 Scenario: NIDP attempts to create JNDI connections to each user store replica during NIDP startup. In this case, NIDP was able to establish connections with the indicated host.
500105003	Failed X509 authentication due to Login Policy Check Extension Method evaluation.	Type: INFO:NIDP:APP:003 Scenario: The directory login policy for the indicated user denied login.
500105004	An recoverable error happened while forwarding a login request.	Type: INFO:NIDP:APP:004 Scenario: The request landed on the wrong cluster member. An attempt was made to proxy the request, but an error occurred! However, this ESP can process this request, so let execution proceed on this box.
500105005		Type: INFO:NIDP:APP:005
500105006		Type: INFO:NIDP:APP:006
500105007		Type: INFO:NIDP:APP:007
500105008		Type: INFO:NIDP:APP:008
500105009		Type: INFO:NIDP:APP:009
500105010		Type: INFO:NIDP:APP:010
500105011		Type: INFO:NIDP:APP:011
500105012		Type: INFO:NIDP:APP:012
500105013		Type: INFO:NIDP:APP:013
500105014		Type: INFO:NIDP:APP:014
500105015		Type: INFO:NIDP:APP:015

Event Code	Message	Remedy
500105016		Type: INFO:NIDP:APP:016
500105017		Type: INFO:NIDP:APP:017
500105018		Type: INFO:NIDP:APP:018
500105019		Type: INFO:NIDP:APP:019
500105020		Type: INFO:NIDP:APP:020
500105021		Type: INFO:NIDP:APP:021
500105022		Type: INFO:NIDP:APP:022
500105023		Type: INFO:NIDP:APP:023
500105024		Type: INFO:NIDP:APP:024
500105025		Type: INFO:NIDP:APP:025
500105026		Type: INFO:NIDP:APP:026
500105027		Type: INFO:NIDP:APP:027
500105028		Type: INFO:NIDP:APP:028
500105029		Type: INFO:NIDP:APP:029
500105030		Type: INFO:NIDP:APP:030
500105031		Type: INFO:NIDP:APP:031
500105032		Type: INFO:NIDP:APP:032
500105033		Type: INFO:NIDP:APP:033
500105034		Type: INFO:NIDP:APP:034
500105035		Type: INFO:NIDP:APP:035
500105036		Type: INFO:NIDP:APP:036
500105037		Type: INFO:NIDP:APP:037
500105038		Type: INFO:NIDP:APP:038
500105039		Type: INFO:NIDP:APP:039
500105040		Type: INFO:NIDP:APP:040
500105041		Type: INFO:NIDP:APP:041
500105042		Type: INFO:NIDP:APP:042
500105043		Type: INFO:NIDP:APP:043
500105044		Type: INFO:NIDP:APP:044
500105045		Type: INFO:NIDP:APP:045

Event Code	Message	Remedy
500105046	The specified identity object was deleted because it was not used for a configurable time period.	Type: INFO:NIDP:APP:046 Scenario: Periodically, the IDP attempts to clean up (delete) identity objects that have not been used for a configurable period of time. If an old unused identity is found, an attempt will be made to delete it. When this delete succeeds, this message will be logged.
500106001		Type: INFO:NIDP:IDFF:001
500106002		Type: INFO:NIDP:IDFF:002
500106003		Type: INFO:NIDP:IDFF:003
500106004		Type: INFO:NIDP:IDFF:004
500106005		Type: INFO:NIDP:IDFF:005
500106006		Type: INFO:NIDP:IDFF:006
500106007		Type: INFO:NIDP:IDFF:007
500106008		Type: INFO:NIDP:IDFF:008
600102001	Verbose user authentication information.	Type: DEBUG:NIDP:WSF:001 Scenario: Adds verbose authentication data to the fact that the user associated with the attribute request was found in the internal databases of the web service provider. See Also: 500102001
600102002	Verbose user authentication information, attribute select string, and data.	Type: DEBUG:NIDP:WSF:002 Scenario: A Web Service request was made to query user attributes. One of the data locations specified for the service is the Liberty User Profile object. The data listed in this message was successfully read for the indicated user using the indicated XPath. See Also: 500102004
600102003	Read single-valued attribute from user authentication LDAP object.	Type: DEBUG:NIDP:WSF:003 Scenario: A Web Service request to query user attribute data was received. One of the data locations was LDAP. This message displays the value read from the indicated LDAP attribute for the indicated user.
600102004	Read multi-valued attribute from user authentication LDAP object.	Type: DEBUG:NIDP:WSF:004 Scenario: A Web Service request to query user attribute data was received. One of the data locations was LDAP. This message displays the value read from the indicated LDAP attribute for the indicated user.

Event Code	Message	Remedy
600102005	Verbose user authentication and attribute information.	Type: DEBUG:NIDP:WSF:005 Scenario: When a user authenticates, the authenticating entity can push user attributes to the NIDP as part of the response to the authentication. The NIDP remembers these attributes for the life of that user session. If one of the data locations specified for a Web Service is remote, then these attributes may be returned as part of a query. See Also: 500102006
600102006	Adds verbose user and attribute information to attributes read from a remote service whose description was obtained at authentication time.	Type: DEBUG:NIDP:WSF:006 Scenario: A request was made to query a user's attributes. One of the data locations for the Web Service was remote. So, a request was made to a remote service to read attributes. See Also: 500102007
600102007	Adds verbose user and attribute information to the final aggregated result of a web service query!	Type: DEBUG:NIDP:WSF:007 Scenario: A request was made to query a user's attributes. If multiple data locations are specified for the Web Service, then attributes may be read from multiple data locations and then aggregated into a composite data structure. See Also: 500102008
600102008	Adds verbose data to reading Credential Profile data from Novell Secret Store.	Type: DEBUG:NIDP:WSF:008 Scenario: A request was made to query data from a user's Credential Profile. The data was successfully read. See Also: 500102011
600102009	The user successfully logged into Novell Secret Store using SAML/SASL.	Type: DEBUG:NIDP:WSF:009 Scenario: To access secrets from Novell Secret Store, the user must authenticate to Novell Secret Store.
600102010	Adds verbose data to reading Credential Profile data from an extended user authentication object attribute.	Type: DEBUG:NIDP:WSF:010 Scenario: A request was made to query data from a user's Credential Profile. The data was read from an extended schema attribute on the user's authenticated user object. See Also: 500102012
600105001	Do not need to proxy HTTP request to other cluster member. Well known URL that does not require the use of a proxy.	Type: DEBUG:NIDP:APP:001 Scenario: The request is one of a well known list of request types that may be processed on any cluster member, so it does not need to be forwarded to another cluster member.

