



# Administration Console Guide

Access 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

<b>About NetIQ Corporation</b>	<b>9</b>
<b>About This Book and the Library</b>	<b>11</b>
<b>1 Administration Console</b>	<b>13</b>
1.1 Security Considerations . . . . .	13
1.1.1 Securing the Administration Console . . . . .	13
1.1.2 Protecting the Configuration Store . . . . .	14
1.1.3 Enabling Auditing and Event Notification . . . . .	15
1.1.4 Configuring the SSL Communication . . . . .	15
1.2 Configuring the Administration Console . . . . .	16
1.2.1 Configuring the Default View . . . . .	16
1.2.2 Changing the Administration Console Session Timeout . . . . .	19
1.2.3 Changing the Password for the Administration Console . . . . .	19
1.2.4 Changing the Administration Password of the User Store in the Identity Server . . . . .	19
1.2.5 Understanding the Administration Console Conventions . . . . .	20
1.3 Multiple Administrators, Multiple Sessions . . . . .	20
1.3.1 Creating Multiple Admin Accounts . . . . .	21
1.4 Managing Policy View Administrators . . . . .	21
1.5 Managing Delegated Administrators . . . . .	22
1.5.1 Access Gateway Administrators . . . . .	23
1.5.2 Policy Container Administrators . . . . .	24
1.5.3 Identity Server Administrators . . . . .	25
1.5.4 SSL VPN Administrators . . . . .	25
1.5.5 Activating eDirectory Auditing for LDAP Events . . . . .	26
1.5.6 Creating Users . . . . .	27
1.6 Enabling Auditing . . . . .	28
1.6.1 Configuring Access Manager Appliance for Auditing . . . . .	28
1.6.2 Querying Data and Generating Reports in Novell Audit . . . . .	31
<b>2 Backing Up and Restoring</b>	<b>33</b>
2.1 How The Backup and Restore Process Works . . . . .	33
2.1.1 Default Parameters . . . . .	33
2.1.2 The Process . . . . .	33
2.2 Backing Up the Access Manager Appliance Configuration . . . . .	34
2.3 Restoring the Access Manager Appliance Configuration . . . . .	35
2.3.1 Restoring the Configuration on the Same Appliance for Which Backup Was Taken . . . . .	36
2.3.2 Restoring the Configuration on a Freshly Installed Appliance with Same IP Address and DNS Settings . . . . .	36
2.4 Running the Diagnostic Configuration Export Utility . . . . .	37
<b>3 Security and Certificate Management</b>	<b>39</b>
3.1 Understanding How Access Manager Appliance Uses Certificates . . . . .	39
3.1.1 Process Flow . . . . .	40
3.2 Creating Certificates . . . . .	41
3.2.1 Creating a Locally Signed Certificate . . . . .	42
3.2.2 Editing the Subject Name . . . . .	45
3.2.3 Assigning Alternate Subject Names . . . . .	48
3.2.4 Generating a Certificate Signing Request . . . . .	48

3.2.5	Importing a Signed Certificate . . . . .	49
3.3	Managing Certificates and Keystores . . . . .	50
3.3.1	Viewing Certificate Details . . . . .	50
3.3.2	Renewing a Certificate. . . . .	52
3.3.3	Exporting a Private/Public Key Pair . . . . .	54
3.3.4	Exporting a Public Certificate. . . . .	54
3.3.5	Importing a Private/Public Key Pair . . . . .	55
3.3.6	Reviewing the Command Status for Certificates . . . . .	55
3.4	Managing Trusted Roots . . . . .	57
3.4.1	Importing Public Key Certificates (Trusted Roots). . . . .	57
3.4.2	Auto-Importing Certificates from Servers. . . . .	57
3.4.3	Exporting the Public Certificate of a Trusted Root . . . . .	58
3.4.4	Viewing Trusted Root Details. . . . .	58
3.5	Viewing External Trusted Roots . . . . .	59
3.6	Security Considerations for Certificates . . . . .	60
3.7	Assigning Certificates to Access Manager Appliance . . . . .	60
<b>4</b>	<b>Monitoring Access Manager By Using Simple Network Management Protocol</b>	<b>61</b>
4.1	SNMP Architecture in Access Manager . . . . .	61
4.2	Features of Monitoring in Access Manager . . . . .	62
4.3	Using the Default MIB File with External SNMP Systems . . . . .	63
4.4	Querying For SNMP Attributes . . . . .	64
4.4.1	Querying Using the Namespace . . . . .	65
4.4.2	Querying Using the OID. . . . .	65
4.5	Installing and Enabling Monitoring for Access Manager Components. . . . .	65
4.5.1	Installing and Enabling Monitoring for Access Manager on Linux . . . . .	65
4.5.2	Installing and Enabling Monitoring for Access Manager on Windows . . . . .	66
<b>5</b>	<b>Access Manager Appliance Logging</b>	<b>69</b>
5.1	Understanding the Types of Logging . . . . .	69
5.1.1	Component Logging for Troubleshooting Configuration or Network Problems . . . . .	69
5.1.2	HTTP Transaction Logging for Proxy Services . . . . .	70
5.2	Downloading the Log Files. . . . .	70
5.2.1	Administration Console Logs . . . . .	71
5.2.2	Identity Server Logs. . . . .	71
5.2.3	Access Gateway Logs . . . . .	72
5.2.4	SSL VPN Server Logs . . . . .	72
5.3	Using the Log Files for Troubleshooting. . . . .	73
5.3.1	Enabling Logging . . . . .	73
5.3.2	Understanding the Log Format . . . . .	73
5.3.3	Sample Authentication Traces . . . . .	76
<b>6</b>	<b>Changing the IP Address of an Access Manager Appliance</b>	<b>81</b>
<b>7</b>	<b>Code Promotion</b>	<b>83</b>
7.1	How Code Promotion Helps? . . . . .	83
7.2	Use Cases . . . . .	84
7.3	Code Promotion Mechanism . . . . .	84
7.4	Sequence of Promoting the Configuration Data . . . . .	85
7.5	Prerequisites . . . . .	85
7.6	Limitations . . . . .	86
7.7	Exporting the Configuration Data by Using Code Promotion . . . . .	86
7.8	Importing the Configuration Data by Using Code Promotion . . . . .	88

7.8.1	Upload Configuration File to Import . . . . .	88
7.8.2	Configuring Identity Server Clusters to Import. . . . .	89
7.8.3	Post-Import Configuration Tasks . . . . .	89
7.9	Exporting the Access Gateway Configuration Data . . . . .	90
7.10	Importing the Access Gateway Configuration Data . . . . .	90
7.11	Troubleshooting . . . . .	92

## 8 Troubleshooting the Administration Console 93

8.1	Global Troubleshooting Options. . . . .	93
8.1.1	Checking for Potential Configuration Problems . . . . .	94
8.1.2	Checking for Invalid Policies . . . . .	95
8.1.3	Checking for Version Conflicts . . . . .	96
8.1.4	Checking and Terminating User Sessions . . . . .	96
8.1.5	Checking for Invalid Policies . . . . .	96
8.1.6	Viewing Device Health . . . . .	96
8.1.7	Viewing Health by Using the Hardware IP Address. . . . .	97
8.1.8	Using the Dashboard . . . . .	97
8.1.9	Viewing System Alerts . . . . .	100
8.2	Logging . . . . .	100
8.3	Event Codes. . . . .	100
8.4	Restoring a Failed Secondary Console . . . . .	100
8.5	Converting a Secondary Access Manager Appliance into a Primary Appliance . . . . .	101
8.5.1	Shutting Down the Primary Access Manager Appliance . . . . .	101
8.5.2	Changing the Master Replica . . . . .	101
8.5.3	Restoring CA Certificates . . . . .	102
8.5.4	Verifying the vcdn.conf File . . . . .	103
8.5.5	Deleting Objects from the eDirectory Configuration Store . . . . .	103
8.5.6	Performing Component-Specific Procedures. . . . .	104
8.5.7	Enabling Backup on the New Primary Appliance . . . . .	106
8.6	Repairing the Configuration Datastore . . . . .	107
8.7	Session Conflicts . . . . .	107
8.8	Unable to Log In to the Administration Console . . . . .	107
8.9	Exception Processing IdentityService_ServerPage.JSP . . . . .	108
8.10	Backup and Restore Failure Because of Special Characters in Passwords . . . . .	108
8.11	Unable to Install NMAS SAML Method . . . . .	108
8.12	Incorrect Audit Configuration . . . . .	109
8.13	Unable to Update the Access gateway Listening IP Address in the Administration Console Reverse Proxy . . . . .	109
8.14	During Access Manager Appliance Installation Any Error Message Should Not Display Successful Status . . . . .	111
8.15	Incorrect Health Is Reported on the Access Gateway . . . . .	111
8.16	Administration Console Does Not Refresh the Command Status Automatically . . . . .	111
8.17	SSL Communication Fails . . . . .	112
8.18	Error: Tomcat did not stop in time. PID file was not removed. . . . .	112
8.19	An IP Address for the Other Known Device Manager List is Missing in the Troubleshooting Page. . . . .	112
8.20	View Objects Do Not Function Properly in Internet Explorer 10 Default Mode . . . . .	112

## 9 Troubleshooting Certificate Issues 113

9.1	Resolving Certificate Import Issues . . . . .	113
9.1.1	Importing an External Certificate Key Pair . . . . .	113
9.1.2	Resolving a -1226 PKI Error . . . . .	114
9.1.3	When the Full Certificate Chain Is Not Returned During an Automatic Import of the Trusted Root . . . . .	114

9.1.4	Using Internet Explorer to Add a Trusted Root Chain . . . . .	114
9.2	Mutual SSL with X.509 Produces Untrusted Chain Messages . . . . .	115
9.3	Certificate Command Failure . . . . .	115
9.4	A Device Reports Certificate Errors . . . . .	115
9.5	Issue while Adding the Access Gateway in a Cluster . . . . .	116
9.6	Renewing the expired eDirectory certificates . . . . .	116

## **A Certificates Terminology 117**

## **B Access Manager Audit Events and Data 119**

B.1	NIDS: Sent a Federate Request (002e0001) . . . . .	121
B.2	NIDS: Received a Federate Request (002e0002) . . . . .	122
B.3	NIDS: Sent a Defederate Request (002e0003) . . . . .	122
B.4	NIDS: Received a Defederate Request (002e0004) . . . . .	123
B.5	NIDS: Sent a Register Name Request (002e0005) . . . . .	123
B.6	NIDS: Received a Register Name Request (002e0006) . . . . .	124
B.7	NIDS: Logged Out an Authentication that Was Provided to a Remote Consumer (002e0007) . . . . .	124
B.8	NIDS: Logged out a Local Authentication (002e0008) . . . . .	125
B.9	NIDS: Provided an Authentication to a Remote Consumer (002e0009) . . . . .	125
B.10	NIDS: User Session Was Authenticated (002e000a) . . . . .	126
B.11	NIDS: Failed to Provide an Authentication to a Remote Consumer (002e000b) . . . . .	126
B.12	NIDS: User Session Authentication Failed (002e000c) . . . . .	127
B.13	NIDS: Received an Attribute Query Request (002e000d) . . . . .	128
B.14	NIDS: User Account Provisioned (002e000e) . . . . .	128
B.15	NIDS: Failed to Provision a User Account (002e000f) . . . . .	129
B.16	NIDS: Web Service Query (002e0010) . . . . .	129
B.17	NIDS: Web Service Modify (002e0011) . . . . .	130
B.18	NIDS: Connection to User Store Replica Lost (002e0012) . . . . .	131
B.19	NIDS: Connection to User Store Replica Reestablished (002e0013) . . . . .	131
B.20	NIDS: Server Started (002e0014) . . . . .	132
B.21	NIDS: Server Stopped (002e0015) . . . . .	132
B.22	NIDS: Server Refreshed (002e0016) . . . . .	133
B.23	NIDS: Intruder Lockout (002e0017) . . . . .	133
B.24	NIDS: Severe Component Log Entry (002e0018) . . . . .	134
B.25	NIDS: Warning Component Log Entry (002e0019) . . . . .	134
B.26	NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider as Identity Provider and Service Provider Are not in Same Group (002E001A) . . . . .	135
B.27	NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider Because a Policy Evaluated to Deny (002E001B) . . . . .	136
B.28	NIDS: Brokered an Authentication from Identity Provider to Service Provider (002E001C) . . . . .	136
B.29	NIDS: Roles PEP Configured (002e0300) . . . . .	137
B.30	Access Gateway: PEP Configured (002e0301) . . . . .	137
B.31	Roles Assignment Policy Evaluation (002e0320) . . . . .	138
B.32	Access Gateway: Authorization Policy Evaluation (002e0321) . . . . .	138
B.33	Access Gateway: Form Fill Policy Evaluation (002e0322) . . . . .	139
B.34	Access Gateway: Identity Injection Policy Evaluation (002e0323) . . . . .	139
B.35	Access Gateway: Access Denied (0x002e0505) . . . . .	140
B.36	Access Gateway: URL Not Found (0x002e0508) . . . . .	140
B.37	Access Gateway: System Started (0x002e0509) . . . . .	141
B.38	Access Gateway: System Shutdown (0x002e050a) . . . . .	142
B.39	Access Gateway: Identity Injection Parameters (0x002e050c) . . . . .	142
B.40	Access Gateway: Identity Injection Failed (0x002e050d) . . . . .	143

B.41	Access Gateway: Form Fill Authentication (0x002e050e) . . . . .	144
B.42	Access Gateway: Form Fill Authentication Failed (0x002e050f) . . . . .	144
B.43	Access Gateway: URL Accessed (0x002e0512) . . . . .	145
B.44	Access Gateway: IP Access Attempted (0x002e0513) . . . . .	146
B.45	Access Gateway: Webserver Down (0x002e0515) . . . . .	147
B.46	Access Gateway: All WebServers for a Service is Down (0x002e0516) . . . . .	147
B.47	Management Communication Channel: Health Change (0x002e0601) . . . . .	148
B.48	Management Communication Channel: Device Imported (0x002e0602) . . . . .	148
B.49	Management Communication Channel: Device Deleted (0x002e0603) . . . . .	149
B.50	Management Communication Channel: Device Configuration Changed (0x002e0604) . . . . .	150
B.51	Management Communication Channel: Device Alert (0x002e0605) . . . . .	150
B.52	SSL VPN: Common Logs (002e0701) . . . . .	151
B.53	SSL VPN: Extended Logs (002e0702) . . . . .	151
B.54	SSL VPN: Servlet Status (002e0706) . . . . .	152
B.55	SSL VPN: Servlet Connection Added (002e0707) . . . . .	152
B.56	SSL VPN: Servlet Connection Failed (002e0708) . . . . .	153
B.57	SSL VPN: Servlet Connection Removed (002e0709) . . . . .	153
B.58	SSL VPN: Cluster Node Status (002e070A) . . . . .	154
B.59	SSL VPN: Servlet New Session Created (002e070B) . . . . .	154
B.60	SSL VPN: Servlet Session Replicated (002e070C) . . . . .	155
B.61	SSL VPN: Servlet Session Removed (002e070D) . . . . .	155
B.62	SSL VPN: Servlet State Transfer Started (002e0710) . . . . .	156
B.63	SSL VPN: Servlet State Transfer Completed (002e0711) . . . . .	156
B.64	SSL VPN: Servlet Cluster Node Is Down (002e0712) . . . . .	157
B.65	SSL VPN: Servlet Cluster Node Is Restarted (002e0713) . . . . .	157
B.66	SSL VPN: Servlet Cluster Error with Reason (002e0714) . . . . .	158
B.67	SSL VPN: Servlet Service Provider Authenticated User (002e0715) . . . . .	158
B.68	SSL VPN: Servlet New Authenticated Connection Received (002e0716) . . . . .	159
B.69	SSL VPN: Servlet Service Provider Re-authenticated User (002e0717) . . . . .	159





---

# 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.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## 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](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto: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

This guide describes the following features of the Access Manager Appliance Administration Console that are not specific to an Access Manager device:

- ♦ [Chapter 1, “Administration Console,” on page 13](#)
- ♦ [Chapter 2, “Backing Up and Restoring,” on page 33](#)
- ♦ [Chapter 3, “Security and Certificate Management,” on page 39](#)
- ♦ [Chapter 4, “Monitoring Access Manager By Using Simple Network Management Protocol,” on page 61](#)
- ♦ [Chapter 5, “Access Manager Appliance Logging,” on page 69](#)
- ♦ [Chapter 6, “Changing the IP Address of an Access Manager Appliance,” on page 81](#)
- ♦ [Chapter 7, “Code Promotion,” on page 83](#)
- ♦ [Chapter 8, “Troubleshooting the Administration Console,” on page 93](#)
- ♦ [Chapter 9, “Troubleshooting Certificate Issues,” on page 113](#)
- ♦ [Appendix A, “Certificates Terminology,” on page 117](#)
- ♦ [Appendix B, “Access Manager Audit Events and Data,” on page 119](#)

## Intended Audience

This guide 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

Before proceeding, you should be familiar with the [NetIQ Access Manager Appliance 4.0 SP1 Installation Guide](#) and the [NetIQ Access Manager Appliance 4.0 SP1 Setup Guide](#), which provides information about setting up Access Manager Appliance.

For information about the other Access Manager devices and features, see the following:

- ♦ [NetIQ Access Manager 4.0 Quick Start](#)
- ♦ [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 SP1Event Codes\*](#)
- ♦ [\*NetIQ Access Manager Appliance 4.0 SSL VPN Server Guide\*](#)
- ♦ [\*NetIQ Access Manager Appliance 4.0 SSL VPN User Guide\*](#)

---

**NOTE:** Contact [namsdk@netiq.com](mailto:namsdk@netiq.com) for any query related to Access Manager SDK.

---

---

# 1 Administration Console

- ♦ [Section 1.1, “Security Considerations,” on page 13](#)
- ♦ [Section 1.2, “Configuring the Administration Console,” on page 16](#)
- ♦ [Section 1.3, “Multiple Administrators, Multiple Sessions,” on page 20](#)
- ♦ [Section 1.4, “Managing Policy View Administrators,” on page 21](#)
- ♦ [Section 1.5, “Managing Delegated Administrators,” on page 22](#)
- ♦ [Section 1.6, “Enabling Auditing,” on page 28](#)

For information about installing secondary consoles for fault tolerance, see [“Clustering and Fault Tolerance”](#) in the *NetIQ Access Manager Appliance 4.0 SP1 Setup Guide*.

For troubleshooting information about converting a secondary Access Manager Appliance into a primary Appliance, see [Section 8.5, “Converting a Secondary Access Manager Appliance into a Primary Appliance,” on page 101](#).

## 1.1 Security Considerations

The Administration Console contains all the configuration information for all Access Manager Appliance components. If you federate your users with other servers, it stores configuration information about these users. You need to protect the Administration Console so that unauthorized users cannot change configuration settings or gain access to the information in the configuration store. When you develop a security plan for Access Manager Appliance, consider the following:

- ♦ [Section 1.1.1, “Securing the Administration Console,” on page 13](#)
- ♦ [Section 1.1.2, “Protecting the Configuration Store,” on page 14](#)
- ♦ [Section 1.1.3, “Enabling Auditing and Event Notification,” on page 15](#)
- ♦ [Section 1.1.4, “Configuring the SSL Communication,” on page 15](#)

### 1.1.1 Securing the Administration Console

When you look for ways to secure the Administration Console from unauthorized access, consider the following:

**Admin User:** The admin user you create when you install the Administration Console has all rights to the Access Manager Appliance components. We recommend that you protect this account by configuring the following features:

- ♦ **Password Restrictions:** When the admin user is created, no password restrictions are set. To ensure that the password meets your minimum security requirements, you should configure the standard eDirectory password restrictions for this account. In the Administration Console, select the **Roles and Tasks** view in the iManager header, then click **Users**. Browse to the admin user (found in the novell container), then click **Restrictions**. For configuration help, use the **Help** button.

- ♦ **Intruder Detection:** The admin user is created in the novell container. You should set up an intruder detection policy for this container. In the Administration Console, select the **Roles and Tasks** view in the iManager header, then click **Directory Administration > Modify Object**. Select **novell**, then click **OK**. Click **Intruder Detection**. For configuration help, use the **Help** button.
- ♦ **Multiple Administrator Accounts:** Only one admin user is created when you install Access Manager Appliance. If something happens to the user who knows the name of this user and password or if the user forgets the password, you cannot access the Administration Console. Novell recommends that you create at least one backup user and make that user security equivalent to the admin user. For instructions, see [Section 1.3.1, “Creating Multiple Admin Accounts,” on page 21](#). For other considerations when you have multiple administrators, see [Section 1.3, “Multiple Administrators, Multiple Sessions,” on page 20](#).

**Network Configuration:** You need to protect the Administration Console from Internet attacks. It should be installed behind your firewall.