Event Code	Message	Remedy
600105002	Do not need to proxy HTTP request to other cluster member. This cluster member can handle requests for this user.	Type: DEBUG:NIDP:APP:002 Scenario: The request arrived at the cluster member that owns the authentication information for the user. The request may have come straight from the router to this cluster member, or the request may have been forwarded here by another cluster member.
600105003	Obtained IP address of cluster member handling this users requests from URL parameter.	Type: DEBUG:NIDP:APP:003 Scenario: Each request must be processed on the cluster member that owns the user authentication information. The IP address of that cluster member was found in a URL parameter.
600105004	Obtained IP address of cluster member handling this users requests from HTTP cookie.	Type: DEBUG:NIDP:APP:004 Scenario: Each request must be processed on the cluster member that owns the user authentication information. The IP address of that cluster member was found in an HTTP cookie.
600105005	Obtained IP address of cluster member handling this user's requests by asking cluster members which one handles this user session.	Type: DEBUG:NIDP:APP:005 Scenario: Each request must be processed on the cluster member that owns the user authentication information. The IP address of that cluster member was found by asking all cluster members which one knew about the user's session.
600105006	Must proxy HTTP request to other cluster member.	Type: DEBUG:NIDP:APP:006 Scenario: Each request must be processed on the cluster member that owns the user authentication information. It has been determined that this cluster member is not the correct cluster member to process this request, so the request must be forwarded to another cluster member.
600105007	Response of proxy HTTP request.	Type: DEBUG:NIDP:APP:007 Scenario: Each request must be processed on the cluster member that owns the user authentication information. It was determined that this cluster member is not the correct cluster member to process this request, so the request was forwarded to another cluster member. The results of the request, as processed on the other cluster member, are displayed here.
600105008	Successfully obtained SOAP response document.	Type: DEBUG:NIDP:APP:008 Scenario: A SOAP request was made and a response was expected, the response was successfully obtained.
600105009		Type:DEBUG:NIDP:APP:009
600105010		Type: DEBUG:NIDP:APP:010
600105011		Type: DEBUG:NIDP:APP:011

4 Linux Access Gateway Appliance(045)

Component 045

Event Code	*Description*	**Remedy**
[1-9]04501000	Multi-homing	See the string value in the message for a description of the cause.
[1-9]04502000	Service manager	See the string value in the message for a description of the cause.
[1-9]04503000	Browser request processing	See the string value in the message for a description of the cause.
[1-9]04504000	Authentication processing	See the string value in the message for a description of the cause.
[1-9]04505000	Authorization processing	See the string value in the message for a description of the cause.
[1-9]04506000	Identity Injection processing	See the string value in the message for a description of the cause.
[1-9]04507000	Form Fill processing	See the string value in the message for a description of the cause.
[1-9]04508000	Caching	See the string value in the message for a description of the cause.
[1-9]04509000	Processing of Web server responses and of responses to browser requests	See the string value in the message for a description of the cause.
[1-9]04511000	Rewriter processing	See the string value in the message for a description of the cause.
[1-9]04512000	SOAP back channel processing	See the string value in the message for a description of the cause.
[1-9]04513000	Device communication channel (VCC)	See the string value in the message for a description of the cause.
[1-9]04514000	VM controller processing	See the string value in the message for a description of the cause.
[1-9]04515000	Connection management	See the string value in the message for a description of the cause.
[1-9]04516000	Core utilities (VXE)	See the string value in the message for a description of the cause.
[1-9]04517000	Data Stream processing	See the string value in the message for a description of the cause.

Event Code	*Description*	**Remedy**
[1-9]04518000	SSL processing	See the string value in the message for a description of the cause.
[1-9]04519000	Command processing	See the string value in the message for a description of the cause.
[1-9]04520000	Profiler	See the string value in the message for a description of the cause.
[1-9]04521000	Proxy start	See the string value in the message for a description of the cause.
[1-9]04522000	Audit event processing	See the string value in the message for a description of the cause.

5 Access Gateway Service (046)

Component 046

- Subgroup 00: URL Request Processing
- Subgroup 01: Authorization Processing
- Subgroup 02: Identity Injection Processing
- Subgroup 03: Form Fill Processing
- Subgroup 30: Web Server Communication Processing
- Subgroup 50: Administration Request Processing
- Subgroup 51: Statistics
- Subgroup 52: Health
- Subgroup 53: Alerts Processing
- Subgroup 54: Configuration Processing
- Subgroup 55: Initialization-Termination Processing

Event Code	Description	Remedy
URL Request Processing (00)		
304600404	Authentication Request: Unknown Contract	**Cause:** An unknown contract was received from the Embedded Service Provider. This can happen if the configuration of the Identity Server and Access Gateway are not synchronized. **Action:** Check to see if the Access Gateway or the Identity Server need to be updated. If their status is current, make a small change to both and update their configuration.
504600000	URL Accessed	A request for access to an unprotected URL has been received.
504600100	Protected Resource Accessed	A request for access to a protected URL has been received.
504600400	Authentication Request: Successful	The user authenticated successfully.
504600401	Login Request: Redirect To ESP	The authentication request was redirected to the Embedded Service Provider
504600402	Authentication Request: Set Cookie	The request has been redirected to set the cookie.
504600403	Authentication Request: Redirect URL with Cookie	The original URL request has been redirected to the Embedded Service Provider with a cookie.