If you are installing the Administration Console on its own machine, ensure that the DNS names resolve between the Identity Server and the Administration Console. This ensures that SSL security functions correctly between the Identity Server and the configuration store in the Administration Console.

**Delegated Administrators:** If you create delegated administrators for policy containers (see [Section 1.5, “Managing Delegated Administrators,” on page 22](#)), be aware that they have sufficient rights to implement a cross-site scripting attack using the Deny Message in an Access Gateway Authorization policy.

They are also granted rights to the LDAP server, which gives them sufficient rights to access the configuration datastore with an LDAP browser. Modifications done with an LDAP browser are not logged by Access Manager. To enable the auditing of these events, see [“Activating eDirectory Auditing for LDAP Events” on page 26](#).

**Test Certificates:** When you install the Administration Console, the NAM-RP certificate is automatically generated and associated with NAM-RP Reverse Proxy (**Devices > Access Gateways > [AG-Cluster] > [NAM-RP]**).

## 1.1.2 Protecting the Configuration Store

The configuration store is an embedded, modified version of eDirectory. It is backed up and restored with command line options, which back up and restore the Access Manager Appliance configuration objects in the ou=accessManagerContainer.o=novell object.

You should back up the configuration store on a regular schedule, and the ZIP file created should be stored in a secure place. See [Section 2, “Backing Up and Restoring,” on page 33](#).

In addition to backing up the configuration store, you should also install at least two Administration Consoles (a primary and a secondary). If the primary console goes down, the secondary console can keep the communication channels open between the various components. You can install up to three Administration Consoles. For installation information, see [“Installing Secondary Versions of Access Manager Appliance” in the \*NetIQ Access Manager Appliance 4.0 SP1 Setup Guide\*](#).

The configuration store should not be used for a user store.

## 1.1.3 Enabling Auditing and Event Notification

For a secure system, you need to set up either auditing or syslogging to notify the system administrator when certain events occur. The most important audit events to monitor are the following:

- ♦ Configuration changes
- ♦ System shutdowns and startups
- ♦ Server imports and deletes
- ♦ Intruder lockout detection (available only for eDirectory user stores)
- ♦ User account provisioning

Audit events are device-specific. You can select events for the following devices:

- ♦ **Administration Console:** In the Administration Console, click **Auditing > Novell Auditing**.
- ♦ **Identity Server:** In the Administration Console, click **Devices > Identity Servers > Edit > Logging**.
- ♦ **Access Gateway:** In the Administration Console, click **Devices > Access Gateways > Edit > Novell Audit**.
- ♦ **SSL VPN:** In the Administration Console, click **Devices > SSL VPNs > Edit > Novell Audit Settings**.

You can configure Access Manager Appliance to send audit events to a Novell Audit Server, a Sentinel server, or a Sentinel Log Manager. For configuration information, see [Section 1.6, “Enabling Auditing,” on page 28](#).

In addition to the selectable events, device-generated alerts are automatically sent to the audit server. These Management Communication Channel events have an ID of 002e0605. All Access Manager events begin with 002e except for SSL VPN events, which start with 0031. You can set up Novell Auditing to send e-mail whenever these events or your selected audit events occur. See “[Configuring System Channels](http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al6t4sd.html)” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al6t4sd.html>) in the *Novell Audit 2.0 Guide* (<http://www.novell.com/documentation/novellaudit20/treetitl.html>).

For information about audit event IDs and field data, see [Appendix B, “Access Manager Audit Events and Data,” on page 119](#).

The Access Gateway also supports a syslog that allows you to send e-mail notification to system administrators. To configure this system in the Administration Console, click **Devices > Access Gateways > Edit > Alerts**.

## 1.1.4 Configuring the SSL Communication

By default, Access Manager Appliance supports the 128-bit SSL communication among the Administration Console, Identity Server, SSL VPN, and browsers. The supported ciphers include:

- ♦ SSL\_RSA\_WITH\_RC4\_128\_MD5
- ♦ TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- ♦ SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- ♦ SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- ♦ SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- ♦ TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_SHA

- ♦ TLS\_KRB5\_WITH\_RC4\_128\_SHA
- ♦ TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- ♦ SSL\_RSA\_WITH\_RC4\_128\_SHA
- ♦ TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

To enable the weak ciphers (not recommended):

- 1 Modify the `server.xml` file located in `/opt/novell/nam/adminconsole/conf/`.
- 2 Add name of the ciphers that you want to enable in the ciphers tag.

To enable the strong 256-bit ciphers:

- 1 Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 from Sun's Java website.
- 2 Extract the zip file and replace the policy jars in `/opt/novell/java/jre/lib/security/`.
- 3 Modify the `server.xml` file located in `/opt/novell/nam/adminconsole/conf/`.
- 4 Add the 256-bit ciphers to the cipher attribute of `<Connectors>`.

For example,

```
<Connector NIDP_Name="connector" port="2443" maxHttpHeaderSize="8192"
maxThreads="200" minSpareThreads="5" enableLookups="false"
disableUploadTimeout="true" acceptCount="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="tls" URIEncoding="UTF-8"
allowUnsafeLegacyRenegotiation="false" keystoreFile="/var/opt/novell/novlwww/
.keystore" keystorePass="changeit" SSLEnabled="true" address="164.99.87.129"
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA" />
```

For a complete list of supported cipher suites and their requirements, see “[The SunJSSE Provider](http://java.sun.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider)” (<http://java.sun.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider>).

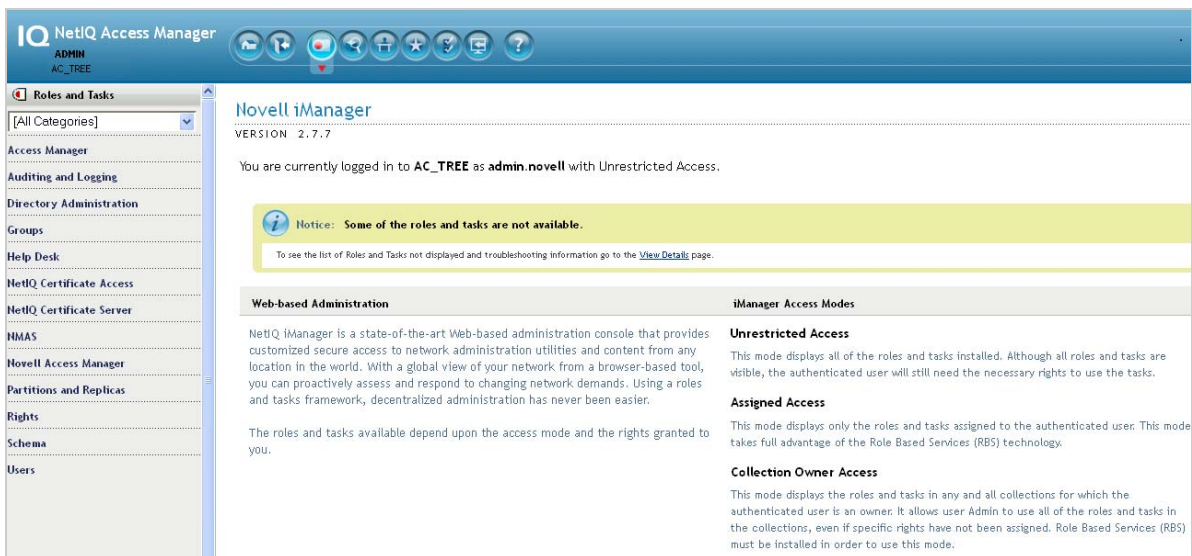
## 1.2 Configuring the Administration Console

- ♦ [Section 1.2.1, “Configuring the Default View,” on page 16](#)
- ♦ [Section 1.2.2, “Changing the Administration Console Session Timeout,” on page 19](#)
- ♦ [Section 1.2.3, “Changing the Password for the Administration Console,” on page 19](#)
- ♦ [Section 1.2.4, “Changing the Administration Password of the User Store in the Identity Server,” on page 19](#)
- ♦ [Section 1.2.5, “Understanding the Administration Console Conventions,” on page 20](#)

### 1.2.1 Configuring the Default View

Access Manager Appliance has two views in the Administration Console. Access Manager and its Support Packs used the **Roles and Tasks** view, with Access Manager Appliance the first listed task in the left hand navigation frame. It looks similar to the following:

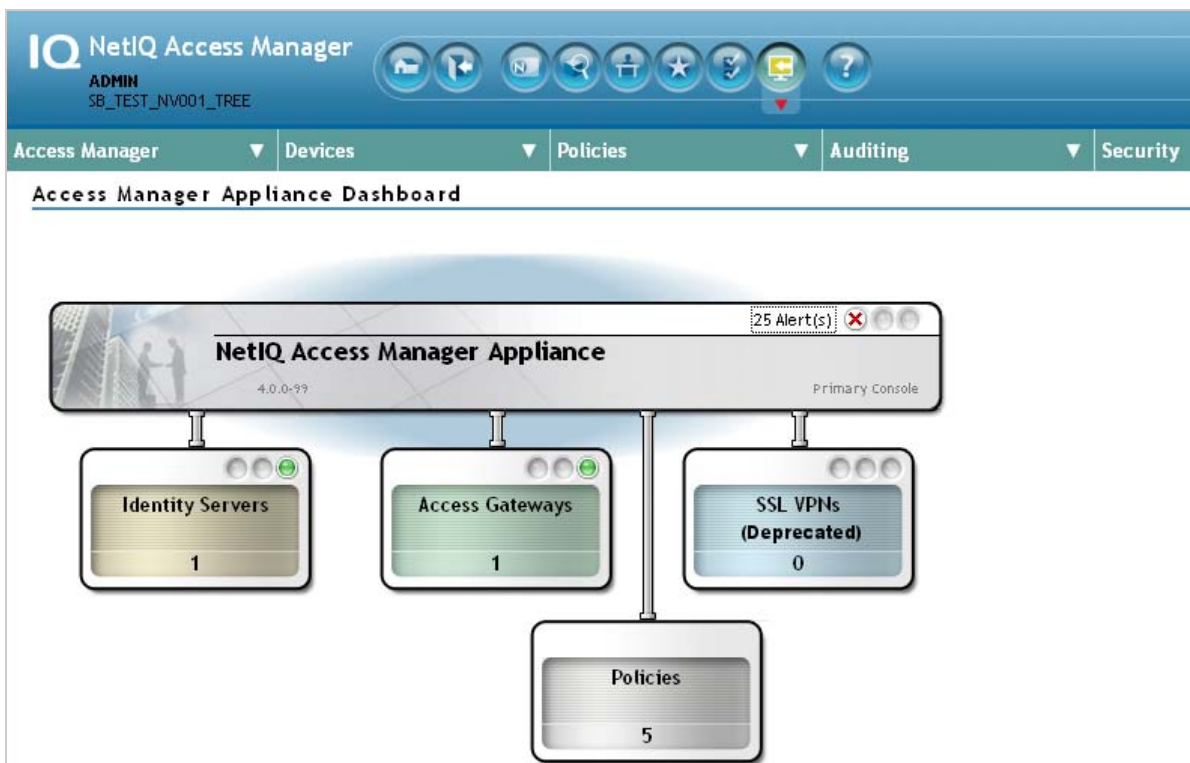




This view has the following advantages:

- ♦ Other tasks that you occasionally need to manage the configuration datastore are visible.
- ♦ If you are familiar with 3.2, you do not need to learn new ways to navigate to configure options.

Access Manager Appliance looks similar to the following:

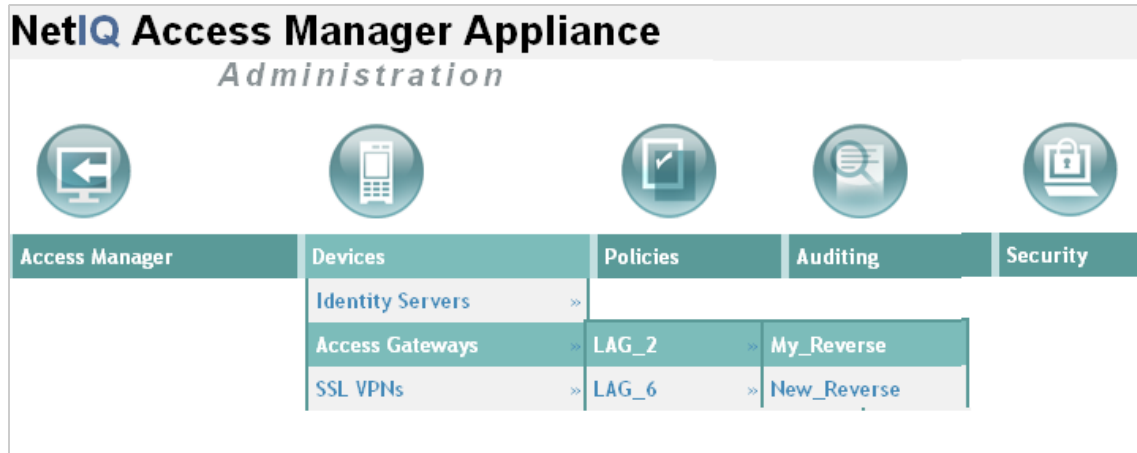


## NOTE

Starting from Access Manager 4.0 release, there will be no enhancements or platform updates for the SSL VPN component. The component is however available and fully supported in Access Manager 4.0. The Administrative Console Dashboard labels the component as "Deprecated" to convey this information. Deprecated means that SSL VPN will be removed from the subsequent version of Access Manager and you may consider other alternative solutions similar to SSL VPN.

This view has the following advantages:

- You can follow a path to a Identity Server cluster configuration or an Access Gateway proxy service with one click. The following image shows the path to the My\_Reverse proxy service of the LAG\_2 Access Gateway.



- It can remember where you have been. For example, if you are configuring the Access Gateway and need to check a setting for a Role policy, you can view that setting. If you click the **Devices** tab, the Administration Console remembers where you were in the Access Gateway configuration. If you click **Access Gateways**, it resets to that view.
- With the navigation moved to the top of the page, the wider configuration pages no longer require a scroll bar to see all of the options.
- Navigation is faster.

When you install or upgrade to Access Manager 3.1 or above and log in to the Administration Console, the default view is set to the Access Manager view.

## Changing the View

- 1 Locate the Header frame.



- 2 Click either the Roles and Tasks view  or the Access Manager view .

## Setting a Permanent Default View

- 1 In the iManager Header frame, click the Preferences view.
- 2 In the left navigation frame, click **Set Initial View**.
- 3 Select your preferred view, then click **OK**.

## 1.2.2 Changing the Administration Console Session Timeout

The `web.xml` file for Tomcat specifies how long an Administration Console session can remain inactive before the session times out and the administrator must authenticate again. The default value is 30 minutes.

To change this value:

- 1 Change to the Tomcat configuration directory:  
`/opt/novell/nam/adminconsole/conf/web.xml`
- 2 Open the `web.xml` file in a text editor and search for the `<session-timeout>` parameter.
- 3 Modify the value and save the file.
- 4 Restart the Administration Console:  
`/etc/init.d/novell-ac restart` OR `rcnovell-ac restart`

## 1.2.3 Changing the Password for the Administration Console

The admin of the Administration Console is a user created in the novell container of the configuration store. To change the password:

- 1 In the Administration Console, click **Users > Modify User**.
- 2 Click the **Object Selector** icon.
- 3 Browse the novell container and select the name of the admin user, then click **OK**.
- 4 Click **Restrictions > Set Password**.
- 5 Enter a password in the **New password** text box.
- 6 Confirm the password in the **Retype new password** text box.
- 7 Click **OK** twice.

## 1.2.4 Changing the Administration Password of the User Store in the Identity Server

Perform the following steps to change the admin password of a user store configured for the Identity Server:

- 1 In the Administration Console, click **Devices > Identity Servers > IDP-Cluster**.
- 2 Go to the **Local** tab and click the existing user store name in the user store's list.
- 3 Enter a password that matches the User Store password in the **Admin password** text box.
- 4 Confirm the password in the **Confirm password** text box.
- 5 Click **Apply**.

## 1.2.5 Understanding the Administration Console Conventions

- ♦ The required fields on a configuration page contain an asterisk by the field name.
- ♦ All actions such as delete, stop, and purge, require verification before they are executed.
- ♦ Changes are not applied to a server until you update the server.
- ♦ Sessions are monitored for activity. If your session becomes inactive, you are asked to log in again and unsaved changes are lost.
- ♦ Do not use the browser Back button. If you need to move back, use one of the following:
  - ♦ Click the **Cancel** button.
  - ♦ Click a link in the breadcrumb path that is displayed under the menu bar.
  - ♦ Use the menu bar to select a location.
- ♦ Right-clicking links in the interface, then selecting to open the link in a new tab or window is not supported.
- ♦ If you are in the Roles and Task view and the left navigation panel is not present in the window or tab, close the session and start a new one.
- ♦ The Administration Console uses a modified version of iManager. The LDAP and PKI plug-ins are packaged with the Administration Console which are useful for troubleshooting LDAP issues and certificates.
- ♦ The Administration Console uses a modified version of iManager. You cannot use standard iManager features or plug-ins with the Access Manager version of the product.
- ♦ If you access the Administration Console as a protected Access Gateway resource, you cannot configure it for single sign-on. The version of iManager used for the Administration Console is not compatible with either Identity Injection or Form Fill for single sign-on.

## 1.3 Multiple Administrators, Multiple Sessions

The Administration Console has been designed to warn you when another administrator is making changes to a policy container or to an Access Manager device (such as an Access Gateway or SSL VPN). The person who is currently editing the configuration is listed at the top of the page with an option to unlock and with the person's distinguished name and IP address. If you select to unlock, you destroy all changes the other administrator is currently working on.

---

**WARNING:** Currently, locking has not been implemented on the pages for modifying the Identity Server. If you have multiple administrators, they need to coordinate with each other so that only one administrator is modifying an Identity Server cluster at any given time.

---

**Multiple Sessions:** You should not start multiple sessions to the Administration Console with the same browser on a workstation. Browser sessions share settings that can result in problems when you apply changes to configuration settings. However, if you are using two different brands of browsers simultaneously, such as Internet Explorer and Firefox, it is possible to avoid the session conflicts.

**Multiple Administration Consoles:** As long as the primary console is running, all configuration changes should be made at the primary console. If you make changes at both a primary console and a secondary console, browser caching can cause you to create an invalid configuration.

The following sections explain how to create additional administrator accounts, how to delegate rights to administrators and how to manage policy view administrators:

- ♦ [Section 1.3.1, “Creating Multiple Admin Accounts,” on page 21](#)
- ♦ [Section 1.4, “Managing Policy View Administrators,” on page 21](#)
- ♦ [Section 1.5, “Managing Delegated Administrators,” on page 22](#)

## 1.3.1 Creating Multiple Admin Accounts

The Administration Console is installed with one admin user account. If you have multiple administrators, you might want to create a user account for each one so that log files reflect the modifications of each administrator. The easiest way to do this is to create a new user as a trustee of the tree root with [Entry Rights] for Supervisor and inheritable rights assignment. This also ensures that you have more than one user who has full access to the Administration Console. If you have only one administrator and something happens to the user who knows the name and password of admin account or if the user forgets the password, you cannot access the Administration Console.

To create a new user as a trustee of the tree root:

- 1 In the Administration Console, select the **Roles and Tasks** view in the iManager header.
- 2 Click **Users > Create User**.

Specify all the required details to create a valid user.

---

**NOTE:** Select the same **Context** that the existing administrator has.

---

- 3 Click **Rights > Modify Trustees**, then select the tree root user.
- 4 Add the newly created user as a trustee of the tree root user.
- 5 Click **Assigned Rights** and specify [Entry Rights] for supervisor and inheritable rights assignment.
- 6 Click **Done**.

You can also create delegated administrators and configure them to have rights to specific components of Access Manager. For configuration information for this type of user, see [Section 1.5, “Managing Delegated Administrators,” on page 22](#).

## 1.4 Managing Policy View Administrators

The super administrators can create a special type of delegated administrators called policy view administrators who can only view the policies in the policy container assigned to them. They policy view administrators can log in to Access Manager with their credentials and they are allowed to view only the policy containers assigned to them.

The policy view administrators are created same as creating users. For more information about creating users, see [Section 1.5.6, “Creating Users,” on page 27](#). In step 5b, select “ou=policyviewusers, o=novell” option in the Context field from the **Contents** list

After creating user, assign rights to the newly created user. For more information, see [Section 1.5.2, “Policy Container Administrators,” on page 24](#).

## 1.5 Managing Delegated Administrators

As the Access Manager admin user, you can create delegated administrators to manage the following Access Manager components.

- ♦ Individual Access Gateways or an Access Gateway cluster
- ♦ Identity Server clusters
- ♦ Individual SSL VPN servers or an SSL VPN cluster
- ♦ Policy containers

---

**IMPORTANT:** You need to trust the users you assign as delegated administrators. They are granted sufficient rights that they can compromise the security of the system. For example if you create delegated administrators with View/Modify rights to policy containers, they have sufficient rights to implement a cross-site scripting attack by using the Deny Message in an Access Gateway Authorization policy.