Event Code	Description	Remedy
504600405	Authentication Request: NRL Request	The protected resource is configured for non-redirected login.
604600001	URL Accessed: Trace Summary	This event accesses the URL trace summary.
604600002	URL Accessed: Scheme Redirect	The URL accessed on wrong scheme is redirected.
604600003	URL Accessed: Pinned	The URL in the PIN list is accessed.
604600301	Session Broker: Cookie Not Found	The session broker returns the status of cokkie not found.
604600302	Session Broker: Add User	The session broker requests to add user.
604600303	Session Broker: Get Cookie	The session broker requests cookie.
604600304	Session Broker: Delete User	The session broker deletes user sent from SOAP request.
604600306	Session Broker: Update User	The session broker updates the user sent from SOAP request.
604600307	Session Broker: Cookie Found	The session broker returned requested cookie.
604600308	Session Broker: Add User SOAP Request	The session broker adds the user sent from SOAP request.
604600309	Session Broker: User Added	The session broker adds user request which are successfully processed.
604600310	Session Broker: Delete User Successful	The session broker deletes the user successfully.
604600311	Session Broker: Delete User Failed	The session broker failed to delete user.
Authorization Processing (01)		
204601102	Policy Configuration Reply: Policy Error	**Cause:** An error was detected while processing a policy configuration request. **Action:** Check the health of the configuration database. If it is unhealthy, repair it or restore it from a backup.
204601302	Policy Evaluation Reply: Policy Error	**Cause:** An error was detected while processing a policy evaluation request. **Action:** Verify that the Embedded Service Provider and the proxy service are running.
504601003	ACL Policy Configuration Request	ACL configuration request is being processed.
504601100	Policy Configuration Reply: Success	The Authorization policy has been configured successfully.
504601203	Policy Evaluation Request	A policy evaluation request has been received; the evaluation has started.
504601300	Policy Configuration Reply: Access allowed, no match	The Authorization policy evaluation results allowed access due to policy default action.

Event Code	Description	Remedy
504601301	Policy Configuration Reply: Access allowed	The Authorization policy evaluation results allowed access.
504601302	Policy Configuration Reply: Access denied	The Authorization policy evaluation results denied access.
Identity Injection Processing (02)		
204602102	Policy Configuration Reply: Policy Error	**Cause:** An error was detected while processing a policy configuration request. **Action:** Check the health of the configuration database. If it is unhealthy, repair it or restore it from a backup.
204602302	Policy Evaluation Reply: Policy Error	**Cause:** An error was detected while processing a policy evaluation request. **Action:** Verify that the Embedded Service Provider and the proxy service are running.
504602100	Policy Configuration Reply: Success	The Identity Injection policy has been configured successfully.
504602300	Policy Evaluation Reply: Inject Authentication Header	This policy injects an authentication header
504602301	Policy Evaluation Reply: Inject Custom Headers	This policy injects custom headers.
504602302	Policy Evaluation Reply: Inject Query Parameters	This policy injects query parameters.
Form Fill Processing (03)		
204603101	Policy Configuration Reply: No Policy ID	The policy ID is not included with policy configuration request.
204603102	Policy Configuration Reply: Policy Error	**Cause:** An error was detected while processing a policy configuration request. **Action:** Check the health of the configuration database. If it is unhealthy, repair it or restore it from a backup.
204603302	Policy Evaluation Reply: Policy Error	**Cause:** An error was detected while processing a policy evaluation request. **Action:** Verify that the Embedded Service Provider and the proxy service are running.
204603304	Policy Evaluation Reply: Parse Error: Unknown field	**Cause:** A parsing error was detected while processing a policy evaluation request. **Action:** Check the Form Fill policy and make sure it matches the form.
504603100	Policy Configuration Reply: Success	The Form Fill policy has been configured successfully.
504603300	Policy Evaluation Reply: Success	The Form Fill policy evaluation was successful.

Event Code	Description	Remedy
504603301	Policy Evaluation Reply: No Policy	The Form Fill policy was not found.
504603400	Get User Attributes	A request has been sent to get user attributes.
504603401	Set User Attributes	A request has been sent to set user attributes.
Administration Request Processing (50)		
204650002	DCC Message Processing	These events will processes the DCC messages.
504650002		
604650002		
704650002		
204650003	JCC	The information is related to sending and processing JCC requests.
204650005	Device Information Requests	These events will process the request of the device information.
504650005		
604650005		
704650005		
204650001	Command Processing	The Administration Console initiates the log events pertaining to processing commands.
504650001		
604650001		
704650001		
304650004	Service Information Requests	The service information requests are processed.
604650004		
504650010	Start	The log events pertaining to a Start command received from the Administration Console.
504650011	Stop	The log events pertaining to a Stop command received from the Administration Console.
504650012	Restart	The log events pertaining to a Restart command received from the Administration Console.
504650013	Refresh Policy	The log events pertaining to a Refresh Policy command received from the Administration Console.
504650014	Cache Clear	The log events pertaining to a Cache Clear command received from the Administration Console.
504650015	IP Scan	The log events pertaining to an IP Scan command received from the Administration Console.
Statistics (51)		

Event Code	Description	Remedy
204651001	Statistics Request Processing	The log events pertaining to the processing of a Statistics request from device manager.
304651001		
504651001		
604651001		
704651001		
504651000	Statistics	The log of current statistics requested by device manager.
Health (52)		
204652001	Health Request Processing	The log events pertaining to the processing of a health request from device manager.
304652001		
604652001		
704652001		
504652000	Health	The log of current health as requested by device manager.

6 SSL VPN Server (005)

Component 005

- Subgroup 01: Server
- Subgroup 02: Client. For a description of these event codes, see "Error Messages" in the *NetIQ Access Manager Appliance 4.0 SSL VPN User Guide*.