Delegated administrators are also granted rights to the LDAP server. They can access the configuration datastore with an LDAP browser. Any modifications made with the LDAP browser are not logged by Access Manager. To log LDAP events, you need to turn on eDirectory auditing. For configuration information, see [“Activating eDirectory Auditing for LDAP Events” on page 26](#).

---

By default, all users except the admin user are assigned no rights to the policy containers and the devices. The admin user has all rights and cannot be configured to have less than all rights. The admin user is the only user who has the rights to delegate rights to other users, and the only user with sufficient rights to modify keystores, create certificates, and import certificates.

The configuration pages for delegated administrators control access to the Access Manager pages. They do not control access to the tasks available for the **Roles and Tasks** view in iManager. If you want your delegated administrators to have rights to any of these tasks such as Directory Administration or Groups, you must use eDirectory methods to grant the user rights to these tasks or enable and configure Role-Based Services in iManager.

To create a delegated administrator, you must first create the user accounts, then assign them rights to the Access Manager components.

- 1 In the Administration Console, select the Roles and Tasks view from the iManager view bar.
- 2 (Optional) If you want to create a container for your delegated administrators, click **Directory Administration > Create Object**, then create a container for the administrators.
- 3 To create the users, click **Users > Create User** and create user accounts for your delegated administrators. You can create the users based on the `delegatedusers` or `policyviewusers` context. For more information about Creating Users, see [Section 1.5.6, “Creating Users,” on page 27](#).
- 4 Return to the Access Manager view, then click **Administrators** in the **Access Manager** menu.
- 5 Select the component you want to assign a user to manage.

For more information about the types of rights you might want to assign for each component, see the following:

- ♦ [“Access Gateway Administrators” on page 23](#)
- ♦ [“Policy Container Administrators” on page 24](#)
- ♦ [“Identity Server Administrators” on page 25](#)
- ♦ [“SSL VPN Administrators” on page 25](#)

- 6 To assign all delegated administrators the same rights to a component, configure **All Users** option by using the drop-down menu and selecting **None**, **View Only**, or **View/Modify**.  
By default, **All Users** is configured for **None**. **All Users** is a quick way to assign everyone View Only rights to a component when you want your delegated administrators to have the rights to view the configuration but not change it.
- 7 To select one or more users to assign rights, click **Add**, then fill in the following fields:  
**Name filter:** Specify a string that you want the user's cn attribute to match. The default value is an asterisk, which matches all cn values.  
**Search from context:** Specify the context you want used for the search. Click the down-arrow to select from a list of available contexts.  
**Include subcontainers:** Specifies whether subcontainers should be searched for users.
- 8 Click **Query**, and the **User** section is populated with the users that match the query.
- 9 In the **User** section, select one or more users to whom you want to grant the same rights.
- 10 For the **Access** option, click the down-arrow and select one of the following values:  
**View/Modify:** Grants full configuration rights to the device. View/Modify rights do not grant the rights to manage keystores, to create certificates, or to import certificates from other servers or certificate authorities. View/Modify rights allow the delegated administrator to perform actions such as stop, start, and update the device.  
If the assignment is to a policy container, this option grants the rights to create policies of any type and to modify any existing policies in the container  
**View Only:** Grants the rights to view all the configuration options of the device or all rules and conditions of the policies in a container.  
**None:** Prevents the user from seeing the device or the policy container.
- 11 In the **Device** or **Policy Containers** section, select the devices, the clusters, or policy containers that you want to assign for delegated administration.
- 12 Click **Apply**.  
The rights are immediately assigned to the selected users. If the user already had a rights assignment to the device or policy container, this new assignment overwrites any previous assignments.
- 13 After assigning a user rights, check the user's effective rights.  
A user's effective rights and assigned rights do not always match. For example, if Kim is granted View Only rights but All Users have been granted View/Modify rights, Kim's effective rights are View/Modify.

## 1.5.1 Access Gateway Administrators

You can assign a user to be a delegated administrator of an Access Gateway cluster or a single Access Gateway that does not belong to a cluster. You cannot assign a user to manage a single member of a cluster.

When a delegated administrator of an Access Gateway cluster is granted View/Modify rights, the administrator has sufficient rights to change the cluster configuration, to stop and start (or reboot and shut down), and to update the Access Gateways in the cluster. However, to configure the Access Gateway to use SSL, you need to be the admin user, rather than a delegated administrator.

When the user is assigned View/Modify rights to manage a cluster or an Access Gateway, the user is automatically granted View Only rights to the master policy container. If you have created other policy containers, these containers are hidden until you grant the delegated administrator rights to them.

View Only rights allows the delegated administrator to view the policies and assign them to protected resources. It does not allow them to modify the policies. If you want the delegated administrator to modify or create policies, you need to grant View/Modify rights to a policy container.

View/Modify rights to an Access Gateway or a cluster allows the delegated administrator to modify which Identity Server cluster the Access Gateway uses for authentication. It does not allow delegated administrators to update the Identity Server configuration, which is required whenever the Access Gateway is configured to trust an Identity Server. To update the Identity Server, the delegated administrator needs View/Modify rights to the Identity Server configuration.

## 1.5.2 Policy Container Administrators

The policy container administrators are of two types:

- ♦ Delegated Administrators
- ♦ Policy View Administrators

### *Delegated Administrators*

All delegated administrators with View/Modify rights to a device have read rights to the master policy container. To create or modify policies, a delegated administrator needs View/Modify rights to a policy container. When a delegated administrator has View/Modify rights to any policy container, the delegated administrator is also granted enough rights to allow the administrator to select shared secret values, attributes, LDAP groups, and LDAP OUs to policies.

If you want your delegated administrators to have full control over a device and its policies, you might want to create a separate policy container for each delegated administrator or for each device that is managed by a group of delegated administrators.

### *Policy View Administrators*

A policy view administrator has rights only to view policy containers. The super administrators can create a special type of delegated administrators called policy view administrators. The policy view administrators can login to Access Manager with their credentials and they are allowed to view only the policy containers assigned to them.

Using Policy Container option the super administrators can add and remove the delegated and policy view administrators.

- ♦ Adding Administrators
- ♦ Removing Administrators

## Adding Administrators

The administrator can assign the rights to the delegated administrators and the users based on the policy containers.

- 1 Log in to Access Manager.
- 2 Click **Roles and Tasks** menu.
- 3 Select **Access Manager > Administrators > Policy Containers > Add Administrators**.
- 4 (Optional) Enter the filter.
- 5 Select the **Access Rights** from the list for the type of administrator. For Example -View/Modify, View Only, and None. The policy view administrators have only **View Only** rights.



- 6 Select the search from context in the list. For example, "ou=delegated users, o=novell, ou=policyviewusers, o=novell". Based on the user selected, the delegated or policy view administrators are created.
- 7 (Optional) Select the **Include Subcontainers** check box, if you want to add it.
- 8 Click **Query**. The users and the policy containers are displayed for the selected query.
- 9 Select the **User** check box and **Policy Container** check box. The users and policy containers list are displayed based on the association with query.
- 10 Click **Apply**.
- 11 Click **Close**.

## Removing Administrators

To remove the administrators from the policy containers list, do the following:

- 1 Log in to Access Manager.
- 2 Click **Roles and Tasks** menu
- 3 Select **Access Manager > Administrators > Policy Containers > Remove Administrators**.
- 4 Select the check box of the user assigned to the administrator and click **Remove**. The selected user will be deleted from the Policy Containers Administrators list.
- 5 Click **Close**.

### 1.5.3 Identity Server Administrators

You cannot assign a delegated administrator to an individual Identity Server. You can only assign a delegated administrator to a cluster configuration, which gives the delegated administrator rights to all the cluster members.

When a delegated administrator of an Identity Server cluster is granted the View/Modify rights, the administrator has sufficient rights to change the cluster configuration and to stop, start, and update the Identity Servers in that cluster. The administrator is granted view rights to the keystores for each Identity Server in the cluster. To change any of the certificates, the administrator needs to be the admin user rather than a delegated administrator.

The delegated administrator of an Identity Server cluster is granted View Only rights to the master policy container. If you want the delegated administrator with View/Modify rights to have sufficient rights to manage policies, grant the following rights:

- ♦ To have sufficient rights to create Role policies, grant View/Modify rights to a policy container.
- ♦ To have sufficient rights to enable Role policies, grant View Only rights to the policy containers with Role policies.

### 1.5.4 SSL VPN Administrators

If the SSL VPN has an Embedded Service Provider and you grant the delegated administrator View/Modify rights to the SSL VPN or its cluster, the delegated administrator is granted sufficient rights to modify which Identity Server the SSL VPN or cluster uses for authentication. It does not allow them to

update the Identity Server configuration, which is required for this type of modification. To update the Identity Server, the delegated administrator needs View/Modify rights to the Identity Server configuration.

If the SSL VPN is a protected resource of an Access Gateway and you want the delegated administrator to have rights to the Access Gateway and the SSL VPN policy, you need to also grant the user View/Modify rights to the Access Gateway and the SSL VPN policy container.

When a delegated administrator of an SSL VPN is granted View/Modify rights, the administrator has sufficient rights to change the configuration, to stop and start the service, and to update the server's configuration.

To set up the secure tunnel certificate, the SSL VPN administrator also needs to be a certificate administrator with View/Modify rights.

## 1.5.5 Activating eDirectory Auditing for LDAP Events

If you are concerned that your delegated administrators might use an LDAP browser to access the configuration datastore, you can configure eDirectory to audit events that come from LDAP connections to the LDAP server.

- 1 In the Administration Console, click **Auditing > Auditing**.
- 2 Ensure that you have configured the IP address and port to use for your Secure Logging Server. The server can be a Novell Audit server, a Sentinel server, or a Sentinel Log Manager. For more information about this process, see [Section 1.6, "Enabling Auditing," on page 28](#).

---

**WARNING:** Whenever you change the port or address of the Secure Logging Server, all Access Gateways must be updated. Then every Access Manager device (Identity Server, Administration Console, Access Gateways and SSL VPN servers) must be rebooted (not just the module stopped and started) before the configuration change takes affect.

---

- 3 From the iManager view bar, select the Roles and Tasks view.
- 4 Click **Directory Administration > Modify Object**.
- 5 Click the **Object Selector** icon, expand the **novell** container, then select the eDirectory server. The eDirectory server uses the tree name, without the \_TREE suffix, for its name. The tree name is displayed in the iManager view bar.
- 6 Click **OK > Novell Audit > eDirectory**.
- 7 From the **Meta**, **Objects**, and **Attributes** sections, select the events that you want to monitor for potential security problems.
  - ♦ In the **Meta** section, you probably want to monitor changes made to groups and ACLs.
  - ♦ In the **Objects** section, you probably want to monitor who is logging in and out and if objects are being created or deleted.
  - ♦ In the **Attributes** section, you probably want to monitor when attribute values are added or deleted.
- 8 Click **Apply**.
- 9 Restart eDirectory and the Audit Server. Enter the following commands:

```
/etc/init.d/ndsd restart  
/etc/init.d/novell-naudit restart OR rcnovell-naudit restart
```

## 1.5.6 Creating Users

After creating users, you can assign the role of a delegated administrator or policy view administrator.

- 1 Log in to Access Manager.
- 2 Click **Roles and Tasks > Users > Create User**.
- 3 **User Name:** Specify the user name. This is a mandatory field.
- 4 **(Optional) First Name:** Specify the first name of the user.
- 5 **Last Name:** Specify the name of the delegated administrator user. This is a mandatory field..
- 6 **(Optional) Full Name:** Specify the full name of the user.
- 7 **Context:** Specify the context as delegated administrators. This is a mandatory field.
  - 7a Click object selector icon. The object selector browser displays the Browse and Search tabs.
  - 7b Click **Browse** tab. Select delegated users option from the **Contents** list. The delegatedusers.novell or policyviewusers.novell is displayed in the context field based on the selection.
- 8 **Password:** Specify the password and retype the password to confirm it.

---

**NOTE:** Failure to enter a password will allow the user to login without a password.

---

- 9 **(Optional) Simple Password:** Select this check box to set the simple password.

---

**NOTE:** Simple Password is not required for normal eDirectory access. The Universal Password feature supersedes Simple Password. When the Universal Password feature is enabled, setting the Simple Password is not required. For more information about the Universal Password feature, refer to [Netware 6.5 Documentation \(http://www.novell.com/documentation/nw65/?page=/documentation/lg/nw65/universal\\_password/data/front.html\)](http://www.novell.com/documentation/nw65/?page=/documentation/lg/nw65/universal_password/data/front.html)

---

- 10 **(Optional) Copy from Template or User Object:** Copies the attributes from a user template that you've created.
- 11 **(Optional) Create Home Directory:** You can create a home directory for this new User object if you have sufficient eDirectory rights. To do this, specify the path where you want to create the user's home directory.
  - 11a **Volume:** Applies only to NCP-enabled volumes.
  - 11b **Path:** You must specify a valid, existing directory path. The last directory typed in the path is the one that is created; all other directories in the path must already exist. For example, if you specify the path corp/home/sclark, the directories corp and home must already exist. The directory sclark is the only directory created.
- 12 **(Optional) Enter or Select the title, location, department, telephone number, fax number, email address of the delegated user from the list.**
- 13 **(Optional) Enter the description if there are any to the user.** You are able to add, remove and edit the information as per the requirement.
- 14 Click **OK** to continue.
- 15 Click **Cancel** to exit.

After creating a user, assign rights to the newly created user. For more information, see [Section 1.5.2, "Policy Container Administrators,"](#) on page 24.

## 1.6 Enabling Auditing

Access Manager Appliance supports audit logging and file logging at the component level. Access Manager Appliance includes a licensed version of Novell Audit to provide compliance assurance logging and to maintain audit log entries that can be subsequently included in reports. In addition to selectable events, device-generated alerts are automatically sent to the audit server. Access Manager Appliance comes preconfigured to use the Novell Audit server. You can configure Access Manager Appliance to use an already existing Novell Audit server, a Sentinel server, or a Sentinel Log Manager server.

The audit logs record events that have occurred in the identity and access management system and are primarily intended for auditing and compliance purposes. You can configure the following types of events for logging:

- ♦ Starting, stopping, and configuring a component
- ♦ Success or failure of user authentication
- ♦ Role assignment
- ♦ Allowed or denied access to a protected resource
- ♦ Error events
- ♦ Denial of service attacks
- ♦ Security violations and other events necessary for verifying the correct and expected operation of the identity and access management system.

Audit logging does not track the operational processing of the Access Manager Appliance components; that is, the processing and interactions between the Access Manager Appliance components required to fulfill a user request. (For this type of logging, see “[Configuring Component Logging](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.) The audit logs record the results of user and administrator requests and other system events. Although the primary purpose for audit logging is for auditing and compliance, the types of events logged can also be useful for detecting abnormal and error conditions and can be used as a first alert mechanism for system support. You can configure the audit log entries to generate alerts by leveraging the Novell Audit Notification feature. You can select to generate e-mail, syslog, and SNMP notifications.

Access Manager Appliance has been assigned the Novell Audit server-alert event code 0x002E0605. The Novell Audit Platform Agent is responsible for packaging and forwarding the audit log entries to the configured audit server. If the audit server is not available, the Platform Agent caches log entries until the server is operational and can accept audit log data.

- ♦ [Section 1.6.1, “Configuring Access Manager Appliance for Auditing,” on page 28](#)
- ♦ [Section 1.6.2, “Querying Data and Generating Reports in Novell Audit,” on page 31](#)

### 1.6.1 Configuring Access Manager Appliance for Auditing

By default, Access Manager Appliance is preconfigured to use the Novell Audit server. If you install more than one instance of Access Manager Appliance for failover, Novell Audit is installed with each instance. However, if you already use Novell Audit, you can configure Access Manager Appliance to

use your audit server. You also need to register Access Manager Appliance with your audit servers by importing the `nids_en.lsc` and `sslvpn_en.lsc` files. If you have a Sentinel server or a Sentinel Log Manager server, you can configure Access Manager Appliance to send the events to them.

Access Manager Appliance allows you to specify only one audit server. You still have failover if the audit server goes down. The auditing clients on Access Manager Appliance go into caching mode when the audit server is not available. They save all events until the entries can be sent to the audit server.

This section includes the following topics:

- ♦ “[Specifying the Logging Server and Console Events](#)” on page 29
- ♦ “[Configuring the Platform Agent](#)” on page 30

## Specifying the Logging Server and Console Events

The Secure Logging Server manages the flow of information to and from the auditing system. It receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. It can also be configured to automatically reset critical system attributes according to a specified policy.

- 1 To specify the logging server, click **Auditing > Auditing**.
- 2 Fill in the following fields:

**Server Listening Address:** Specify the IP address or DNS name of the audit logging server you want to use. By default, the system uses the primary Administration Console IP address. If you want to use a different Secure Logging Server, specify that server here.

**Server Public NAT Address:** If your auditing server is in the private network, then you have to enter Public NAT IP Address of the auditing server using which devices can reach the auditing server.

To use a Sentinel server or a Sentinel Log Manager instead of Novell Audit, specify the IP address or DNS name of your Collector.

- ♦ For more information about Sentinel, see [Sentinel 6.1 \(http://www.novell.com/documentation/sentinel61/index.html\)](http://www.novell.com/documentation/sentinel61/index.html).
- ♦ For more information about Sentinel Log Manager, see [Sentinel Log Manager 1.0 \(http://www.novell.com/documentation/novelllogmanager10/\)](http://www.novell.com/documentation/novelllogmanager10/).

**Port:** Specify the port that the Platform Agents use to connect to the Secure Logging Server.

To use a Sentinel server or Sentinel Log Manager instead of Novell Audit, specify the port of your Collector.

---

**IMPORTANT:** Whenever you change the port or address of the Secure Logging Server, all Access Gateways must be updated, then every Access Manager device (Identity Server, Administration Console, Access Gateways, and SSL VPN servers) must be rebooted (not just stopping and starting the module) before the configuration change takes affect.

---

**Stop Service on Audit Server Failure:** Enable this option to stop the Apache services when the audit server is offline or not reachable and audit events could not be cached.

- 3 Under **Management Console Audit Events**, specify the system-wide events you want to audit:

**Select All:** Selects all of the audit events.

**Health Changes:** Generated whenever the health of a server changes.

**Server Imports:** Generated whenever a server is imported into the Administration Console.

**Server Deletes:** Generated whenever a server is deleted from the Administration Console.

**Configuration Changes:** Generated whenever you change a server configuration.

**4 Click OK.**

If you did not change the address or port of the Secure Logging Server, this completes the process. It might take up to fifteen minutes for the events you selected to start appearing in the audit files.

**5 (Conditional) If you have changed the port of the Secure Logging Server in step 2, complete the following steps:**

**5a** In the Administration Console, select the Roles and Tasks view.

**5b** Click **Auditing and logging > Logging Server Options > Object Selector > Logging Services** and select **Novell Audit Secure Logging Server**.

**5c** Click **OK**.

**5d** Go to **Configuration** in the **General** tab. Change the **Secure Logging Server Port** from 289 to the required port that the Platform Agents use to connect to the Secure Logging Server.

**5e** Click **OK**.

**6 Restart the Administration Console. Open a terminal window, then enter the command for your platform:**

```
/etc/init.d/novell-ac restart OR rcnovell-ac restart
```

**7 Restart every device imported into the Administration Console.**

The devices (Identity Server, Access Gateway, and SSL VPN) do not start reporting events until they have been restarted.

## Configuring the Platform Agent

The Platform Agents installed with Access Manager Appliance use an embedded certificate. Access Manager Appliance does not currently support the use of custom application certificates. For information about this Novell Audit feature, see “Authenticating Logging Applications” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/am8ewv2.html>) in the *Novell Audit Administration Guide* (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html>).

The Platform Agents that are installed on each Access Manager component can be configured by modifying the `logevent` file. For the location of this file and its parameters, see “Logevent” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al36zjk.html#alibmyw>) in the *Novell Audit Administration Guide* (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html>).

---

**IMPORTANT:** Do not use this file to modify the IP address of the Secure Audit Server. Use the Administration Console for this task (see “[Specifying the Logging Server and Console Events](#)” on [page 29](#)).

If you are using Sentinel, most of the parameters in this file should be set on the collector.

---

When the Platform Agent loses its connection to the audit server, it enters caching mode. The default size of the audit cache file is unlimited. This means that if the connection is broken for long and traffic is high, the cache file can become quite large. When the connection to the audit server is re-established, the Platform Agent becomes very busy while it tries to upload the cached events to the audit server and still process new events. When it comes out of caching mode, the Platform Agent appears unresponsive because it is so busy and because it holds application threads that are logging

new events for a long period of time. If it holds too many threads, the whole system can appear to be hung. You can minimize the effects of this scenario by configuring the following two parameters in the `logevent` file.