Event Code	*Description*	Remedy
	Server Event Codes	
20050101200	Error executing sockd	**Cause:** The /opt/novell/sslvpn/bin/sockd file may not be present, or not executable or corrupted **Action:** Check if the binary is present and has correct permissions. Installation may be a problem
20050101201	Error spawning stunnel	**Cause:** The `/opt/novell/sslvpn/bin/stunnel` file may not be present, or not executable or corrupted **Action:** Check if the binary is present and has correct permissions. Installation may be a problem
20050101202	Server stunnel conf file could not be opened	**Cause:** The `/etc/opt/novell/sslvpn/stunnel.conf` file may be corrupted or not present **Action:** Configuration may be bad. Check for other configuration errors in the logs
20050101203	Server sockd conf file could not be opened	**Cause:** The `/etc/opt/novell/sslvpn/sockd.conf` file may be corrupted or not present **Action:** Configuration may be bad. Check for other configuration errors in the logs
20050101204	Could not find core config file	**Cause:** The `/etc/opt/novell/sslvpn/config.xml` file is not present or corrupted **Action:** Restart the sslvpn service. Apply the changes from device manager and observe for any other errors while applying the changes on the device

Event Code	*Description*	**Remedy**
40050101205	Configuration file does not have proper contents. Parsing configuration failed. Connection Manager has bad configuration data. Could not add new connection	**Cause:** The `/etc/opt/novell/sslvpn/config.xml` file is not properly formatted. XML data corruption could have happened **Action:** Restart the sslvpn service. Apply the changes from device manager and observe for any other errors while applying the changes on the device
20050101206	Resource allocation failed	**Cause:** Might be a potential issue **Action:** Collect all error logs and report to Support
20050101207	Failed to send stunnel response “1231” to fd “5”	**Cause:** Stunnel program may have been stop or not running correctly **Action:** Collect error log reports Restart the sslvpn service
20050101208	Could not open the file “/opt/novell/sslvpn/connmansocket” exiting! Could not get File Lock for ConnMan. Another instance may be already running	**Cause:** The `/opt/novell/sslvpn/connmansocket` file may have been locked by another instance **Action:** Forcefully delete this file and restart sslvpn service
20050101209	Could not open the Unix domain socket	**Cause:** The `/opt/novell/sslvpn/connman` file may have been locked **Action:** Forcefully delete this file and restart sslvpn service
4005010120A	Could not bind the Local socket. TCP socket could not be opened	**Cause:** Invalid configuration or that particular port may be being used by another service **Action:** Check the service running on that port. Change the port in the configuration and restart sslvpn service
4005010120B	VCC has not been started. May be VCC port is invalid	**Cause:** The VCC port is either invalid or some other service is running on that port **Action:** Check `/etc/opt/novell/sslvpn/config.xml` file and verify the VCC port is valid. If it is not, change it to the correct value, delete the device from the Administration Console, then restart the JCC-proxy using the `/etc/init.d/novell-jcc restart` command.
2005010120C	Failed to parse Stunnel certificate. error code = XXXX	**Cause:** Stunnel Certificate is in bad format **Action:** Recreate the Stunnel certificate in device manager and apply changes to the device

Event Code	*Description*	**Remedy**
2005010120D	SOCKD is not running/registered... cannot add a new connection request. Failed to send disconnect notification to sockd. Failed to send the new connection notification to sockd. Failed to send servlet response to fd. Failed to send servlet init success response to fd, fd. Failed to send servlet response %x to fd %d msgType, fd. Failed to send socks response %x to fd %d msgType, fd	**Cause:** One of the programs of SSLVPN service is not running. And the SSLVPN Gateway is in bad state **Action:** Restart the sslvpn service and restart the novell-tomcat where sslvpn servlet is running
2005010120E	Restricting the number of policies for the role %s to %d .. because of insufficient buffer size, tmp->rolename, numRules Restricting the number of policies for the role	**Cause:** Too many number of traffic rules for that particular role **Action:** Revisit the configuration and reduce the number of traffic rules for that particular role
2005010120F	Error: Servlet is already registered. Servlet_connect_connection: Servlet is not registered. Received disconnect from servlet. But servlet is not registered	**Cause:** Communication channel between servlet and connection manager have gone bad **Action:** Restart the sslvpn service and restart the novell-tomcat where sslvpn servlet is running
30050101210	Cannot add new connection. Maximum number of connections reached	**Cause:** Maximum number of connections reached. No more connections can be added **Action:** Contact system administrator
50050101400	Failed to connect to connection Manager	**Cause:** Connection manager may not be running **Action:** Start the connection using the `sslvpnc -up` command.
20050101401	Error in sending message to Connection Manager	**Cause:** Connection Manager socket would have closed **Action:** Make sure connection Manager running
20050101402	Error in receiving message	**Cause:** May be connection socket would have closed **Action:** Make sure connection Manager running
20050101403	Failed to get the lock of the connection Manager socket. Service cannot be stopped	**Cause:** This happens with down command and If connmanSocket lock is not available **Action:** Retry
20050101404	Failed to update SSLVPN Server Configuration	**Cause:** This happens if the `config.xml` is not well formed **Action:** Make sure that `config.xml` is correct and well formed

Event Code	*Description*	**Remedy**
50050101405	Too many arguments	**Cause:** User entered the more arguments than the command can use. **Action:** Type `sslvpn -help`, read the command syntax, and use it.
50050101406	Too few arguments	**Cause:** User entered fewer arguments than the command requires. **Action:** Type `sslvpn -help`, read the command syntax, and use it.
50050101407	Invalid command	**Cause:** User entered the wrong command **Action:** Type `sslvpn -help`, read the command syntax, and use it.
30050101408	Failed to start SSL VPN service. Check log(/var/log/messages)	**Cause:** The `config.xml` file is probably invalid. **Action:** Check the `config.xml` file and correct it.
50050101409	Invalid argument	**Cause:** The user has entered invalid arguments. **Action:** Use the `sslvpnc -help` command to discover the valid arguments.