Parameter	Description
LogMaxCacheSize	Sets a limit to the amount of cache the Platform Agent can consume to log events when the audit server is unreachable. The default is unlimited.
LogCacheLimitAction	Specifies what the Platform Agent should do with incoming events when the maximum cache size limit is reached. You can select one of the following actions:  Delete the current cache file and start logging events in a new cache file.  Stop logging, which preserves all entries in cache and stops collecting new events.

When you set a finite cache file size, it limits the number of events that must be uploaded to the audit server when caching mode is terminated and keeps the Platform Agent responsive to new audit events that are registered. If you have many users and are logging many events, you might need to configure these parameters.

For more information about these parameters, see “Logevent” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al36zjk.html#alibmyw>) in the *Novell Audit Administration Guide* (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html>).

## 1.6.2 Querying Data and Generating Reports in Novell Audit

Queries let you create, run, edit, and delete queries and event verifications. You can create two kinds of queries in Access Manager Appliance: manual queries and saved queries. Manual queries are simple queries that are not saved; they only run one time. All verification queries are saved. Saved queries and verifications are listed in the Queries list and can be run again and again against different databases.

Access Manager Appliance uses queries to request information from MySQL and Oracle databases. All queries are defined in SQL. Although you must be familiar with the SQL language to create SQL query statements, this is the most powerful and flexible query method.

Novell Audit provides two tools to query events and generate reports: the Novell Audit iManager plug-in and Novell Audit Report (`LReport`).

The following sections provide more information about these tools:

- ♦ “The Novell Audit iManager Plug-In” on page 31
- ♦ “Novell Audit Report” on page 32

### The Novell Audit iManager Plug-In

The Novell Audit iManager plug-in is a Web-based JDBC application that enables you to query MySQL and Oracle databases. All queries are defined in SQL.

iManager includes several predefined queries and it includes a Query Builder to help you define basic query statements. Of course, you can also build your own SQL query statements.



For complete information about defining and running queries in iManager, see the following sections in the *Novell Audit 2.0 Administration Guide* (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html>).

- ♦ “Defining Your Query Databases in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#alost1z>)
- ♦ “Defining Queries in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#alpvc0a>)
- ♦ “Running Queries in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#alpv7ft>)
- ♦ “Verifying Event Authenticity in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#b34tzvi>)
- ♦ “Exporting Query Results in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#alqvrze>)
- ♦ “Printing Query Results in iManager” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpq2.html#alqvzva>)

## Novell Audit Report

Novell Audit Report is a Windows-based, ODBC-compliant application that can use SQL query statements or Crystal Decisions Reports to query Oracle and MySQL data stores (or any other database that has ODBC driver support). You can define your own SQL query statements or import existing query statements and reports. Query results are returned in simple data tables; rows represent individual records and columns represent fields within those records.

For complete information about defining and running queries in Novell Audit Report, see the following sections in the *Novell Audit 2.0 Administration Guide* (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html>).

- ♦ “Novell Audit Report Interface” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpgw.html#als9vcm>)
- ♦ “Defining Your Databases in Novell Audit Report” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpgw.html#als94w4>)
- ♦ “Verifying Event Authenticity in Novell Audit Report” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpgw.html#am9dbll>)
- ♦ “Working with Reports in Novell Audit Report” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpgw.html#alsn2fj>)
- ♦ “Working with Queries in Novell Audit Report” (<http://www.novell.com/documentation/novellaudit20/novellaudit20/data/alorpgw.html#alshpuw>)



---

# 2 Backing Up and Restoring

The backup and restore utilities are scripts that are run from the command line, and they allow you to back up and restore your Access Manager Appliance configuration. An additional script allows you to export your configuration so NetIQ Support can help diagnose possible configuration problems.

The following sections describe how to back up and restore your Access Manager Appliance configuration, how to export your configuration for NetIQ Support, and how to restore the configuration to the Identity Servers and Access Gateways:

- ♦ [Section 2.1, “How The Backup and Restore Process Works,” on page 33](#)
- ♦ [Section 2.2, “Backing Up the Access Manager Appliance Configuration,” on page 34](#)
- ♦ [Section 2.3, “Restoring the Access Manager Appliance Configuration,” on page 35](#)
- ♦ [Section 2.4, “Running the Diagnostic Configuration Export Utility,” on page 37](#)

## 2.1 How The Backup and Restore Process Works

- ♦ [Section 2.1.1, “Default Parameters,” on page 33](#)
- ♦ [Section 2.1.2, “The Process,” on page 33](#)

### 2.1.1 Default Parameters

All scripts call the `getparams.sh` script to request the parameters from the user. The `defbkparm.sh` script is created by the Access Manager installation. It contains the default parameters for different options required by the underlying backup and restore utilities. If the entries in this file are commented out, the user is prompted for additional parameters.

### 2.1.2 The Process

The backup script must be run on the primary Administration Console. It creates a ZIP file that contains all the certificates that the various devices are using and an encrypted LDIF file that contains the configuration parameters for all imported devices. This means that you do not need to back up the configuration of individual devices. By backing up the primary Administration Console, you back up the configuration of all Access Manager devices.

The backup script backs up the objects in the `ou=accessManagerContainer.o=novell` container. It does not back up the following:

- ♦ Admin user account and password
- ♦ Delegated administrator accounts, their passwords, or rights
- ♦ Policy View user accounts, their passwords, or rights
- ♦ Role Based Services (RBS) configuration
- ♦ Modified configuration files on the devices such as the `web.xml` file
- ♦ Local files installed on devices such as touch files or log files
- ♦ Custom login pages, custom error pages, or custom messages

You need to perform your own backup of custom or modified configuration files.

For information about how to perform a configuration backup, see [Section 2.2, “Backing Up the Access Manager Appliance Configuration,” on page 34](#).

The only time you need to restore a backup is when the Administration Console fails. If another device fails, you simply replace the hardware, reinstall the appliance using the same IP address as the failed appliance, and the device imports into the Administration Console and acquires the configuration of the failed appliance.

If the Administration Console fails, you need to restore the files you backed up. In this case, you replace the hardware and reinstall the Administration Console using the same DNS name and IP address as the failed console. You then use the restore utility to restore the certificates and the device configuration. The Administration Console notifies all the devices that it is online, and they resume communicating with it rather than a secondary console.

## 2.2 Backing Up the Access Manager Appliance Configuration

- 1 On the primary Administration Console, change to the utility directory.

```
/opt/novell/devman/bin
```

- 2 Run the following command:

```
./ambkup.sh
```

- 3 Specify the Access Manager administration password.
- 4 Re-specify the password for verification.
- 5 Specify a path for where you want the backup files stored. Press Enter to use the default location.

If the specified path does not exist, the backup script displays a message to confirm whether you want to create this location.

- 6 Specify a password for encrypting and decrypting private keys, then re-specify it for verification. You must use the same password for both backup and restore.
- 7 Press Enter.

---

**NOTE:** After running the backup script, check the logs to verify that no errors occurred while running the backup script. The log file location is displayed at the end of the script execution.

---

The backup script creates a ZIP file containing several files, including the certificate information. This file contains the following:

- ♦ The configurations store's CA key.
- ♦ The certificates contained in the configuration store.
- ♦ The trusted roots in the trustedRoots container of the accessManagerContainer object.
- ♦ An encrypted LDIF file, containing everything found in the OU=accessManagerContainer,O=novell container.
- ♦ A `server.xml` file containing the Tomcat configuration information for the Administration Console.
- ♦ A “delegatedusers\_list” file containing the details of delegated users.

- ♦ A “policyviewusers\_list” file containing the details of delegated users.
- ♦ A “backup\_info” file that contains the basic details of the system on which the backup is being taken.

The trusted roots are backed up in both the LDIF file and the ZIP file. They are added to the ZIP file so that the ZIP file has the complete certificate-related configuration.

---

**IMPORTANT:** The backup utility prompts you for a location to store the backup file. Select a location from where the backup file will not be deleted when you uninstall the product. The default location is `/root/nambkup`.

Name of the backup zip file stores some information. Do not change the name.

---

---

**NOTE:** Whenever the configuration store contains a Key Material Object (KMO) with a certificate signing request in pending state, the KMO will not be exported by using the `amdiagcfg` script and not be backed up by using the `ambkup` script.

---

---

**NOTE:** For security purposes, delegated users, policy view users, and users in the trusted and configuration stores are not backed up. You need to recreate them while restoring the configuration. You can find the common name and full name of these users during the restore process or in the files in the zip file.

---

## 2.3 Restoring the Access Manager Appliance Configuration

The restore script replaces the configuration records in the configuration database with the records in the backup of the configuration store. It should be used to restore configuration data for one of the following types of scenarios:

- ♦ An upgrade failed and you need to return to the configuration before the upgrade.
- ♦ You want to return to the backed up configuration because the current modified configuration does not meet your needs.

If the primary Administration Console machine has failed, you have lost both the configuration and the configuration database. To recover from this scenario, you need to do more than restore the configuration.

The restore script cannot be used to move the Administration Console to a different platform, even if the new machine is configured to use the same IP address and DNS name. The backup files contains path information that is specific to the operating system.

- ♦ [Section 2.3.1, “Restoring the Configuration on the Same Appliance for Which Backup Was Taken,” on page 36](#)
- ♦ [Section 2.3.2, “Restoring the Configuration on a Freshly Installed Appliance with Same IP Address and DNS Settings,” on page 36](#)

---

**NOTE:** Restore should be made on the same version that was used to take the backup.

---

## 2.3.1 Restoring the Configuration on the Same Appliance for Which Backup Was Taken

- 1 Ensure that the zip file created during the backup process is accessible.
- 2 Log in as `root`.
- 3 Change the current directory to the utility directory: `/opt/novell/devman/bin`
- 4 Run the following command:  

```
./amrestore.sh
```
- 5 Specify and re-specify the Access Manager administration password.
- 6 Specify the path where the backup file is available.
- 7 Specify the name of the backup file. Do not include the `.zip` extension.
- 8 Specify the private key encryption password, then press Enter.
- 9 Re-specify the private key encryption password, then press Enter.  
Wait for the restore process to complete.
- 10 (Conditional) If you have a secondary appliance installed, reboot the machines.
- 11 (Conditional) If any devices report certificate errors, you need to re-push the certificates.
  - 11a Click **Auditing > Troubleshooting > Certificates**.
  - 11b Select the store that is reporting errors, then click **Re-push Certificates**.  
You can select multiple stores at the same time.
  - 11c (Optional) To verify that the re-push of the certificates was successful, click **Security > Command Status**.

## 2.3.2 Restoring the Configuration on a Freshly Installed Appliance with Same IP Address and DNS Settings

In this scenario, apart from restoring the Administration Console configuration, you need to re-import the device settings too.

- 1 Ensure that the zip file created during the backup process is accessible.
- 2 Log in as `root`.
- 3 Change the current directory to the `/opt/novell/devman/bin` directory.
- 4 Run the following command:  

```
./amrestore.sh
```
- 5 Specify and re-specify the Access Manager administration password.
- 6 Specify the path where the backup file is available.
- 7 Specify the name of the backup file. Do not include the `.zip` extension.
- 8 Specify the private key encryption password, then press Enter.
- 9 Re-specify the private key encryption password, then press Enter.  
Wait for the restore process to complete.
- 10 Change the current directory to the utility directory:  

```
/opt/novell/devman/jcc
```
- 11 Run the following command:

- ```
conf/reimport_nidp.sh jcc
```
- 12 Follow the steps to re-import the jcc settings.  
Wait for jcc to start.
  - 13 Run the following command:  

```
conf/reimport_nidp.sh nidp
```
  - 14 Follow the steps to re-import the Identity Server settings.  
Wait for the Identity Server health to turn green. You can check this in the Administration Console Dashboard.
  - 15 Run the following command:  

```
conf/reimport_agm.sh agm
```
  - 16 Follow the steps to re-import the Access Gateway settings.  
Wait for the Access Gateway health to turn green. You can check this in the Administration Console Dashboard.
  - 17 Run the following command:  

```
conf/reimport_agm.sh sslvpn
```
  - 18 Follow the steps to re-import SSL VPN settings.  
Wait for the SSL VPN health to turn green. You can check this in the Administration Console Dashboard.
  - 19 (Conditional) If you have a secondary appliance installed, reboot the machines.
  - 20 (Conditional) If any devices report certificate errors, you need to re-push the certificates.
    - 20a Click **Auditing > Troubleshooting > Certificates**.
    - 20b Select the store that is reporting errors, then click **Re-push Certificates**.  
You can select multiple stores at the same time.
    - 20c (Optional) To verify that the re-push of the certificates was successful, click **Security > Command Status**.

## 2.4 Running the Diagnostic Configuration Export Utility

In the Administration Console, you can create a `.ldif` file that you can export for diagnostic purposes:

- 1 Log in as `root`.
- 2 **On Linux:** Change to the `/opt/novell/devman/bin` directory and run the following command:  

```
./amdiagcfg.sh
```

**On Windows:** Go to the `C:\Program Files (x86)\Novell\bin` directory and run the following command:  

```
./amdiagcfg.bat
```
- 3 Specify the Access Manager administrator's password.
- 4 Confirm the password.
- 5 Specify the path where you want to store the diagnostic file.
- 6 Specify a name for the diagnostic file. The system adds `.xml` automatically as file extension.
- 7 Press Enter.

The Diagnostic Configuration Export utility is almost identical to the backup utility because it also creates a LDIF file with an addition of an XML Dump file. Passwords from the final LDIF file are removed by a program called Strippasswd.

Strippasswd removes occurrences of passwords in the LDIF file and replaces them with empty strings. If you look at the LDIF file, you will see that password strings are blank. You might see occurrences within the file or text that looks similar to password="String". These are not instances of passwords, but rather definitions that describe passwords as string types.

The XML file or LDIF file (if required) can then be sent to NetIQ Support for help in diagnosing configuration problems.

---

# 3 Security and Certificate Management

- ♦ [Section 3.1, “Understanding How Access Manager Appliance Uses Certificates,” on page 39](#)
- ♦ [Section 3.2, “Creating Certificates,” on page 41](#)
- ♦ [Section 3.3, “Managing Certificates and Keystores,” on page 50](#)
- ♦ [Section 3.4, “Managing Trusted Roots,” on page 57](#)
- ♦ [Section 3.5, “Viewing External Trusted Roots,” on page 59](#)
- ♦ [Section 3.6, “Security Considerations for Certificates,” on page 60](#)
- ♦ [Section 3.7, “Assigning Certificates to Access Manager Appliance,” on page 60](#)

## 3.1 Understanding How Access Manager Appliance Uses Certificates

Access Manager Appliance allows you to manage centrally stored certificates used for digital signatures and data encryption. eDirectory resides on the Administration Console and is the main certificate store for all of the Access Manager Appliance components. If you use a Novell Certificate Server, you can create certificates there and import them into Access Manager Appliance.

By default, all Access Manager Appliance components (Identity Server, Access Gateway and SSL VPN) trust the local Access Manager Appliance certificate authority (CA). However, if the Identity Server is configured to use an SSL certificate signed externally, the trust store of the Embedded Service Provider for each component must be configured to trust this new CA.

Certificate management commands issued from a secondary Administration Console can work only if the primary console is also running properly. Other commands can work independently of the primary console.

You can create and distribute certificates to the following components:

- ♦ **Identity Server:** Uses certificates and trust stores to provide secure authentication to the Identity Server and enable encrypted content from the Identity Server portal via HTTPS. Certificates also provide secure communications between trusted Identity Servers and user stores.

Liberty and SAML 2.0 protocol messages that are exchanged between identity and service providers often need to be digitally signed. The Identity Server uses the signing certificate included with the metadata of a trusted provider to validate signed messages from the trusted provider. For protocol messages to be exchanged between providers through SSL, each provider must trust the CA of the other provider. You must import the public key of the CA used by the other provider.

The Identity Server also has a trust store for OCSP (Online Certificate Status Protocol) certificates, which is used to check the revocation status of a certificate.

- ♦ **Access Gateway:** Uses server certificates and trusted roots to protect Web servers, provide single sign-on, and enable the product's data confidentiality features, such as encryption. They are used for background communication with the Identity Server and policy engine and to establish trust between the Identity Server and the Access Gateway.
- ♦ **SSL VPN:** Uses server certificates and trusted roots to secure access to non-HTTP applications.

To ensure the validity of X.509 certificates, Access Manager Appliance supports both Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) methods of verification.

When X509 authentication is configured as the authentication contract, it works even after you revoke the certificate for the X509 mutual authentication. When you access the nidp login page from the client browser and select the revoked certificate, browser does not throw an error message telling that the certificate has been revoked. You can either issue a CRL or wait until the next CRL issuance date. The revoked certificates will work until the next CRL issuance date.

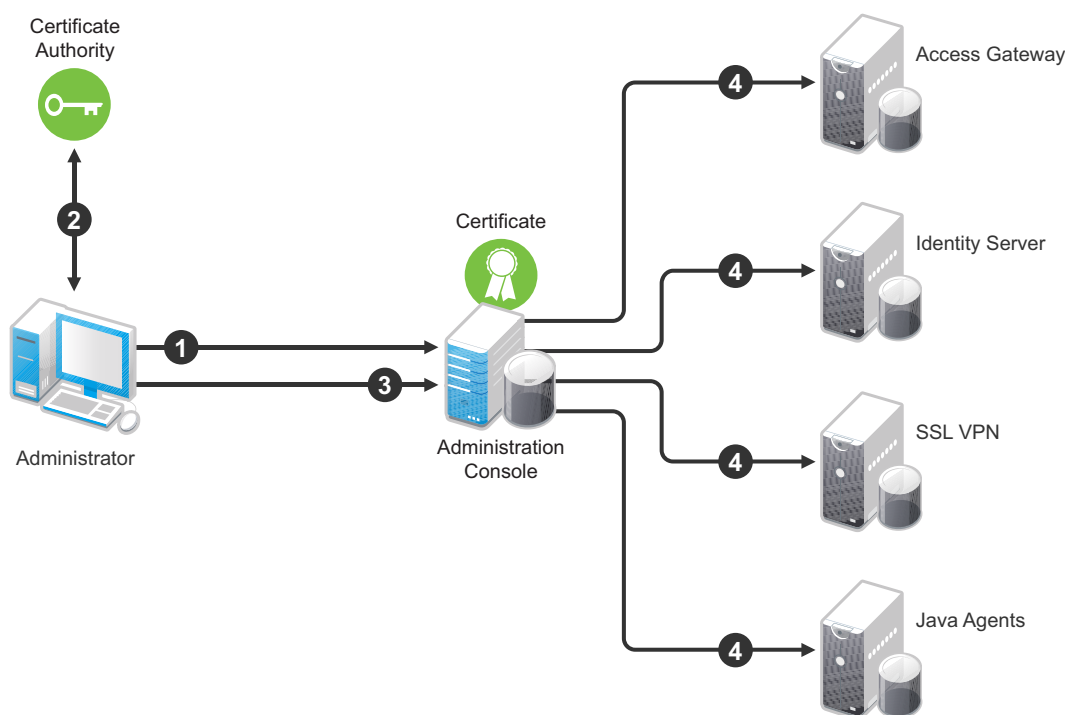
If you do not want to wait and issue a CRL now, perform the following steps:

- 1 Navigate to **Roles and Tasks > NetIQ Certificate Server > Configure Certificate Authority > CRL**.
- 2 Click **CRL**.
- 3 Under Next CRL Issuance, click **Issue Now**.
- 4 Click **OK**.
- 5 Restart the Identity Server.

### 3.1.1 Process Flow

You can install and distribute certificates to the Access Manager Appliance components and configure how the components use certificates. This includes central storage, distribution, and expired certificate renewal. [Figure 3-1](#) illustrates the primary administrative actions for certificate management in Access Manager Appliance:

**Figure 3-1** Certificate Management



1. Generate a certificate signing request (CSR). See [Section 3.2.4, "Generating a Certificate Signing Request,"](#) on page 48.
2. Send the CSR to the external certificate authority (CA) for signing.



A CA is a third-party or network authority that issues and manages security credentials and public keys for message encryption. The CA's certificate is held in the configuration store of the computers that trust the CA.

3. Import the signed certificate and CA chain into the configuration store. See [“Importing Public Key Certificates \(Trusted Roots\)” on page 57](#).
4. Assign certificates to devices. See [“Assigning Certificates to Access Manager Appliance” on page 60](#).

If you are unfamiliar with public key cryptography concepts, see [“Public Key Cryptography Basics”](#) (<http://www.novell.com/documentation/crt311/crtadmin/data/a2uqrry.html#a2uqrry>) in the *Novell Certificate Server 3.1.1 Guide* (<http://www.novell.com/documentation/crt33/crtadmin/data/a2ebomw.html>).