7 Policy Engine (008)

Component 008

- Subgroup 01: Engine
- Subgroup 02: Condition Handler
- Subgroup 03: Action Handler
- Subgroup 04: Configure Information Context
- Subgroup 05: Information Context
- Subgroup 06: Response Context

* = any Sub group

Event Code	*Description*	**Remedy**
100801001 100802001 100803001 100804001 100805001 100806001	Error No Memory: Memory allocation failed.	**Cause:** Low system memory. Resource allocation failed. **Action:** Determine cause for low system memory and resolve.
200801002 200802002 200803002 200804002 200805002 200806002	Error Bad Data: Policy configuration contains an invalid policy parameter list enumerative value.	**Cause:** The Administration Console has produced an invalid policy configuration document. **Cause:** Policy configuration document has been corrupted. **Action:** Take any or all of the following actions: 1. Submit the log file to Novell Support to aid in determining and fixing the source of the problem. 2. Back up to a previously working policy configuration until the problem has been fixed. 3. Examine the policy configuration document (available in PEP trace entries) to determine the erroneous policy document element and remove the corresponding policy statement from your policy configuration until a fix for the problem is available.

Event Code	*Description*	**Remedy**
200801003 200802003 200803003 200804003 200805003 200806003	Error Configuration. The policy configuration is syntactically incorrect or malformed.	**Cause:** The Administration Console has produced an invalid policy configuration document. **Cause:** Policy configuration document has been corrupted. **Action:** Take any or all of the following actions: 1. Submit the log file to Novell Support to aid in determining and fixing the source of the problem. 2. Back up to a previously working policy configuration until the problem has been fixed. 3. Examine the policy configuration document (available in PEP trace entries) to determine the erroneous policy document element and remove the corresponding policy statement from your policy configuration until a fix for the problem is available.
200801004 200802004 200803004 200804004 200805004 200806004	General Failure: Internal software error.	**Cause:** Unexpected exception caught during policy evaluation. **Action:** Submit log file to Novell Support for analysis and problem resolution.

Event Code	*Description*	**Remedy**
200801072 200802072 200803072 200804072 200805072 200806072	Interface Unavailable: Invalid InformationContext or ResponseContext enumerative value.	**Cause:** The Administration Console has produced an invalid policy configuration document. Invalid PolicyTypeSpec schema. **Cause:** Policy configuration document has been corrupted. **Action:** Take any or all of the following actions: 1. Submit the log file to Novell Support to aid in determining and fixing the source of the problem. 2. Back up to a previously working policy configuration until the problem has been fixed. 3. Examine the policy configuration document (available in PEP trace entries) to determine the erroneous policy document element and remove the corresponding policy statement from your policy configuration until a fix for the problem is available.
200801073 200802073 200803073 200804073 200805073 200806073	Data Unavailable: Policy Engine could not obtain needed information to complete policy evaluation.	**Cause:** Inaccessible user store or database. **Action:** Ensure user store or database is available. **Cause:** Network connectivity problems. **Action:** Ensure network is operational.
200801074 200802074 200803074 200804074 200805074 200806074	Illegal State: Policy Engine caught NullPtrException during policy configuration or evaluation.	**Cause:** Unexpected software exceptions. **Action:** Submit log to Novell Support for analysis and resolution.
200801075 200802075 200803075 200804075 200805075 200806075	Illegal Argument: Internal software error.	**Cause:** Invalid method argument received. **Action:** Submit log to Novell Support for analysis and resolution.

Event Code	*Description*	**Remedy**
300801071 300802071 300803071 300804071 300805071 300806071	Evaluation Canceled: Active policy evaluation canceled.	**Cause:** May occur during system shutdown. **Action:** If not caused by system shutdown, submit log to Novell Support for analysis and resolution.
500801000 500802000 500803000 500804000 500805000 500806000	Success: Policy operation completed without error.	**Cause:** Policy Evaluation. **Action:** No Action. Informational only.
500801005 500802005 500803005 500804005 500805005 500806005	Operation Pending: Policy operation is in progress	**Cause:** Policy Evaluation. **Action:** No Action. Informational only.
500803064	Permit Action: Policy evaluation rendered a Permit Action.	**Cause:** Permit action executed. **Action:** No Action. Informational only.
500803065	Deny Action: Policy evaluation rendered a Deny Action.	**Cause:** Deny action executed. **Action:** No Action. Informational only.
500803066	Obligation Action: Policy evaluation rendered an Obligation Action.	**Cause:** Obligation action executed. **Action:** No Action. Informational only.
500801067 500802067 500803067 500804067 500805067 500806067	No Action: Policy evaluation rendered no Action.	**Cause:** No action was executed during a policy evaluation. **Action:** No Action. Informational only.
500802068	Condition False: Policy condition returned FALSE.	**Cause:** Policy Evaluation. **Action:** No Action. Informational only.

Event Code	*Description*	**Remedy**
500802069	Condition True: Policy condition returned TRUE.	**Cause:** Policy Evaluation. **Action:** No Action. Informational only.
200802070	Condition Unknown. Policy configuration contains an unsupported condition handler definition.	**Cause:** The Administration Console has produced an invalid policy configuration document. **Cause:** Policy configuration document has been corrupted. **Action:** Take any or all of the following actions: 1. Submit the log file to Novell Support to aid in determining and fixing the source of the problem. 2. Back up to a previously working policy configuration until the problem has been fixed. 3. Examine the policy configuration document (available in PEP trace entries) to determine the erroneous policy document element and remove the corresponding policy statement from your policy configuration until a fix for the problem is available.

8 SOAP Policy Enforcement Point (011)

The SOAP Policy Enforcement Point (PEP) interface is used by the NetWare and Linux Access Gateways for policy evaluation.

Component 011

- Subgroup 01: General/Configuration
- Subgroup 02: Authorization PEP
- Subgroup 03: Identity Injection PEP
- Subgroup 04: Form Fill PEP

Messages are logged to the catalina.out for trace and application level logging when Identity Server logging is enabled.