See [Appendix A, “Certificates Terminology,” on page 117](#) for information about certificate terminology.

## 3.2 Creating Certificates

Access Manager Appliance comes with certificates for testing purposes. At a minimum, you must create one SSL certificates for Identity Server and Access Gateway reverse proxy (NAM-RP). Then you replace the predefined certificates with the new ones.

If you install a secondary Administration Console, the certificate authority (CA) is installed with the first instance of eDirectory, and the secondary consoles have eDirectory replicas and therefore no CA software. All certificate management must be done from the primary Administration Console. Certificate management commands issued from a secondary Administration Console can work only if the primary console is also running properly. Other commands can work independently of the primary console.

---

**IMPORTANT:** Before generating any certificates with the Administration Console CA, ensure that time is synchronized within one minute among all of your Access Manager Appliance devices. If the time of the Administration Console is ahead of the device for which you are creating the certificate, the device rejects the certificate.

---

- 1 In the Administration Console, click **Security > Certificates**.

### Certificates

| Certificates                                                     |                          |                                 |               |              |       |  |
|------------------------------------------------------------------|--------------------------|---------------------------------|---------------|--------------|-------|--|
| Certificates Trusted Roots External Trusted Roots Command Status |                          |                                 |               |              |       |  |
| New..                                                            | Delete                   | Import Private/Public Keypair.. |               |              |       |  |
| <input type="checkbox"/> Name                                    | Subject                  | Used By                         | Starting Date | Ending Date  | State |  |
| <input type="checkbox"/> <a href="#">alice_client.crt</a>        | O=novell, CN=alice       |                                 | June 6, 2011  | June 6, 2013 |       |  |
| <input type="checkbox"/> <a href="#">NAM-RP-Certificate</a>      | CN=mova-sbdew.novell.com | 1 Reverse Proxy ▼               | June 4, 2011  | June 4, 2021 |       |  |

- 2 Select from the following actions:

**New:** To create a new certificate, click **New**. For information about the fields you need to fill in, see [Section 3.2.1, “Creating a Locally Signed Certificate,” on page 42](#) and [Section 3.2.4, “Generating a Certificate Signing Request,” on page 48](#).

**Delete:** To delete a certificate, select the certificate, then click **Delete**. If the certificate is assigned to a keystore, a warning message appears. You must remove a certificate from all keystores before it can be deleted.

**Import Private/Public Keypair:** To import a key pair, click **Import Private/Public Keypair**. For more information, see [Section 3.3.5, “Importing a Private/Public Key Pair,” on page 55](#).

### 3.2.1 Creating a Locally Signed Certificate

By default, the Access Manager Appliance installation process creates the local CA that can issue and sign certificates and installs a certificate server that generates certificates, keys, and CSRs (certificate signing requests) and imports certificates and keys.

- 1 In the Administration Console, click **Security > Certificates**.
- 2 Click **New**.

**New**

☒ Use local certificate authority  
Creates a certificate signed by the configuration store's CA.

☐ Use external certificate authority  
Generates a CSR (Certificate Signing Request) to be sent to an external CA for signing which must then be imported using Import Signed Certificate.

Certificate name:

Subject:

Signature algorithm: RSA with SHA1

Valid from: August 2, 2012 10:25:42 AM GMT

Months valid: 24

Key size: 1024

**Advanced options**

Key usage ☐ Critical (enforce key usage specified)

☒ Encrypt other keys

☒ Encrypt data directly

☒ Create digital signatures

☐ Non-repudiation

☐ This key is for a Certificate Authority

Basic Constraints ☐ Critical (enforce basic constraints specified)

☒ Unlimited

☐ Do not allow intermediate signing certificates in certificate chain

☐ Number of allowable intermediate signing certificates in signing chain. 1

Alternative name(s):  ☐ Critical (enforce alternate names specified)

OK Cancel

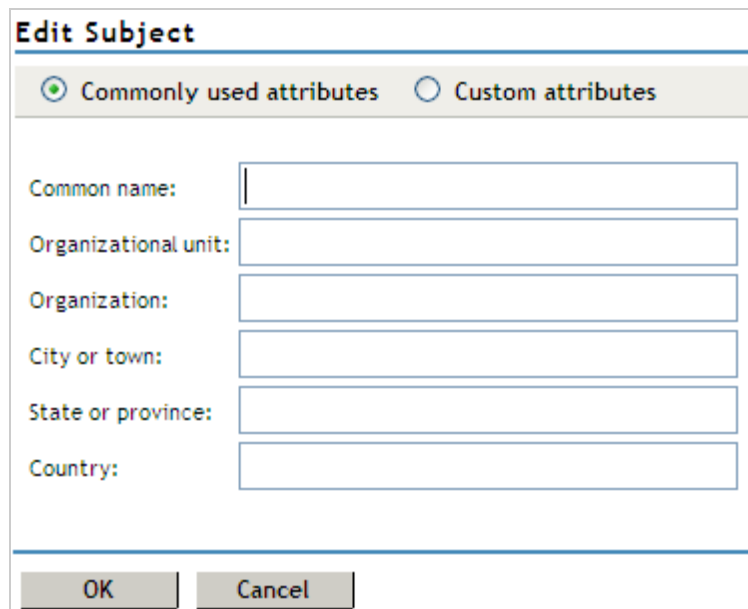
3 Select the following option:

**Use local certificate authority:** Creates a certificate signed by the local CA (or Organizational CA), and creates the private key. For information about creating a CSR, see [“Generating a Certificate Signing Request” on page 48](#).

4 Provide a certificate name:

**Certificate name:** The name of the certificate. Pick a unique, system-wide name for the certificate that you can easily associate with the certificate's purpose. The name must contain only alphanumeric characters and no spaces.

- 5 For **Subject**, click **Edit** to display a dialog box that lets you add the appropriate attributes for the subject name.

The image shows a dialog box titled "Edit Subject". At the top, there are two radio buttons: "Commonly used attributes" (which is selected) and "Custom attributes". Below this, there are six text input fields with labels: "Common name:", "Organizational unit:", "Organization:", "City or town:", "State or province:", and "Country:". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

The subject is an X.500 formatted distinguished name that identifies the entity that is bound to the public key in an X.509 certificate. Choose the subject name that the browser expects to find in the certificate. The name you enter must be fully distinguished. Completing all the fields creates a fully distinguished name that includes the appropriate types (such as C for country, ST for state, L for location, O for organization, OU for organizational unit, and CN for common name). For example, cn=AcmeWebServer.ou=Sales.o=Acme.c=US.

**Common name:** If you are creating a certificate for an Identity Server, specify the DNS name of the Identity Server. If you are creating a certificate for an Access Gateway, specify the published DNS name of the proxy service. Specifying values for the other attributes is optional.

For more information about the other attributes, see [Section 3.2.2, "Editing the Subject Name," on page 45](#).

- 6 Click **OK**, then fill in the following fields:

**Signature algorithm:** The algorithm you want to use (SHA-1, MD-2, or MD-5). SHA-1 is currently recommended.

---

**IMPORTANT:** You cannot create an SHA-2 algorithm in the Administration Console. But if you have an SHA-2 certificate created externally, you can import the certificate into Administration Console. For details, see [Section 3.2.5, "Importing a Signed Certificate," on page 49](#)

---

**Valid from:** The date from which the certificate is valid. For externally signed certificates, the external certificate authority sets the validity period.

**Months valid:** The number of months that the certificate is valid.

**Key size:** The size of the key. Select 512, 1024, 2048, or 4096.

- 7 (Optional) To configure advanced options, click **Advanced Options**.

- 8 Configure the following options as necessary for your organization:

**Critical:** Specifies that an application should reject the certificate if the application does not understand the key usage extensions.

**Encrypt other keys:** Specifies that the certificate is used to encrypt keys.

**Encrypt data directly:** Encrypts data for private transmission to the key pair owner. Only the intended receiver can read the data.

**Create digital signatures:** Specifies that the certificate is used to create digital signatures.

**Non-repudiation:** Links a digital signature to the signer and the data. This prevents others from duplicating the signature because no one else has the signer's private key. Additionally, the signer cannot deny having signed the data.

- 9 (Conditional) If you are creating a key for a certificate authority, configure the following options:

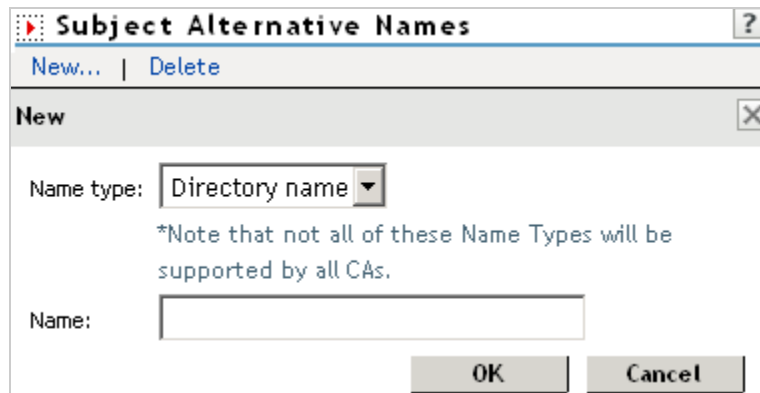
**This key is for a Certificate Authority:** Specifies that this certificate is for the local configuration (eDirectory) certificate authority.

If you create a new CA, all the keys signed by the CA being replaced no longer have a trusted CA. You might also need to reassign the new CA to all the trust stores that contained the old CA.

**Critical:** Enforces the basic constraints you specify. Select one of the following:

- ♦ **Unlimited:** Specifies no restriction on the number of subordinate certificates that the CA can verify.
- ♦ **Do not allow intermediate signing certificates in certificate chain:** Prevents the CA from creating other CAs, but it can create server or user certificates.
- ♦ **Number of allowable intermediate signing certificates in signing chain:** Specifies how many subordinate certificates are allowed in the certificate chain. Values must be 1 or more. Entering 0 creates only entity objects.

- 10 (Optional) To create subject alternative names used by the certificate, click **Edit Subject Alternate Names**, then click **New**.



Alternate names can represent the entity identified by the certificate. The certificate can identify the subject CN=www.OU=novell.O=com, but the subject can also be known by an IP address, such as 222.111.100.101, or a URI, such as www.novell.com, for example. For more information, see [Section 3.2.3, "Assigning Alternate Subject Names," on page 48](#).

- 11 Click **OK**.
- 12 (Conditional) If you assigned alternate names, determine how you want applications to handle the alternate names. Select **Critical** if you want an application that does not understand the alternate name extensions to reject the certificate.
- 13 Click **OK**.

## 3.2.2 Editing the Subject Name

- 1 Fill in one or more of the following attributes.

The following attributes are the most common ones used in certificate subjects:

**Common name:** The DNS name of the server.

Specify the value, for example AcmeWebServer.provo.com. Do not include the type (cn=). The UI adds that for you.

For the Identity Server, this is the domain name of the base URL of the Identity Server configuration. This value cannot be an IP address or begin with a number, in order to ensure that trust does not fail between providers.

For the Access Gateway, this is the published DNS name of the proxy service.

**Organizational unit:** Describes departments or divisions.

**Organization:** Differentiates between organizational divisions.

**City or town:** Commonly referred to as the Locality.

**State or province:** Commonly referred to as the State. Do not abbreviate the name.

**Country:** The country, such as US.

## 2 Use the drop-down menus to add additional attributes.

These values allow you to specify additional fields that are supported by eDirectory, and you can include them as part of the subject to further identify the entity represented by the certificate.

**CN:** The **Common name** attribute in the list of **Commonly used attributes** (OID: 2.5.4.3)

**C:** The **Country attribute** in the list of **Commonly used attributes** (OID: 2.5.4.6)

**SN:** The surname attribute (OID: 2.5.4.4)

**L:** The locality attribute, which is the **City or town** attribute in the list of **Commonly used attributes** (OID: 2.5.4.7)

**ST:** The **State or province** attribute in the list of **Commonly used attributes** (OID: 2.5.4.8)

**S:** The **State or province** attribute in the list of **Commonly used attributes** (OID: 2.5.4.8)

**O:** The Organization attribute in the list of Commonly used attributes (OID: 2.5.4.10)

**OU:** The Organizational unit attribute in the list of Commonly used attributes (OID: 2.5.4.11)

**street:** Describes the street address (OID: 2.5.4.9)

**serialNumber:** Specifies the serial number of a device (OID: 2.5.4.5)

**title:** Describes the position or function of an object (OID: 2.5.4.12)

**description:** Describes the associated object (OID: 2.5.4.13)

**searchGuide:** Specifies a search filter (OID: 2.5.4.14)

**businessCategory:** Describes the kind of business performed by an organization (OID: 2.5.4.15)

**postalAddress:** Specifies address information required for the physical delivery of postal messages (OID: 2.5.4.16)

**postalCode:** Specifies the postal code of an object (OID: 2.5.4.17)

**postOfficeBox:** Specifies the post office box for the physical delivery of mail (OID: 2.5.4.18)

**physicalDeliveryOfficeName:** Specifies the name of the city or place where a physical delivery office is located (OID: 2.5.4.19)

**telephoneNumber:** Specifies a telephone number (OID: 2.5.4.20)

**telexNumber:** Specifies a telex number (OID: 2.5.4.21)

**teletexTerminalIdentifier:** Specifies an identifier for a telex terminal (OID: 2.5.4.22)

**facsimileTelephoneNumber:** Specifies the telephone number for a facsimile terminal (OID: 2.5.4.23)

**x121Address:** Specifies the address used in electronic data exchange (OID: 2.5.4.24)

**internationalISDNNumber:** Specifies an international ISDN number used in voice, video, and data transmission (OID: 2.5.4.25)

**registeredAddress:** Specifies the postal address for the delivery of telegrams or expedited documents (OID: 2.5.4.26)

**destinationIndicator:** Specifies an attribute used in telegram services (OID: 2.5.4.27)

**preferredDeliveryMethod:** Specifies the preferred delivery method for a message (OID: 2.5.4.28)

**presentationAddress:** Specifies an OSI presentation layer address (OID: 2.5.4.29)

**supportedApplicationContext:** Specifies the identifiers for the OSI application contexts in the application layer (OID: 2.5.4.30)

**member:** Specifies the distinguished name of an object associated with a group or a list (OID: 2.5.4.31)

**owner:** Specifies the name of an object that has responsibility for another object (OID: 2.5.4.32)

**roleOccupant:** Specifies the distinguished name of an object that fulfills an organizational role (OID: 2.5.4.33)

**seeAlso:** Specifies the distinguished name of an object that contains additional information about the same real-world object (OID: 2.5.4.34)

**userPassword:** Specifies the object's password (OID: 2.5.4.35)

**name:** Specifies a name that is in the UTF-8 form of the ISO 10646 character set (OID: 2.5.4.41)

**givenName:** Specifies the given or first name of an object (OID: 2.5.4.42)

**initials:** Specifies the initials of an object (OID: 2.5.4.43)

**generationQualifier:** Specifies the generation of an object, which is usually a suffix (OID: 2.5.4.44)

**x500UniqueIdentifier:** Specifies an identifier that distinguishes between objects when a DN has been reused (OID: 2.5.4.45)

**dnQualifier:** Specifies information that makes an object unique when information is being merged from multiple sources and objects could have the same RDNs (OID: 2.5.4.46)

**enhancedSearchGuide:** Specifies a search filter used by X.500 users (OID: 2.5.4.47)

**protocolInformation:** Specifies information that is used with the presentationAddress attribute (OID: 2.5.4.48)

**distinguishedName:** Specifies the distinguished name of an object (OID: 2.5.4.49)

**uniqueMember:** Specifies the distinguished name of an object associated with a group or a list (OID: 2.5.4.50)

**houseIdentifier:** Identifies a building within a location (OID: 2.5.4.51)

**dmdName:** Specifies a directory management domain (OID: 2.5.4.54)

**E:** Specifies an e-mail address.

**EM:** Specifies an e-mail address.

**DC:** Specifies the domain name for an object (OID: 0.9.2342.19200300.100.1.25)

**uniqueID:** Contains an RDN-type name that can be used to create a unique name in the tree (OID: 0.9.2342.19200300.100.1.1)

**T:** Specifies the name of the tree root object (OID: 2.16.840.1.113719.1.1.4.1.181)

**OID:** Specifies an object identifier in dot notation.

- 3 To create a certificate, continue with [Step 6 on page 44](#), or to create a signing request, continue with [Step 5 on page 48](#).

## 3.2.3 Assigning Alternate Subject Names

- 1 Fill in the following fields:

**Name Type:** Names as specified by RFC 2459. Use the drop-down list to specify a name type, such as:

- ♦ **Directory name:** An X.500 directory name. The required format for the name is `.<attribute name>=<attribute value>`. For example:

`.O=novell.C=US`

Access Manager Appliance supports the following attributes:

Country (C)

Organization (O)

Organizational Unit (OU)

State or Province (S or ST)

Locality (L)

Common Name (CN)

- ♦ **IP Address:** An IP address such as 222.123.123.123
- ♦ **URI:** A URI such as `www.novell.com`.
- ♦ **Registered ID:** An ASN.1 object identifier.
- ♦ **DNS Name:** A domain name such as `novell.com`.
- ♦ **Email Address (RFC 822 name):** An e-mail address such as `ca@novell.com`.
- ♦ **X400 Name:** The messaging and e-mail standard specified by the ITU-TS (International Telecommunications Union - Telecommunication Standard Sector). It is an alternative to the more prevalent Simple Mail Transfer Protocol (SMTP) e-mail protocol. X.400 is common in Europe and Canada.
- ♦ **EDI Party:** EDI (Electronic Data Interchange) is a standard format for exchanging business data.
- ♦ **Other:** A user-defined name.

**Name:** The display alternative name.

- 2 Continue with [Step 11 on page 45](#).

## 3.2.4 Generating a Certificate Signing Request

- 1 In the Administration Console, click **Security > Certificates > New**.

- 2 To create a certificate signing request (CSR), select **Use external certificate authority**.

This option generates a CSR for you to send to the CA for signing. A third-party CA is managed by a third party outside of the eDirectory tree. An example of a third party CA is VeriSign. After the signed certificate is received, you need to import the certificate.

- 3 Specify a Certificate name.

Pick a unique, system-wide name for the certificate that you can easily associate with the certificate's purpose. The name must contain only alphanumeric characters and no spaces.

- 4 Click the **Edit** button to display a dialog box that lets you add appropriate locality information types for the subject name.

For more information, see [Section 3.2.2, "Editing the Subject Name," on page 45](#).

- 5 Click **OK**, then fill in the following fields:



**Signature algorithm:** The algorithm you want to use (SHA-1, MD-2, or MD-5). SHA-1 is currently recommended.

**Valid from:** The date from which the certificate is valid. For externally signed certificates, the external certificate authority sets the validity period.

**Months valid:** The number of months that the certificate is valid.

**Key size:** The size of the key. Select 512, 1024, 2048, or 4096.

- 6 (Conditional) If you are creating a key for a certificate authority, click **Advanced Options**, then configure the following:

**This key is for a Certificate Authority:** Select this option.

**Critical:** Enforces the basic constraints you specify. Select one of the following:

- ♦ **Unlimited:** Specifies no restriction on the number of subordinate certificates that the CA can verify.
- ♦ **Do not allow intermediate signing certificates in certificate chain:** Prevents the CA from creating other CAs, but it can create server or user certificates.
- ♦ **Number of allowable intermediate signing certificates in signing chain:** Specifies how many subordinate certificates are allowed in the certificate chain. Values must be 1 or more. Entering 0 creates only entity objects.

- 7 Click **OK**.

- 8 Click the name of the certificate, copy the CSR data and send the information to the external CA. The certificate status is CSR Pending until you import the signed certificate.

- 9 Click **Close**.

- 10 When you receive the signed certificate and the trusted root (CA chain), continue with [“Importing a Signed Certificate” on page 49](#).

## 3.2.5 Importing a Signed Certificate

After you receive the signed certificate and the CA chain, you must import it. CA can return the certificate in multiple ways. Typically, the CA either returns one or more files each containing one certificate, or returns a file with multiple certificates in it.

The following figure illustrates a certificate chain example.

**Figure 3-2** Illustration of a Certificate Chain Example



To import this certificate chain:

- 1 In the Administration Console, click **Security > Certificates**, then click the name of a certificate that is in a CSR Pending state.
- 2 Click **Import Signed Certificate**.
- 3 In the Import Signed Certificate dialog box, browse to locate the Entity certificate data file or paste the Entity certificate data text into the **Certificate data text** field.
- 4 To import the CA chain, click **Add trusted root** and then locate the Root certificate data.

- 5 Click **Add intermediate certificate** if you need to continue adding certificates to the chain for example, add Intermediate cert 1 and cert 2 in that order.
- 6 Click **OK**, then click **Close** on the Certificate Details page.