Event Code	Description	Remedy
General/Configuration		
501101010	Start Policy Soap Handler	Policy Soap Message Handler received start command. **Cause:** Embedded Service Provider has been started **Action:** None. Informational message only.
501101011	Stop Policy Soap Handler	Policy Soap Message Handler received stop command. **Cause:** Embedded Service Provider has been stopped **Action:** None. Informational message only.
101101012	Policy Evaluator Not Running	The Policy Evaluator has been stopped. **Cause:** The Embedded Service Provider has been stopped by an administrator **Action:** Restart the Embedded Service Provider for the device.
101101013	General Failure	General failure processing policy request. **Cause:** Most often caused by incorrectly formatted XML. **Action:** Check catalina.out for stack trace and possibly more detailed information regarding the failure.

Event Code	Description	Remedy
501101020	Request Received	Soap request received. **Cause:** Informational message which logs the type of request received **Action:** None. Informational message used for checking soap handler interactions.
501101021	Response Sent	Soap response sent. **Cause:** Informational message regarding soap response to a request **Action:** None. Informational message used for checking soap handler interactions.
101101022	Unsupported request received	A NXPES command other than configure, evaluate or terminate was received. **Cause:** The policy engine revision is incompatible with the application. **Action:** Validate the software installation.
201101023	Unrecognized Policy Identifier	Policy evaluation was requested for an unknown policy. **Cause:** The policy identifier known to the Access Gateway is stale. **Action:** Most often, this problem is detected by the Access Gateway and the policies are reconfigured. If the problem persists, send an Apply or Apply Changes to the device from the CLI or Administrative Console.
501101030	Configure Success	Successful policy configuration. **Cause:** Policy configuration succeeded **Action:** None. Informational message used for checking policy configuration.
201101030	Configure Warning	Policy Configuration Warning. **Cause:** Policy configuration request reported a problem in retrieving configuration data from the config store **Action:** Check the policy definitions in the Administration Console to ensure the configuration store is working properly, then reapply the configuration to the device.

Event Code	Description	Remedy
101101031	Configure Failure	The policy requested is malformed or causes an exception during the configuration process. **Cause:** This is accompanied with a possible reason for the failure. **Action:** Check the policy configuration in the administrative console and reapply the configuration to the device.
501101032	Configure - Empty Policy Set	The set of policies requested either do not apply to the policy enforcement point or the set of policies do not match the categories selected in the policy enforcement list. **Cause:** This may be normal operation. **Action:** If a policy is expected, check the category of the policy and make sure the policy is enabled for the device.
501101040	Terminating policy	The set of policies represented by the policy ID are no longer needed and will be removed from the operating policy set. **Cause:** This happens each time a configuration is applied to the device. **Action:** None. This is an informational message only.
501101050	Evaluating policy	An evaluation request has been received for the set of policies represented by the policy ID. **Cause:** This happens at least once per user session per configured policy enforcement point. **Action:** None. This is an informational message only.

Event Code	Description	Remedy
501101051	Policy Evaluation - Invalid User Error	User session received for policy evaluation was not found or contains invalid data. **Cause:** The Identity Service Provider which authenticated the user is not accessible from the Embedded Service Provider. **Action:** Most often, this error will automatically restart the user identification process for the Access Gateway. If that doesn't occur: **Administrator:** If problem persists, check health status of Identity Service Provider and take appropriate action. **End User:** Retry request. If not redirected to the Identity Service Provider, force a refresh of the current browser page and the Access Gateway/Embedded Service Provider will reinitiate the authentication process.
501101052	Policy Evaluation - Information Query Error	The Policy Evaluator is unable to gain access to information required by the policy. **Cause:** This is accompanied with a possible reason for failure. **Action:** As the administrator, check the health status of Identity Service Provider and take appropriate action.
501101053	Policy Evaluation - WSC Query Error	An attempt to use the WSC query mechanism of the ESP failed, the requested policy data is unavailable. **Cause:** This is accompanied with a possible reason for failure. **Action:** As the administrator, check the health status of Identity Service Provider and take appropriate action.

Event Code	Description	Remedy
501101054	Policy Evaluation - Cluster Data Query Error	Attempt to retrieve user session data from ESP cluster member failed. **Cause:** The Embedded Service Provider which authenticated the user may not be accessible from the Embedded Service Provider evaluating the policy. **Action:** Most often, this error will automatically restart the user identification process for the Access Gateway. If that doesn't occur: **End User:** Close browser and retry request. **Administrator:** Check the health status of Embedded Service Provider referenced by IP address in the log and take appropriate action.
501101055	Policy Evaluation - Cluster Query Retry Count	Informational message containing the number of retries the ESP has made to request policy information from another cluster member. **Cause:** The Embedded Service Provider which authenticated the user may not be accessible from the Embedded Service Provider evaluating the policy. **Action:** None, this is an informational message only.
Authorization PEP		
501102050	Policy Evaluation Trace	Trace of an individual policy evaluation. **Cause:** Policy evaluation. **Action:** None. Informational message used for checking policy evaluation.
Identity Injection PEP		
501103050	Policy Evaluation Trace	Trace of an individual policy evaluation. **Cause:** Policy evaluation. **Action:** None. Informational message used for checking policy evaluation.
Form Fill PEP		
501104050	Policy Evaluation Trace	Trace of an individual policy evaluation. **Cause:** Policy evaluation. **Action:** None. Informational message used for checking policy evaluation.

9 Backup and Restore (010)

Backup and restore are invoked by script files:

- defbkparm.sh: Created by install. This has the default values for the scripts.
- getparams.sh: Prompts administrator for information needed to do the backup or restore operation.
- ambkup.sh: Script to run to perform a backup.
- amrestore.sh: Script to run to perform a restore.