The certificate is now available for use by Access Manager Appliance devices.

---

**NOTE:** When there is a server certificate and more than two intermediate CA certificates, use PKCS7 format file and import the certificate and its CA chain.

---

If you receive an error when attempting to import the certificate, see [Chapter 9, “Troubleshooting Certificate Issues,”](#) on page 113.

## 3.3 Managing Certificates and Keystores

You can import certificates created by an external certificate authority. These certificates then need to be assigned to a device by adding the certificate to the device’s keystore. The subject name of the certificate needs to match the DNS name of the device, or if you are using wildcard certificates, the main domain name needs to match. You can perform the following certificate tasks:

- ♦ [Section 3.3.1, “Viewing Certificate Details,”](#) on page 50
- ♦ [Section 3.3.2, “Renewing a Certificate,”](#) on page 52
- ♦ [Section 3.3.3, “Exporting a Private/Public Key Pair,”](#) on page 54
- ♦ [Section 3.3.4, “Exporting a Public Certificate,”](#) on page 54
- ♦ [Section 3.3.5, “Importing a Private/Public Key Pair,”](#) on page 55
- ♦ [Section 3.3.6, “Reviewing the Command Status for Certificates,”](#) on page 55

### 3.3.1 Viewing Certificate Details

The Certificate Details page lists the properties of a certificate, such as certificate type, name, subject, and assigned keystores. The fields are not editable.

- 1 In the Administration Console, click **Security > Certificates**.
- 2 Select one of the following:
  - ♦ Click the name of a certificate that is not in a CSR Pending state. The Certificate Details page contains the following information about the certificate:

| Field                | Description                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Issuer</b>        | The name of the CA that created the certificate.                                                                |
| <b>Serial number</b> | The serial number of the certificate.                                                                           |
| <b>Subject</b>       | The subject name of the certificate.                                                                            |
| <b>Valid from</b>    | The first date and time that the certificate is valid.                                                          |
| <b>Valid to</b>      | The date and time that the certificate expires.                                                                 |
| <b>Devices</b>       | The devices that are configured to hold this certificate on their file system and the keystore that holds them. |
| <b>Key size</b>      | The key size that was used to create the certificate.                                                           |

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Signature algorithm</b>               | The signature algorithm that was used to create the certificate.                                                                                                                                                                                                                                                                                                 |
| <b>Finger print (MD5)</b>                | The certificate's message digest that was calculated with the MD5 algorithm. It is embedded into the certificate at creation time. It can be used to uniquely identify a certificate. For example, users can verify that a certificate is the one they think it is by matching this published MD5 fingerprint with the MD5 fingerprint on the local certificate. |
| <b>Finger print (SHA1)</b>               | The certificate's message digest that was calculated with the SHA1 algorithm. It is embedded into the certificate at creation time. It can be used to uniquely identify a certificate. For example, users can verify that a certificate is the one they think it is by matching a published SHA1 fingerprint with the SHA1 fingerprint on the local certificate. |
| <b>Subject Alternate Names: Critical</b> | Indicates whether an application should reject the certificate if the application does not understand the alternate name extensions. Any configured alternate names are displayed in the list.                                                                                                                                                                   |
| <b>Key Usage: Critical</b>               | Indicates whether an application should reject the certificate if the application does not understand the key usage extensions.                                                                                                                                                                                                                                  |
| <b>Sign CRLs</b>                         | Indicates whether the certificate is used to sign CRLs (Certificate Revocation Lists).                                                                                                                                                                                                                                                                           |
| <b>Sign certificates</b>                 | Indicates whether the certificate is used to sign other certificates.                                                                                                                                                                                                                                                                                            |
| <b>Encrypt other keys</b>                | Indicates whether the certificate is used to encrypt keys.                                                                                                                                                                                                                                                                                                       |
| <b>Encrypt data directly</b>             | Indicates whether the certificate can encrypted data for private transmission to the key pair owner. Only the intended receiver can read the data.                                                                                                                                                                                                               |
| <b>Create digital signatures</b>         | Indicates whether the certificate can create digital signatures.                                                                                                                                                                                                                                                                                                 |
| <b>Non-repudiation</b>                   | Indicates whether the certificate links a digital signature to the signer and the data. This prevents others from duplicating the signature because no one else has the signer's private key. Additionally, the signer cannot deny having signed the data.                                                                                                       |
| <b>CRL Distribution Points</b>           | A list of Certificate Revocation List (CRL) distribution points that are embedded into the certificate as an extension at certificate creation time. Implementations search the CRL from each distribution point (the distribution point is usually a URI that points to a store of revoked certificates) to see whether a certificate has been revoked.         |
| <b>Authority Info Access (OCSP)</b>      | A list of Online Certificate Status Protocol (OCSP) responders that are embedded into the certificate as an extension at certificate creation time. Implementations query the OCSP responder to see whether a certificate has been revoked.                                                                                                                      |

- Click the name of a certification in a CSR Pending state. The following information is displayed:

---

|                            |                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Subject</b>             | The subject name of the certificate.                                                                               |
| <b>Valid from</b>          | The date and time that the request was generated.                                                                  |
| <b>Valid to</b>            | The date and time that the request expires.                                                                        |
| <b>Devices</b>             | No entries. A CSR cannot be assigned to a device.                                                                  |
| <b>Key size</b>            | The key size that was used to create the request.                                                                  |
| <b>Signature algorithm</b> | The signature algorithm that was used to create the request.                                                       |
| <b>State</b>               | Displays <code>CSR Pending</code> , indicating that the request has been generated.                                |
| <b>CSR data</b>            | The certificate signing request data. You can either export this data or copy and paste it into CA's request tool. |

---

- (Conditional) For a certificate not in a CSR Pending state, select one of the following actions:

**Renew:** Allows you to renew the certificate. For more information, see [Section 3.3.2, “Renewing a Certificate,” on page 52](#).

**Export Private/Public Keypair:** Allows you to export private certificates to obtain a backup copy of the key, to move the key to a different server, or to share the key between servers. For more information, see [Section 3.3.3, “Exporting a Private/Public Key Pair,” on page 54](#)

**Export Public Certificate:** Allows you to export a public key certificate to a file. For more information, see [Section 3.3.4, “Exporting a Public Certificate,” on page 54](#).

- (Conditional) For a certificate in a CSR Pending state, select one of the following actions:

**Import Signed Certificate:** Allows you to import the certificate that was generated for this request. For more information, see [Section 3.2.5, “Importing a Signed Certificate,” on page 49](#).

**Export CSR:** Allows you to export the CSR to a CSR file.

---

**NOTE:** Whenever the configuration store contains a Key Material Object (KMO) with a CSR in pending state, the KMO will not be exported by using the `amdiagcfg` script and not be backed up by using the `ambkup` script.

---

## 3.3.2 Renewing a Certificate

The Certificate Details page lists the properties of a certificate, such as certificate type, name, subject, and assigned keystores. This page also includes the original CSR when the certificate is still in a pending state (for example, you have generated the CSR, but you have not yet received and imported the signed certificate). If the certificate is expiring, you can cut and paste its text to send it to the CA to get a renewed certificate, then import the newly signed certificate.

For the certificates that Access Manager Appliance uses internally, a certificate process is started with Tomcat. This process runs once every 24 hours. It checks all the internal certificates and determines if they are going to expire within 30 days. If they are due to expire, the process automatically regenerates the certificate or trusted root. When a certificate is regenerated, the following message appears:

```
One or more automatically created certificates were regenerated. Reboot the entire
administration console as soon as possible to avoid interruption of service.
```

This message appears when the administrator logs in to the Administration Console, or if the administrator is already logged in, when the administrator switches from one page to another.

This event is also auditing. Another audit event is also generated which tells the administrator to restart any effected services. When the Administration Console certificate and the eDirectory certificates are expiring, a log entry is written to the app\_sc log file. The log entry contains the "Recreating auto-generated certificates" string as well as a couple success or failure messages per key re-generated.

Certificates and trusted roots that are manually created with the Access Manager Appliance CA or are imported into Administration Console use a different process. The administrator is warned that these certificates are expiring when the administrator logs in to the Administration Console. The following message is displayed:

```
Warning: the following certificates are expired or will expire within X days:  
<certA>, <certB>.
```

This message is displayed each time the administrator logs in to the Administration Console. Events for the expiration of these certificates are not audited and are not logged.

The following figure illustrates the certificate chain example.

**Figure 3-3** Illustration of a Certificate Chain Example



To renew a certificate:

- 1 In the Administration Console, click **Security > Certificates**.
- 2 Click the certificate name.
- 3 Click **Renew**.
- 4 On the Renew page, either browse to locate and select the certificate or select the **Certificate data text (PCM/Base64)** option and paste the certificate data into the text box.
- 5 To import the CA chain, click **Add trusted root** and then locate the Root certificate data.
- 6 Update the device using the certificate.
- 7 Click **Add intermediate certificate** if you need to continue adding certificates to the chain for example, add Intermediate cert 1 and cert 2 in that order.
- 8 Click **OK**, then click **Close**.

### 3.3.3 Exporting a Private/Public Key Pair

When you create a certificate, you can specify whether it is exportable. If a key is exportable, it can be extracted and put in a file along with the associated certificate. The file is written in an industry standard format, PKCS#12, which allows it to be transported to other platforms. It is encrypted with a user-specified password to protect the private key. You can export private certificates to obtain a backup copy of the key, to move the key to a different server, or to share the key between servers.

You cannot export a certificate if you enabled the **Do not allow private key to be exportable option** while creating the certificate.

- 1 In the Administration Console, click **Security > Certificates**.
- 2 On the Certificates page, click the certificate.
- 3 On the Certificate Details page, click **Export Private/Public Keypair**.



- 4 Select a format for the key:  
**PFX/PKCS12:** Public Key Cryptography Standards #12 (PKCS#12) format, which is also called PFX format. This format can be used to create JKS or PEM files.  
**JKS:** Java keystore format.
  - 5 Specify the password in the **Encryption/decryption** password field, then click OK.
- 
- IMPORTANT:** Remember this password because you need it to re-import the key.
- 
- 6 Click **OK**.

### 3.3.4 Exporting a Public Certificate

You can export a trusted root or a public key certificate to a file so that a client can use it to verify the certificate chain sent by a cryptography-enabled application, or to have a backup copy of the file.

You can export the certificate in the following formats:

- ♦ DER-encoded (.der) to a file.
- ♦ PEM-encoded to a file. This is a Base64-encoded DER certificate that is enclosed between the BEGIN CERTIFICATE and END CERTIFICATE tags.
- ♦ PEM CUT/Paste Buffer. This displays the certificate data so you can copy it to the system Clipboard. You can then pasted it directly into a cryptography-enabled application.

To export the public certificate:

- 1 In the Administration Console, click **Security > Certificates**.
- 2 Click the certificate name.

- 3 On the Certificate Details page, click **Export Public Certificate**, then click the file type.
- 4 Save the output file to the location of your choosing.

### 3.3.5 Importing a Private/Public Key Pair

If you created a key pair that was exported from another certificate management system, you can import the key pair and then assign it to an Access Manager device. The file needs to be in PFX/PKCS12 (\*.pfx or \*.p12) format.

- 1 In the Administration Console, click **Security > Certificates**.
- 2 Choose **Actions > Import Private/Public Keypair**.
- 3 Fill in the following fields:

**Certificate name:** The name of the certificate. This is a system-wide, unique name used by Access Manager. The name must contain only alphanumeric characters and no spaces. If the name starts with a number, an underline (\_) prefix is added to the name so that the name conforms to XML requirements. If the name contains invalid characters, it is automatically renamed.

**Keystore password:** Type the encryption/decryption password established when exporting the certificate.

**Certificate data file (PFX/PKCS12):** The certificate file to import. You can browse to locate the \*.pfx or \*.p12 file.

**Certificate data file (JKS):** To locate a JKS file, select this option, then click **Browse**.

- 4 Click **OK**.

If you receive an error when importing the certificate, the error comes from either NCI or PKI. For a description of these error codes, see *Novell Certificate Server Error Codes and Novell International Cryptographic Infrastructure* (<http://www.novell.com/documentation/nwec/index.html>). For general certificate import issues, see [Section 9.1.1, "Importing an External Certificate Key Pair," on page 113](#).

### 3.3.6 Reviewing the Command Status for Certificates

You can view the status of the commands that have been sent to the certificate server for execution.

- 1 In the Administration Console, click **Security > Certificates**, then click **Command Status**.
- 2 Use the following options to review or change a server's certificate command status:
  - ♦ **Delete:** To delete a command, select the check box for the command, then click **Delete**. The selected command is cleared.
  - ♦ **Refresh:** Click **Refresh** to update the current cache of recently executed commands.
  - ♦ **Name:** Click this box to select all the commands in the list, then click **Refresh** or **Delete**.

The following table describes the features on this page:

| Column Name            | Description                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>            | Contains the display name of the command. Click the link to view additional details about the command.                                 |
| <b>Status</b>          | Specifies the status of the command. Some of the possible states of the command include Pending, Incomplete, Executing, and Succeeded. |
| <b>Type</b>            | Specifies the type of server, such as Identity Server or Access Gateway.                                                               |
| <b>Commands</b>        | Specifies the command given, such as Import certificate, or Import trusted root.                                                       |
| <b>Admin</b>           | Specifies if the system or a user issued the command. If a user issued the command, the DN of the user is displayed.                   |
| <b>Date &amp; Time</b> | Specifies the local date and time the command was issued.                                                                              |

- 3 To review command information, click a link under the **Name** column.

**Server Details Edit: Server Scheduled Command**

Note: Date and time entries are specified in local time.

**Command Information**

[Refresh](#) | [Delete](#)

|                   |                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------|
| Name:             | Import trusted root with name (configCA) to trust store (Proxy Trust Store) on (151.155.1 |
| Type:             | Import trusted root                                                                       |
| Admin:            | cn=admin,o=novell                                                                         |
| Status:           | Succeeded                                                                                 |
| Last Executed On: | Jun 4, 2007 8:22 AM                                                                       |

**Command Execution Details**

| Command      | Command Result |
|--------------|----------------|
| CertTRImport | Success        |

This page displays status information about the command and allows you to perform the following tasks:

**Refresh:** Select this option to refresh the data for this command.

**Delete:** Select this option to clear this command.

The following command information is listed:

**Name:** Specifies the display name that has been given to the command.

**Type:** Specifies the type of command.

**Admin:** Specifies whether the system or a user issued the command. If a user issued the command, the field contains the DN of the user.

**Status:** Specifies the status of the command, and includes such states as **Pending**, **Incomplete**, **Executing**, and **Succeeded**.

**Last Executed On:** Specifies when the command was issued. The date and time are displayed in local time. If the command failed, additional information is available.



For a command that the Administration Console can successfully process, the page displays a **Command Execution Details** section with the name of the command and the command results.

- 4 Click **Close**.

## 3.4 Managing Trusted Roots

A certificate from a certificate authority (CA) is commonly referred to as trusted root. A trusted root is a trusted certificate, or the certificate of a known CA. These certificates are self-signed and are recognized as representing a CA that is trusted. To validate a digital signature, you must trust at least one of the certificates in the user or server's certificate chain. You can directly trust the certificate of the user or server, or you can choose to trust any other certificate in the chain. Typically, the certificate that is trusted is the root CA's certificate.

- 1 In the Administration Console, click **Security > Trusted Roots**.

- 2 Select from the following actions:

**Import:** Allows you to import trusted roots so that Access Manager devices can trust the certificate sent by other computers at runtime. For more information, see [Section 3.4.1, "Importing Public Key Certificates \(Trusted Roots\)," on page 57](#).

**Delete:** To delete a trusted root, select the trusted root, then click **Delete**.

**Auto Import From Server:** To import a trusted root from another server, click **Auto Import From Server**. For more information, see [Section 3.4.2, "Auto-Importing Certificates from Servers," on page 57](#).

### 3.4.1 Importing Public Key Certificates (Trusted Roots)

You import trusted roots so that the specific device can trust the certificate sent by other computers at runtime. After you import a trusted root, you can assign it to the proper trust store associated with a device, which allows the device to trust certificates signed by the trusted root.

- 1 In the Administration Console, click **Security > Trusted Roots**.

- 2 Click **Import**, then specify a name for the certificate.

This is a system-wide, unique name used by Access Manager Appliance.

- 3 Select one of the following methods to import the public key:

- ♦ **Certificate data file (DER/PKM/PCS7):** Select this method to browse to a file. Click **Browse** to locate the file on your file system.
- ♦ **Certificate data text (PKM/Base64):** Select this method to paste Base64-encoded certificate data text.

- 4 Click **OK**.

### 3.4.2 Auto-Importing Certificates from Servers

You can import certificates from other servers (such as an LDAP server, an identity provider, or service provider) and make them available for use in Access Manager Appliance. You must provide the IP address, port, and certificate name.

- 1 In the Administration Console, click **Security > Trusted Roots > Auto-Import from Server**.

- 2 Fill in the following fields:

**Server IP Address:** Specify the server IP address. You can use a DNS name.

**Server Port:** Specify the server port.

**Certificate Name:** Specify a unique name of the certificate to store in Access Manager.

- 3 Click **OK**.

### 3.4.3 Exporting the Public Certificate of a Trusted Root

You can export a trusted root or a public key certificate to a file so that a client can use it to verify the certificate chain sent by a cryptography-enabled application, or to have a backup copy of the file.

You can export the certificate in the following formats:

- ♦ DER-encoded (.der) to a file.
- ♦ PEM-encoded to a file. This is a Base64-encoded DER certificate that is enclosed between BEGIN CERTIFICATE and END CERTIFICATE tags.
- ♦ PEM CUT/Paste Buffer. This displays the certificate data so you can copy it to the system Clipboard. You can then pasted it directly into a cryptography-enabled application.

To export the public certificate:

- 1 In the Administration Console, click **Security > Trusted Roots**.
- 2 Click the name of the trusted root.
- 3 On the Certificate Details page, click **Export Public Certificate**, then click the file type.
- 4 Save the output file.

### 3.4.4 Viewing Trusted Root Details

- 1 In the Administration Console, click **Security > Trusted Roots**.
- 2 Click the name of a trusted root.
- 3 View the following information:

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Issuer</b>              | The name of the CA that created the certificate.                                                                                                                                                                                                                                                                                                                 |
| <b>Serial number</b>       | The serial number of the certificate.                                                                                                                                                                                                                                                                                                                            |
| <b>Subject</b>             | The subject name of the certificate.                                                                                                                                                                                                                                                                                                                             |
| <b>Valid from</b>          | The first date and time that the certificate is valid.                                                                                                                                                                                                                                                                                                           |
| <b>Valid to</b>            | The date and time that the certificate expires.                                                                                                                                                                                                                                                                                                                  |
| <b>Key size</b>            | The key size that was used to create the certificate.                                                                                                                                                                                                                                                                                                            |
| <b>Signature algorithm</b> | The signature algorithm that was used to create the certificate.                                                                                                                                                                                                                                                                                                 |
| <b>Finger print (MD5)</b>  | The certificate's message digest that was calculated with the MD5 algorithm. It is embedded into the certificate at creation time. It can be used to uniquely identify a certificate. For example, users can verify that a certificate is the one they think it is by matching this published MD5 fingerprint with the MD5 fingerprint on the local certificate. |

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Finger print (SHA1)</b> | The certificate's message digest that was calculated with the SHA1 algorithm. It is embedded into the certificate at creation time. It can be used to uniquely identify a certificate. For example, users can verify that a certificate is the one they think it is by matching a published SHA1 fingerprint with the SHA1 fingerprint on the local certificate. |

The **Subject Alternate Names** section indicates whether an application should reject the certificate if the application does not understand the alternate name extensions. Any configured alternate names are displayed in the list.

The **Key Usage** section indicates whether an application should reject the certificate if the application does not understand the key usage extensions. The following are possible:

**Sign CRLs:** Indicates whether the certificate is used to sign CRLs (Certificate Revocation Lists).

**Sign certificates:** Indicates that the certificate is used to sign other certificates.

**Encrypt other keys:** Indicates that the certificate is used to encrypt keys.

**Encrypt data directly:** Indicates that the certificate encrypts data for private transmission to the key pair owner. Only the intended receiver can read the data.

**Create digital signatures:** Indicates that the certificate is used to create digital signatures.

**Non-repudiation:** Indicates that the certificate links a digital signature to the signer and the data. This prevents others from duplicating the signature because no one else has the signer's private key. Additionally, the signer cannot deny having signed the data.

**CRL Distribution Points:** Displays a list of Certificate Revocation List (CRL) distribution points that are embedded into the certificate as an extension at certificate creation time. Implementations search the CRL from each distribution point (the distribution point is usually a URI that points to a store of revoked certificates) to see whether a certificate has been revoked.