Other programs used by backup and restore:

- ICE: This is the Novell eDirectory utility to import and export LDIF file in and out of eDirectory.
- ldifReverse: This is a program that reverses the order of the records in the LDIF file exported from eDirectory. Reversing the order of records allows the LDIF file to be imported without errors.
- certtool.jar: This is a eDirectory certificate utility that backs up and restores the CA key, server keys, and trusted roots to a zip file.

Component 010

- Subgroup 01: Backup
- Subgroup 02: Restore
- Subgroup 03: certtool (certificate backup and restore)

Messages are logged to the ambkup.log file.

Event Code	*Description*	**Remedy**
	Backup	
201001001	Backup failed to export data from the configuration store.	**Cause:** The ICE utility failed to export directory information to an LDIF file. **Action:** Make sure that ICE is in the proper location (Linux: `/opt/novell/eDirectory/bin`). **Action:** Make sure that the host IP address, port, administrator, password are all correct. **Action:** Make sure the back up file is writable

Event Code	*Description*	**Remedy**
201001002	Backup failed to format data for a successful restore.	**Cause:** The ldifReverse utility failed to sort the LDIF records. **Action:** Make sure that ldifReverse is in the proper location (Same directory as backup command). **Action:** Make sure the back up file is writable **Action:** Check for the backup file you specified with "_pre" appended to the file name. If the file exists, run the following command: `ldifReverse bkupfile_pre bkupfile` Replace `bkupfile` with the filename you specified for the backup file. It should create `bkupfile` which is the desired back up file.
201001003	Backup failed to export certificates to the backup zip file.	**Cause:** The certtool utility failed to export the certificates to a zip file. **Action:** Make sure that `certtool.jar` is in the proper location (Same directory as backup command). **Action:** Make sure the back up file is writable. **Action:** Manually export the certificates to a zip file: `java -Djava.library.path=/opt/novell/lib -jar certtool.jar -edirTree your_tree -edirIP 000.000.000.000 -edirServer cn=!ServerName.0=novell -edirUser cn=admin.o=novell -edirPwd secret -bkup -file ServerName _20060828_0930.zip -pwd certsecret -trcontainer trustedRoots.access ManagerContainer.novell -caName "your_tree CA"`
	Restore	
201002001	Backup file does not exist.	**Cause:** The backup file does not exist. The name of the backup file specified in answer to the prompt should not include the final the `.ldif` or `.zip` extension. **Action:** Specify the correct name of the back up file.
201002002	Backup file does not appear to be valid.	**Cause:** An simple analysis of the backup file indicates that the LDIF file specified backup file (with `.ldif` appended to the name) is not a valid backup file. **Action:** Make sure to specify a backup file that was created by the Access Manager Appliance Backup utility.
201002003	Restore failed to access the configuration store.	**Cause:** The ICE utility failed to access the eDirectory configuration store. **Action:** Make sure that ICE is in the proper location (Linux: `/opt/novell/eDirectory/bin`). Make sure that the host IP address, port, administrator, password are all correct.

Event Code	*Description*	**Remedy**
201002004	Restore failed to format the current configuration store data.	**Cause:** Restore was not able to save a current copy of the configuration store. A current copy of the config store is saved before the import in case the import fails. **Action:** Make sure that ldifReverse is in the proper location (Same directory as backup command).
201002005	Restore failed to prepare the configuration store for data import.	**Cause:** ICE failed. Unknown reason because it has previously been invoked successfully in the restore script.
201002006	Restore failed to prepare the configuration store for data import.	**Cause:** ICE failed. Unknown reason because it has previously been invoked successfully in the restore script.

101002007	Restore failed to restore the backup data.	**Cause:** ICE failed. Unknown reason because it has previously been invoked successfully in the restore script.
		
		Action: Check the configuration store for the following container:
		
		`ou=accessManagerContainer,o=novell`
		
		If it is not there, locate the `recover.ldif` file. It should be in the directory where you ran the restore command. Run ICE to recover the configuration store to the state it was in before you attempted the restore. Enter the following command:
		
		`/opt/novell/eDirectory/bin/ice -SLDIF -f recover.ldif -C -n -DLDAP -sxxx.xxx.xxx.xxx -p636 -k -dcn=admin, o=novell -wadmin_password -F`

101002008	Failed to restore certificate from backup file.	**Cause:** The java program restores the certificate failed. The java program is certtool.jar which provides command line access to various eDirectory certificate functions. **Action:** See the log file (`ambkup.log`) for more specific details. The log file contains a listing of relevant parameters with each error message. Assuming the back up from which you are trying to restore was successful, failure to restore is probably an incorrectly supplied parameter. Enter the following command: `JAVA -classpath vcdnbkup.jar:cert tool.jar com.novell.nids.bkuputil. Util -userid cn=admin,o=novell -pwd secret -vcdnUser`
101002009	Failed to reconfigure VCDN user objects.	**Cause:** The VCDN user objects were not restored with their passwords. Device Manager will not start up until the passwords have been properly set. **Action:** This is accompanied with an error x01004xxx. Please refer to that error.
	certtool utility	

Event Code	*Description*	**Remedy**
201003002	IP address is missing.	**Cause:** The certtool.jar was launched without the -edirIP option. A script file might have been incorrectly modified. **Action:** Make sure the -edirIP option is specified in the script when it launches the certtool utility.
201003005	eDirectory user id missing.	**Cause:** The certtool.jar was launched without the -eDirUser option. A script file might have been incorrectly modified. **Action:** Make sure the -edirUser cn=admin.o=novell option is specified in the script when it launches the certtool utility.
201003006	eDirectory user password missing.	**Cause:** The certtool.jar was launched without the -edirPwd option. A script file may have been incorrectly modified. **Action:** Make sure the -edirPwd option is specified in the script when it launches the certtool utility.
201003009	File name missing.	**Cause:** The certtool.jar was launched without the -file (name of backup file) option. A script file may have been incorrectly modified. **Action:** Make sure the -file option is specified in the script when it launches the certtool utility.
201003011	Encryption password missing.	**Cause:** The certtool.jar was launched without the -pwd option. A script file may have been incorrectly modified. **Action:** Make sure the -pwd option is specified in the script when it launches the certtool utility.
201003013	Name of trusted root container missing.	**Cause:** The certtool.jar was launched without the -trContainer (trusted root container) option. A script file may have been incorrectly modified. **Action:** Make sure the -trcontainer option is specified in the script when it launches the certtool utility.
201003040	Failed to open backup file for writing.	**Cause:** Backup was unable to create or access the backup file in which to save certificate information. **Action:** Ensure that user running backup sufficient rights.
201003041	Failed to retrieve certificate names from eDirectory.	**Cause:** A PKI or eDirectory error. **Action:** This error will be accompanied by an error string.
201003042	Failed to retrieve certificate xxxx from eDirectory.	**Cause:** The certtool failed to retrieve the certificate identified in the error. Problems have been seen trying to export certificate with pending CSRs. **Action:** This error will be accompanied by an error string.

Event Code	*Description*	**Remedy**
201003043	Failed to write certificate xxxx to backup file.	**Cause:** The certificate identified in the error message did not get saved to the backup file. **Action:** An exception string included in the message my provide additional information.
301003044	Error closing backup.	**Cause:** Likely will not cause a problem. **Action:** Try extracting the contents of the zip file created by backup to verify the integrity of the zip file.
201003045	Failed to write trusted root xxxx to backup file.	**Cause:** The trusted root identified in error messages did not get saved to the backup file. **Action:** An exception string included in the message might provide additional information.
201003046	Failed to retrieve trusted root xxxx from eDirectory.	**Cause:** The certtool failed to retrieve the trusted root identified in the error. Likely a PKI or eDirectory error. **Action:** This error will be accompanied by an error string.
201003048	Not all items were backed up.	**Cause:** See accompanying errors. **Action:** Refer to previous error messages to identify which certificates or trusted roots were not backed up.
201003049	Failed to retrieve the CA xxxx from eDirectory. Likely a PKI or eDirectory error.	**Cause:** The certtool failed to retrieve the CA key identified in the error. **Action:** This error will be accompanied by an error string.
201003050	Failed to write CA key xxxx to backup file.	**Cause:** The CA key identified in the error did not get written to the backup file. **Action:** An exception string included in the message my provide additional information.
201003051	Failed to open backup file for reading.	**Action:** Make sure the backup file exists. Do not include `.ldif` or `.zip` in the name of the back up file. **Action:** Make sure the user logged in has sufficient rights to access the file.
201003052	Not all items were restored.	**Cause:** See accompanying errors. **Action:** Refer to previous error messages to identify which certificates or trusted roots were not backed up.
301003053	Error closing backup.	**Action:** This error occurred after all restore operations had completed. Should not cause any problem.
201003056	Error importing CA key: xxxx	**Action:** The CA key was not restored. See the accompanying Error for more information. Likely a PKI error. **Action:** Make sure the password you provided matches the encryption password used when backing up the data.

Event Code	*Description*	**Remedy**
201003057	Error importing key: xxxx	**Cause:** The CA key was not restored. See the accompanying Error for more information. Likely a PKI error. **Action:** Make sure the password you provided matches the encryption password used when backing up the data.
201003058	Error importing trusted root: xxxx	**Cause:** The trusted root was not restored. See the accompanying Error for more information. Likely a PKI error.
	VCDN configuration	
201004001	Failed to configure VCDN objects for data store access.	The VCDN user objects were not restored with their passwords. Device Manager will not start up until the passwords have been properly set. **Cause:** The vcdnbkup.jar utility failed to reset passwords for VCDN objects. This causes errors starting up device manager. **Action:** Make sure `/opt/volera/roma/conf/vcdn.conf` file is present and has the correct information. To fix enter the following command in the /opt/novell/devman/bin directory: `java -jar vcdnbkup.jar -userid cn=admin,o=novell -pwd admin_password -vcdnUser`
201004002	Application Error.	The VCDN user objects were not restored with their passwords. Device Manager will not start up until the passwords have been properly set. Accompanied by a stack trace with more information. **Cause:** vcdnbkup.jar utility failed to reset passwords for VCDN objects. This will cause errors starting up device manager. **Action:** Make sure the information in `/opt/volera/roma/conf/vcdn.conf` file is correct: Fix the file by running the following command (in /opt/novell/devman/bin): `java -jar vcdnbkup.jar -userid cn=admin,o=novell -pwd admin_password -vcdnUser`

10 Novell Modular Authentication Class (012)

The Novell Modular Authentication Service (NMAS) Class provides access to a number of advanced authentication mechanisms available from Novell, Inc. and Novell partners.

Component 012

- Subgroup 01: General/Configuration
- Log file: catalina.out for trace and application level logging as enabled by the log settings (click *Identity Server > Edit > Logging)*

Event Code	Description	Remedy
General/Configuration		
301201001	NMAS Authentication Class	The log message language resource file could not be located. **Cause:** The log message language resource file was not found **Action:** Verify installation.
101201002	NMAS Authentication Class	Error getting LDAP host address. **Cause:** System configuration. **Action:** Verify installation and availability of LDAP host server.
101201003	NMAS Authentication Class	The NMAS_LOGIN_SEQUENCE initialization property were not provided. **Cause:** The NMAS_LOGIN_SEQUENCE property was not defined for the authentication class. **Action:** Use the management interface to add the NMAS_LOGIN_SEQUENCE property to either the class or the method, and assign it the name of a valid NMAS login sequence.
101201004	NMAS Authentication Class	Unable to write to HTTPResponse **Cause:** Unknown **Action:** Check system status.

Event Code	Description	Remedy
501201005	NMAS Authentication Class	UserID not found. **Cause:** Invalid User ID. **Action:** Verify username
101201006	NMAS Authentication Class	Invalid NMAS Login state. **Cause:** Unknown **Action:** Check server status.
101201007	NMAS Authentication Class	NMAS Login Error. **Cause:** See NMAS Error codes. **Action:** Indicated by NMAS error code.