**Authority Info Access (OCSP):** Displays a list of Online Certificate Status Protocol (OCSP) responders that are embedded into the certificate as an extension at certificate creation time. Implementations query the OCSP responder to see whether a certificate has been revoked.

- 4 **Export Public Certificate:** Allows you to export a trusted root to a file so that a client can use it to verify the certificate chain sent by a cryptography-enabled application. For more information, see [Section 3.3.4, "Exporting a Public Certificate,"](#) on page 54.

- 5 Click **Close**.

## 3.5 Viewing External Trusted Roots

The Identity Server uses local Access Manager Appliance CA and external certificate authorities to verify the SSL certificates. The external certificates are listed in the **External Trusted Roots** tab.

**NOTE:** All the well-known trusted roots are added to the proxy trust store during the Access Manager Appliance Installation.

- 1 In Administration Console, click **Security > Trusted Roots > External Trusted Roots**.

The **External Trusted Roots** tab lists all the external trusted roots that Access Manager Appliance supports.

2 View the following information:

| Field         | Description                                                          |
|---------------|----------------------------------------------------------------------|
| Alias         | The name of the certificate as seen by the Access Manager appliance. |
| Issuer        | The name of the CA that created the certificate.                     |
| Subject       | The subject name of the certificate.                                 |
| Starting Date | The date and time from which the certificate is valid.               |
| Ending Date   | The date and time till that the certificate is valid.                |

## 3.6 Security Considerations for Certificates

Your security deployment plan should contain policies for the following:

- ♦ **Key size for certificates:** Access Manager Appliance ships with a CA that can create certificates with a key size of 512, 1024, 2048, or 4096. Select the maximum size supported by the applications that you are protecting with Access Manager Appliance.
- ♦ **Certificate renewal dates:** Certificates should be renewed every two years. Your security needs might allow for a longer or shorter period.
- ♦ **Trusted certificate authorities:** Access Manager Appliance ships with a CA, and during installation of the various components, it creates and distributes certificates. For added security, you might want to replace these certificates with certificates from a well-known CA.

For more information about how to import certificates, see [Section 3.2.5, “Importing a Signed Certificate,” on page 49](#).

## 3.7 Assigning Certificates to Access Manager Appliance

This section discusses how you update, renew, and assign certificates to Access Manager Appliance.

The Access Gateway can be configured to use certificates for SSL communication with two types of entities:

- ♦ **Client Browsers:** You can enable SSL communication between the client browsers and the Access Gateway. When setting up this feature, you can either have the Access Manager Appliance CA automatically generate a certificate key or you can select a certificate key you have already imported (or created) for the reverse proxy. To manage this certificate in the Administration Console, click **Access Gateways** > **[Configuration Link]** > **[Name of Reverse Proxy]**. For more information, see “[Managing Reverse Proxies and Authentication](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*.
- ♦ **Protected Web Servers:** You can enable SSL communication between the Access Gateway and the protected Web servers. This option is only available if you have enabled SSL communication between the browsers and the Access Gateway. You can enable SSL or mutual SSL. To manage these certificates in the Administration Console, click **Access Gateways** > **[Configuration Link]** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **Web Servers**.

---

# 4 Monitoring Access Manager By Using Simple Network Management Protocol

The Administration Console captures all statistics sent by the Identity Server and the Access Gateway. These statistics sent at periodic intervals, are stored in eDirectory.

You can use any Network Monitoring System (NMS) or an SNMP-enabled client to gather statistics from the Administration Console by using Simple Network Management Protocol (SNMP). Simple Network Management Protocol (SNMP) is a network management protocol for network management that collects information from devices on a network. Access Manager supports SNMP v2 for the purpose of monitoring Identity Server and Access Gateway.

---

**NOTE:** This release of Access Manager does not support SNMP traps.

---

## 4.1 SNMP Architecture in Access Manager

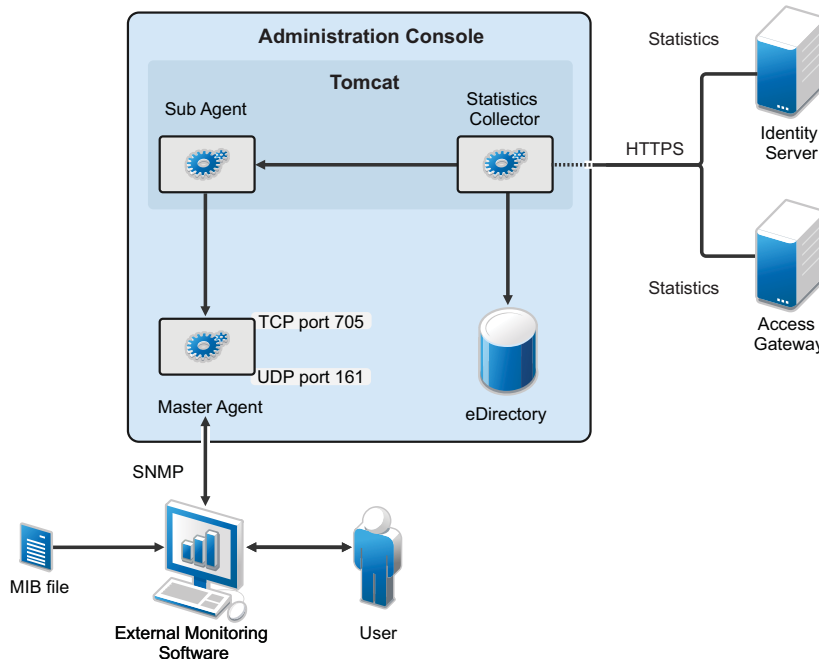
Access Manager introduces Master Agent, Sub Agent, and a Management Information base (MIB) file to work with any third-party monitoring software using SNMP.

The Master Agent runs as a service in the Administration Console and listens to the Sub Agents registered with it. A Sub Agent is a managed device that is registered with the Master Agent and exchanges information with it using TCP port 705. The MIB file contains a hierarchical list of variables and defines the information that is provided by the devices. Each variable in this list is uniquely identified by an OID (Object Identifier) and are read-only in nature.

The Administration Console contains both Master Agent and Sub Agent. Master Agent runs as a separate service and the Sub Agents are registered with the Master Agent for monitoring. The Administration Console gathers statistics from all devices and acts as a centralized repository for any monitoring tool to access the data by using SNMP. The external NMS contacts the Administration Console to get the data about any Identity Server or Access Gateway by using SNMP. For this communication it uses UDP port 161 (by default).

In a clustered Administration Console setup, the devices send statistics to the secondary Administration Console in case the primary Administration Console is down.

**Figure 4-1** Architecture of SNMP Components in Access Manager



This MIB file contains all the Identity Server and Access Gateway attributes available to monitor the state of the system. [Figure 4-1 on page 62](#) illustrates how Administration Console uses SNMP to monitor the Identity Server and the Access Gateway.

If you are installing or upgrading Access Manager on a Linux server, the Master Agent is automatically installed. A Windows server has an inbuilt SNMP Master Agent, but it does not support the AgentX protocol. The AgentX protocol is used for communication between the Master Agent and Sub Agent. Due to this, if you are installing Access Manager on a Windows server, the Master Agent has to be downloaded and installed manually. For more information about installing the Master Agent on a Windows server, see [Section 4.5.2, “Installing and Enabling Monitoring for Access Manager on Windows,” on page 66](#)

## 4.2 Features of Monitoring in Access Manager

In Access Manager 4.0, monitoring using SNMP includes the following features:

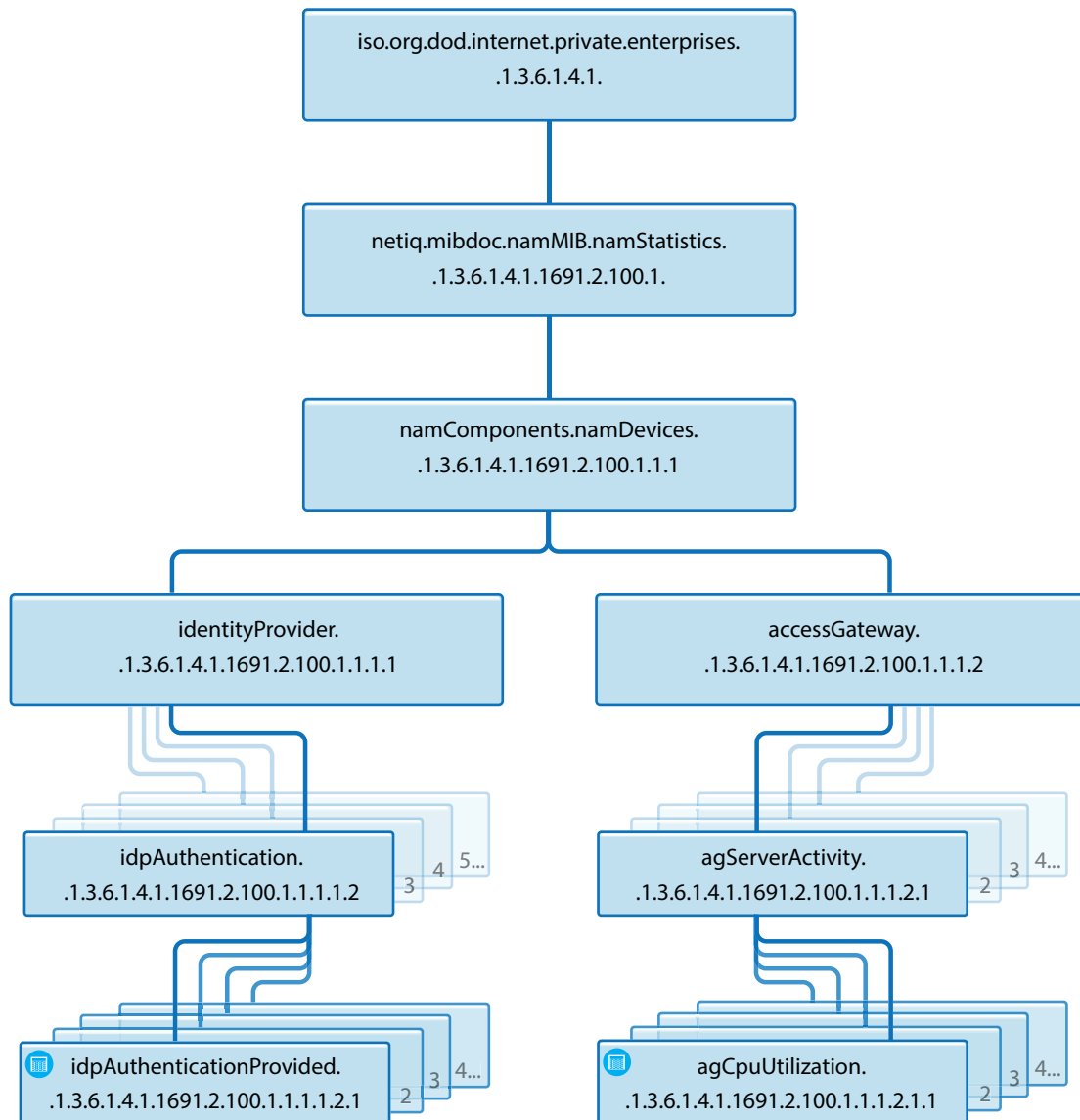
- ♦ Ability to enable/disable monitoring - By default SNMP is not enabled. You can configure it to enable monitoring for Access Manager components. For details about enabling monitoring, see [“Installing and Enabling Monitoring for Access Manager Components” on page 65](#)
- ♦ Facility to change port information or IP address of the Master Agent- You can configure the Master Agent to listen on a different port or IP address. The default port is TCP 705.
- ♦ Master Agent and Sub Agent architecture support multiple sub agents - The Master Agent - Sub Agent architecture helps you configure additional Sub Agents to be monitored. For example, you can configure a single Master Agent to receive data from Access Manager components, eDirectory as well as SLES Sub-Agents.
- ♦ Automatic data synchronization on device addition or removal - The MIB structure is automatically adjusted for dynamic addition or removal of components
- ♦ Automatic reconnect to Master Agent - Every time the Administration Console is restarted the reconnection to the MasterAgent happens automatically. No manual steps are required.

## 4.3 Using the Default MIB File with External SNMP Systems

When Access Manager is installed, NAM.mib file is placed in the `opt/novell/devman/share/conf` folder. On a Windows server this file is placed in the `C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\` folder.

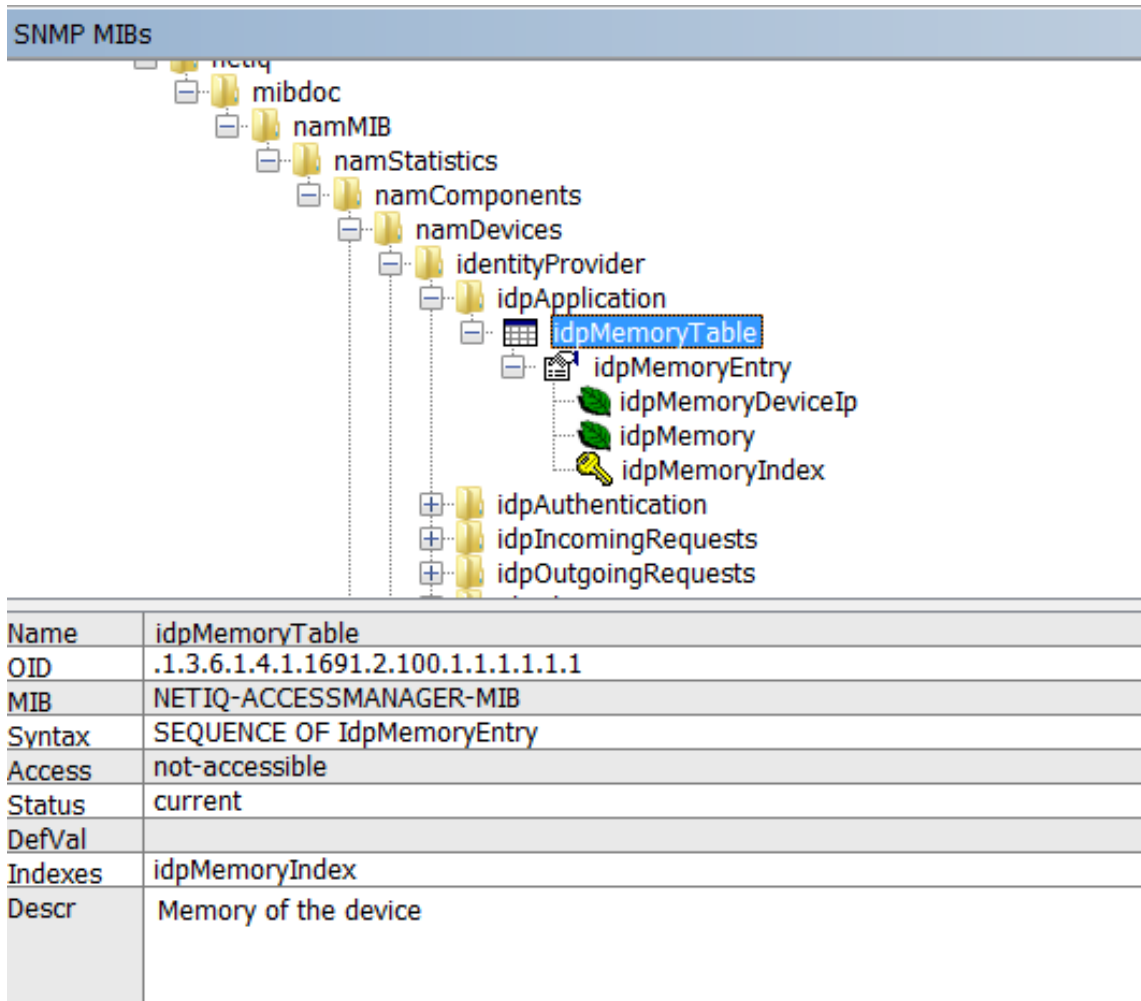
This MIB file contains textual information of Identity Server and Access Gateway attributes. You can use these attributes to monitor the state of the system. The attributes are uniquely identified by an OID (Object Identifier) or namespace. [Figure 4-2 on page 63](#) shows the hierarchy of a MIB file when viewed with a MIB browser.

**Figure 4-2** The MIB file viewed in a MIB Browser



Each statistic entry in the MIB file has a corresponding description to help identify the attribute.

**Figure 4-3** Description of an attribute in the MIB file



Every time a new Identity Server or Access Gateway is added or removed the SNMP data available in the Administration Console is updated. If a device is not accessible for some reason, the MIB file (when viewed with a MIB Browser) displays the last reported statistics for all the attributes except for the Health Status of the devices. The Health Status of the devices are updated periodically.

## 4.4 Querying For SNMP Attributes

To query any SNMP attribute the following details are needed:

- ♦ IP Address of the Administration Console
- ♦ The community string name
- ♦ The Object Identifier (OID) of the attributeID
- ♦ The IP address of the device - Identity Server or Access Gateway.

For example, consider a scenario where you want to query the memory utilization of an Identity Server with IP address 10.0.0.0. The query is issued to the Administration Console whose IP address is 192.168.0.0

You can perform the query either by using the OID or by using the namespace of the object.



If you are using the net-snmp package for monitoring, the equivalent command to retrieve memory utilization details are:

## 4.4.1 Querying Using the Namespace

```
snmpget -v2c -m NETIQ-ACCESSMANAGER-MIB -c netiq 192.168.0.0
.iso.org.dod.internet.private.enterprises.netiq.mibdoc.namMIB.namStatistics.namCom
ponents.namDevices.identityProvider.idpApplication.idpMemoryTable.idpMemoryEntry.i
dpMemory.10.0.0.0
```

## 4.4.2 Querying Using the OID

```
snmpget -v2c -c netiq 192.168.0.0 .1.3.6.1.4.1.1691.2.100.1.1.1.1.1.1.1.1.
10.0.0.0
```

In the same manner you can query values of various attributes supported by the Identity server and the Access Gateway.

Using the same example if you query idpHealthEntry parameter using the Namespace, the command is:

```
snmpget -v2c -m NETIQ-ACCESSMANAGER-MIB -c netiq 192.168.0.0
.iso.org.dod.internet.private.enterprises.netiq.mibdoc.namMIB.namStatistics.namCom
ponents.namDevices.identityProvider.idpApplication.idpHealthEntry.idpMemoryEntry.i
dpMemory.10.0.0.0
```

The idpApplication parameter is substituted with the idpHealthEntry attribute in the above example.

## Understanding Return Values of an SNMP Query

When an SNMP query is performed, it retrieves the last fetched data from the Administration Console. If the device is down or not reachable a negative value is retrieved.

For example: If you query for the idpHealthyEntry attribute, the value that is returned can be Red, Yellow, Green or NoReport.

---

**NOTE:** The return value of NoReport indicates a server that is disconnected or unavailable.

---

## 4.5 Installing and Enabling Monitoring for Access Manager Components

- [Section 4.5.1, “Installing and Enabling Monitoring for Access Manager on Linux,” on page 65](#)
- [Section 4.5.2, “Installing and Enabling Monitoring for Access Manager on Windows,” on page 66](#)

### 4.5.1 Installing and Enabling Monitoring for Access Manager on Linux

- 1 To install the Master Agent and Sub Agent on Linux, no manual steps are required.

All packages necessary to monitor Access Manager are automatically installed during upgrade or installation. The Administration Console is automatically installed and configured as the Master Agent and the Sub Agents are in turn registered with the Administration Console for monitoring.

- 2 In the `opt/novell/devman/share/conf/platform.conf` file, traverse to the `vcdn` module for SNMP. In `<stringParam name="enable" value="false"`, replace `false` with `true`. This enables monitoring between Access Manager devices.  
  
The `vcdn` module also contains port details. If needed, you can configure the Master Agent to listen on a different port or IP address. The default port is TCP 705.
- 3 In the `snmp-master-agent.conf` file, change the community name. The default name is `netiq`. Changing the community name is recommended for security purpose.
- 4 Start the Master Agent by using the `/etc/init.d/novell-snmpd start` command.
- 5 Restart the Administration Console using `/etc/init.d/novell-ac restart` command for the changes to take effect.
- 6 If you encounter any errors while enabling monitoring, review the `platform.0.log` file available in the `/var/opt/novell/nam/logs/adminconsole/volera` folder.

## 4.5.2 Installing and Enabling Monitoring for Access Manager on Windows

- 1 On a Windows server, the Master Agent has to be manually installed and configured.  
  
Download the `net-snmp 5.4.2` package and install it. For downloading binaries, go to [Sourceforge \(http://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/\)](http://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/) (The supported version is 5.4.2).
- 2 Register windows service by running the following command:  
  

```
C:\usr\bin\snmpd.exe -register -Lf "C:/usr/log/snmpd.log" -c "C:/Program Files (x86)/Novell/Tomcat/webapps/roma/WEB-INF/conf/snmp-master-agent.conf"
```

  
If you uninstall `net-snmp`, it is important to unregister. Use the following command to unregister:  
  

```
C:\usr\bin\snmpd.exe -unregister -Lf "C:/usr/log/snmpd.log" -c "C:/Program Files (x86)/Novell/Tomcat/webapps/roma/WEB-INF/conf/snmp-master-agent.conf"
```
- 3 In the `C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\platform.conf` file, traverse to the `vcdn` module.  
  
In `<stringParam name="enable" value="false"`, replace `false` with `true`. This enables monitoring between Access Manager devices.  
  
The `vcdn` module also contains port details. If needed, you can configure the Master Agent to listen on a different port or IP address. The default port is TCP 705.
- 4 In the `snmp-master-agent.conf` file, change the community name. The default name is `netiq`. Changing the community name is recommended for security purpose.
- 5 Start the Master Agent by using the `net start "Net-SNMP Agent"` command.

---

**NOTE:** Ensure that you specify the command within quotes to start the Master Agent.

---

- 6 Restart the Administration Console for the changes to take effect.
- 7 If you encounter any errors while enabling monitoring, review the logs available in the `c:\Program Files(x86)\Novell\log\platform.0.log` folder.

If you are on a Windows 2008 R2 server (upgraded to Access Manager 4.0 from an Access Manager 3.x version), then enabling SNMP monitoring does not update the `platform.0.log` file.

To enable SNMP Monitoring and ensure `platform.0.log` file is updated, perform the following steps:

**7a** Stop Tomcat server

**7b** Edit the `C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\conf\platform.conf` file.

**7c** Traverse to the end of the `platform.conf` file and locate the last `</vcdnModule>` tag.

**7d** Add the following content to appear after the last `</vcdnModule>` tag

```
<vcdnModule name="snmp"
className="com.volera.vcdn.platform.snmp.SnmpAgentInit"
sequence="3">
    <stringParam name="enable" value="true"/>
    <stringParam name="masterAgentIp" value="127.0.0.1"/>
    <stringParam name="masterAgentPort" value="705"/>
</vcdnModule>.
```

Ensure that this content is placed inside the `<vcdnApplicationModule>` tag.

**7e** Start the Tomcat server.

This ensures that SNMP Monitoring is enabled on a Windows 2008 R2 server and the `platform.log` file is also updated.



---

# 5 Access Manager Appliance Logging

- ♦ [Section 5.1, “Understanding the Types of Logging,” on page 69](#)
- ♦ [Section 5.2, “Downloading the Log Files,” on page 70](#)
- ♦ [Section 5.3, “Using the Log Files for Troubleshooting,” on page 73](#)

## 5.1 Understanding the Types of Logging

Access Manager Appliance supports two types of logging:

- ♦ [Section 5.1.1, “Component Logging for Troubleshooting Configuration or Network Problems,” on page 69](#)
- ♦ [Section 5.1.2, “HTTP Transaction Logging for Proxy Services,” on page 70](#)

### 5.1.1 Component Logging for Troubleshooting Configuration or Network Problems

Each Access Manager Appliance component maintains log files that contain entries documenting the operation of the component. Component file logging records the processing and interactions between the Access Manager components that occur while satisfying user and administrative requests and during general system processing. By enabling the correct levels of logging for the various Access Manager components, an administrator can monitor how the Access Manager Appliance processes user and administrative requests. Transaction flows have been defined to help the administrator identify the processing steps that occur during the execution of specific types of user or administrative requests. All component file logs include tags and values that allow the administrator to identify and correlate which component file log entries pertain to a given transaction and user.

Component file logs are not primarily intended for debugging the software itself, although they can be used to detect software that is not behaving properly. Rather, the intent of component file logging is to document the operational processing of the Access Manager components so that system administrators and support personnel can identify and isolate problems caused by configuration errors, invalid user data, or network problems such as broken connections. However, component file logging is typically the first step in identifying software bugs.

Component file logging is more verbose than audit logging. It increases processing load, and on a day-to-day basis, it should be enabled only to log error conditions and system warnings. If a specific problem occurs, component file logging can be set to **info** or **config** to gather the information needed to isolate and repair the detected problem. When the problem is resolved, component file logging should be reconfigured to log only error conditions and system warnings.

Log files can be configured to include entries for the following events:

- ♦ Initialization and shutdown
- ♦ Configuration
- ♦ Events processed by the component, such as authentication, role assignment, resource access, and policy evaluation
- ♦ Error conditions

See “[Configuring Component Logging](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.

## 5.1.2 HTTP Transaction Logging for Proxy Services

The Access Gateway allows you to log HTTP transactions. You can log what happens with an HTTP request and response during certain times:

- ♦ Between the browser and the Access Gateway
- ♦ Between the Access Gateway and the back-end Web server

You select fields from the HTTP header of a request and these fields are logged. You can then use these logged transactions to bill customers for Web services or to troubleshoot whether a request is refused because the browser didn't send the required information or because the Access Gateway didn't send the Web server the required information.

This type of logging conforms to the W3C specification for proxy server logging in the common and extended log formats. This type of logging provides no information about the exchanges between the Access Gateway and the Identity Server. If you need to discover whether the Access Gateway is obtaining the correct information from the Identity Server for an Identity Injection or Form Fill policy, you need to turn on component logging. See “[Configuring Component Logging](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.

For HTTP transaction logging, see “[Configuring Logging for a Proxy Service](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*.

## 5.2 Downloading the Log Files

The General Logging page displays the location of the files that the Access Manager Appliance components use for logging system messages. There are some exceptions:

- ♦ **Default Auditing File:** If you have configured Novell Audit to send events to the default audit file (/var/opt/novell/naudit/logs/auditlog), this file does not appear in the list.

If you want this file to appear in this list, you must make this file readable by the novlwww user. It is a breach of Novell Audit security for Access Manager code to change the permissions on this file. You must decide whether changing its permissions and displaying the file in this list compromises your security.

To add this file in the list of files for the Administration Console, configure the following:

- ♦ Use commands similar to the following to grant the novlwww user executable permissions to the naudit directories:

```
chmod o+rx /var/opt/novell/naudit
```

```
chmod o+rx /var/opt/novell/naudit/logs
```

- ♦ Use a command similar to the following to grant the novlwww user read access to the auditlog file:

```
chmod o+r /var/opt/novell/naudit/logs/auditlog
```

- ♦ **Proxy Service Log Files:** If you enable proxy service logging, these files are not available for downloading from this page because there could be potentially hundreds of these files. If this type of logging has been enabled, the directory where they are located is displayed. For more information about this type of logging, see [“Configuring Logging for a Proxy Service”](#) in the *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*.

To view or download the log file:

- 1 In the Administration Console, click **Auditing > General Logging**.
- 2 Select one or more log files, click **Download**, then open it or save it to disk.  
You can use any text editor to view the file.

---

**NOTE:** `/var/opt/novell/nam` is the central location for all log files.

---

Each Access Manager Appliance component generates multiple log files. The following tables lists these files and the types of messages they contain.

- ♦ [Section 5.2.1, “Administration Console Logs,” on page 71](#)
- ♦ [Section 5.2.2, “Identity Server Logs,” on page 71](#)
- ♦ [Section 5.2.3, “Access Gateway Logs,” on page 72](#)
- ♦ [Section 5.2.4, “SSL VPN Server Logs,” on page 72](#)

## 5.2.1 Administration Console Logs

| Filename                                                                 | Description                                                                                                                                          |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/var/opt/novell/nam/logs/adminconsole/tomcat/catalina.out</code>   | Contains Tomcat errors.                                                                                                                              |
| <code>/var/opt/novell/nam/logs/adminconsole/volera/app_sc.0.log</code>   | Contains events related to importing devices, device configuration changes, health status changes, statistics reporting, and communication problems. |
| <code>/var/opt/novell/nam/logs/adminconsole/volera/app_cc.0.log</code>   | Contains events related to policy configuration.                                                                                                     |
| <code>/var/opt/novell/nam/logs/adminconsole/volera/platform.0.log</code> | Contains XML events for configuration changes. This log file contains very little useful information for system administrators.                      |

## 5.2.2 Identity Server Logs

| Filename                                                      | Description                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/var/opt/novell/nam/logs/idp/tomcat/catalina.out</code> | Logging to this file occurs only if you have selected the <b>Echo to Console</b> option from the <b>Identity Servers &gt; Servers &gt; Edit &gt; Logging</b> page.<br><br>When component logging has been set to info for Applications, it contains entries tracing user authentication and role assignments. |

| Filename                                 | Description                                                                                                                                                                                                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/opt/novell/nam/logs/jcc/jcc-0.log.0 | Contains the log entries for the server communications module related to interaction of the Identity Server with the Administration Console, such as imports, certificates, health checks, and configuration. |

## 5.2.3 Access Gateway Logs

| Filename                                             | Description                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/opt/novell/nam/logs/mag/tomcat/catalina.out     | Logging to this file only occurs if you have selected the <b>Echo to Console</b> option from the <b>Identity Servers &gt; Servers &gt; Edit &gt; Logging</b> page.<br><br>Check this file for entries tracing the evaluation of authorization, identity injection, and form fill policies. |
| /var/log/novell/reverse/<proxy_service-name>         | If logging is enabled on one or more reverse proxies, this directory contains the log files.<br><br>A directory is listed for each reverse proxy on which you have enabled logging.                                                                                                        |
| /var/opt/novell/nam/logs/jcc/jcc-0.log.0             | Contains the log entries for the server communications module related to interaction of the Access Gateway with the Administration Console, such as imports, certificates, health checks, and configuration.                                                                               |
| /var/opt/novell/nam/logs/mag/apache2/error_log       | This directory also contains the Apache generated log files such as the <code>error_log</code> file.                                                                                                                                                                                       |
| /var/opt/novell/nam/logs/mag/amlogging/ags_error.log | Contains the messages generated for configuration, device imports, health, and statistics. It also contains entries for the policy evaluation processes done by the Gateway Service Manager module.                                                                                        |
| /var/opt/novell/nam/logs/mag/amlogging/verbose_log   | Contains the verbose log entries.                                                                                                                                                                                                                                                          |

## 5.2.4 SSL VPN Server Logs

| Filename                                            | Description                                                                                                                                                                            |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/opt/novell/nam/logs/sslvpn/tomcat/catalina.out | Logging to this file occurs only if you have selected the <b>Echo to Console</b> option from the <b>Identity Servers &gt; Servers &gt; Edit &gt; Logging</b> page.                     |
| /var/opt/novell/nam/logs/jcc/jcc-0.log.0            | Contains the log entries for the server communications module related to interaction of the SSL VPN with the Administration Console, such as imports, certificates, and configuration. |
| /var/log/messages                                   | Contains the log entries for the Connection Manager and SOCKS servers.                                                                                                                 |



| Filename                    | Description                                                                |
|-----------------------------|----------------------------------------------------------------------------|
| /var/log/novell-openvpn.log | Contains log entries for the OpenVPN server or the Enterprise mode server. |
| /var/log/stunnel.log        | Contains log entries for Stunnel or the Kiosk mode server.                 |

## 5.3 Using the Log Files for Troubleshooting

The following sections describe the logging features available in Access Manager Appliance and provide information about how you can use them for troubleshooting problems:

- ♦ [Section 5.3.1, “Enabling Logging,” on page 73](#)
- ♦ [Section 5.3.2, “Understanding the Log Format,” on page 73](#)
- ♦ [Section 5.3.3, “Sample Authentication Traces,” on page 76](#)

For information about policy tracing, see “[Understanding Policy Evaluation Traces](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Policy Guide*.

### 5.3.1 Enabling Logging

Each Access Manager Appliance device has configuration options for logging:

**Identity Server:** Logging is turned off and must be enabled. When you enable Identity Server logging, you also enable logging for the Embedded Service Providers that are configured to use the Identity Server for authentication. For configuration information, see “[Configuring Component Logging](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.

**Embedded Service Providers:** Each Access Manager Appliance device has an Embedded Service Provider that communicates with the Identity Server. Its log level is controlled by configuring Identity Server logging.

**Access Gateway Service:** The Gateway Service logs contain the messages sent between the Gateway Service and the Embedded Service Provider and between the Gateway Service and the Web server. This type of logging is turned off and must be enabled. For information, see “[Managing Access Gateway Logs](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Access Gateway Guide*.

### 5.3.2 Understanding the Log Format

Access Manager Appliance does not have a fixed format for file log entries. However, to facilitate the use of non-interactive stream-oriented editors such as `sgrep`, `sed`, `awk`, and `grep` and to improve log entry readability, the log entries in the `catalina.out` files use some standard elements. These entries use the beginning and ending log entry tags and the log entry correlation tags. The data portion of log entries is the most flexible part. A log entry has the following fields:

```
<amLogEntry> [\n]
    time-date-stamp
    [log preamble]:
    AM#event-code:
    AMDEVICE#device-id:
    AMAUTHID#auth-id:
    AMEVENTID#event-id:
    [..additional correlating information][\n]
    [supplementary log entry data and text ... \n]
</amLogEntry> [\n]
```

Most log entries do not use the optional line breaks (`[\\n]`). Notice that the time-date-stamp, the log preamble, the correlation tags, and optional additional correlating information are on the same line so that stream-oriented editors that use only one line (such as `grep`) can be used to locate log entries that are related. The following entry is an example entry that is logged when a user has initiated a login sequence.

```
<amLogEntry> 2009-06-08T21:06:25Z INFO NIDS Application: AM#500105014:
AMDEVICEID#9921459858EAAC29: AMAUTHID#BB11C254B7521B5E836D8703826287 AF:
Attempting to authenticate user cn=jwilson,o=novell with provided credentials. </
amLogEntry>
```

**Table 5-1** Fields in a Log Entry

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Beginning, ending tags             | The <code>&lt;amLogEntry&gt;</code> and <code>&lt;/amLogEntry&gt;</code> tags mark the beginning and the end of a log entry. These tags allow stream-oriented editors to extract log entries for processing.                                                                                                                                                                                                                                                                                                                                                                                     |
| Time-date-stamp tag                | The date and time is specified in the W3C profile format of ISO 8061. It has the following fields: year-month-day-T-hour-minutes-seconds-time zone. The Z value for the time zone indicates that the time is specified in UTC.                                                                                                                                                                                                                                                                                                                                                                   |
| Log preamble                       | <p>This information is optional, and usually consists of a string indicating the logging level (such as warning, informational, or debug) and a string identifying the type of module making the entry.</p> <p>In the example log entry, the preamble has a log level and a module identifier and contains the following strings: <code>INFO NIDS Application:</code></p>                                                                                                                                                                                                                        |
| Correlation tags                   | <p>The correlation tags uniquely identify the event, the device that produced the event, and the user who requested the action. The example log entry contains the following correlation tags:</p> <pre>AM#500105014: AMDEVICEID#9921459858EAAC29: AMAUTHID#BB11C254B7521B5E836D8703826287AF:</pre> <p>For more information, see <a href="#">“Understanding the Correlation Tags in the Log Files” on page 75</a>.</p>                                                                                                                                                                           |
| Additional correlation information | <p>This information is optional and contains correlation tags and data unique to a specific type of trace. For example, a policy evaluation trace created by the Embedded Service Provider contains the following additional tags:</p> <ul style="list-style-type: none"> <li>◆ <code>NXPESID#value</code></li> <li>◆ <code>POLICYID#value</code></li> </ul> <p>The example log entry does not contain any additional correlation information. For a log entry that does, see <a href="#">“Identity Injection Traces”</a> in the <i>NetIQ Access Manager Appliance 4.0 SP1 Policy Guide</i>.</p> |
| Supplementary information          | <p>This information is optional and contains information that is specific to the log entry. It can be as simple as an informational string, such as the string in the example log entry:</p> <pre>Attempting to authenticate user cn=jwilson,o=novell with provided credentials.</pre> <p>The supplementary information can have a very specific format. For an example and explanation of the policy trace information, see <a href="#">“Understanding Policy Evaluation Traces”</a> in the <i>NetIQ Access Manager Appliance 4.0 SP1 Policy Guide</i>.</p>                                     |

## Understanding the Correlation Tags in the Log Files

There is no fixed field format for log file entries. However, because most requests handled by Access Manager Appliance are processed by multiple Access Manager Appliance components, there is a mechanism that facilitates the correlation of log entries for a single Access Manager Appliance request in the various component log files. A correlation tag has the following general format:

`<tag name>#<tag value>:`

The `<tag name>` is a fixed value, defined in the Format column of [Table 5-2](#). It is always terminated by the `#` character. The `<tag value>` immediately follows the `#` character and is always terminated by the `:` character. The `<tag value>` is not a fixed value, but a uniquely assigned value to identify an event, a user, or a transaction. [Table 5-2](#) lists the defined correlation tags:

**Table 5-2** Correlation Tags

| Type       | Format           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Event code | AM#<Event-Code>: | An event number defined in <a href="#">NetIQ Access Manager Appliance 4.0 SP1 Event Codes</a> . This tag is included in all log entries that record an event and in all events that are presented to the user as an informational or error page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| User ID    | AMAUTHID#<ID>:   | <p>An authentication identifier that the Identity Server or the Embedded Service Provider (ESP) assigns to each authenticated user. This tag is included in all entries that pertain to a request made by an authenticated user.</p> <p>Currently the Identity Server and ESP assign different authentication IDs. When correlating the flow of events between the Identity Server and the ESP for an authentication sequence, you can use the event code of the authentication events and find the artifact that the ESP and the Identity Server exchange.</p> <p>In the <code>catalina.out</code> file of the Identity Server, search for AM#500105018 events. This is the event that sends the artifact to the ESP. Search for a corresponding artifact in the Access Gateway log. Events AM#500105020 and AM#500105021 contain the artifact value.</p> |
| Device ID  | AMDEVICE#<ID>    | <p>An identifier that uniquely identifies the Access Manager Appliance device that is generating the log entry.</p> <p>You can view the identifier that is assigned to each device on the General Logging page in the Administration Console (click <b>Auditing &gt; General Logging</b>). The ID begins with a prefix that identifies the type of device such as <code>idp</code> for Identity Server, <code>ag</code> for an Access Gateway, and <code>idp-esp</code> for ESP of the device. The prefix is followed by a 16-digit hexadecimal number.</p> <p>In log entries, the <code>idp</code> prefix is not recorded. For example, the General Logging page displays <code>idp-AA257DA77ED48DB0</code> for the ID of the Identity Server, but in the <code>catalina.out</code> file, the value is <code>AMDEVICE#AA257DA77ED48DB0</code>.</p>        |

| Type           | Format           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transaction ID | AMEVENTID#<ID> : | <p>An identifier assigned to each Access Manager Appliance or system administration transaction. Access Manager Appliance transactions are actions such as authenticating a user, processing a request for access to a resource, and federating an identity.</p> <p>If a user requests access to multiple resources, each request is given a separate transaction ID. When the Access Gateway evaluates a policy for a protected resource page and the page contains links, the policy is evaluated for each link, and each of these evaluations generates a new transaction ID.</p> <p>System administration transactions are actions such as importing a device, deleting a device, stopping or starting a device, and configuring or modifying the configuration of a device.</p> |

## Sample Scenario

The following scenario illustrates how these tags can be used. A user receives an error page indicating that the user has been refused access to a protected resource. The error page contains an event code. The user contacts the system administrator and reports the event code contained in the message. The code displayed to the user includes both an event number and an identifier indicating the device detecting the error, for example, 300101023-92E1B234. The 300101023 value is the event number and 92E1B234 is the device identifier. The device identifier is the number assigned to the Access Manager Appliance device reporting the error. You can make a textual search of log entries using the tags and values AM#300101023: and AMDEVICEID#92E1B234: to locate candidate log entries of the target Access Manager Appliance transaction flow. When the desired log entry is found, the AMEVENTID# tag and value and the AMAUTHID# tag (assuming the user has been authenticated) from the log entry can be used to locate all other log entries pertaining to the user in the context of the transaction.

### 5.3.3 Sample Authentication Traces

An authentication trace is logged to the `catalina.out` file of the Identity Server that authenticates the user. If the Access Gateway initiates the authentication because of a user request to a protected resource, the Embedded Service Provider log file of the Access Gateway also contains entries for the authentication sequence. Identity Server logging must be enabled to produce authentication traces (see [“Configuring Component Logging”](#) in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*).

This section describes the following types of authentication traces:

- ♦ [“Direct Authentication Request to the Identity Server” on page 77](#)
- ♦ [“Protected Resource Authentication Trace” on page 79](#)

## Direct Authentication Request to the Identity Server

The following trace is an example of a user logging directly into the Identity Server to access the end user portal. The log entries are numbered, so that they can be described.

```
1. <amLogEntry> 2009-06-14T17:14:30Z INFO NIDS Application: AM#500105015:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Processing
login request with TARGET = http://10.10.15.19:8080/nidp/app, saved TARGET = . </
amLogEntry>

2. <amLogEntry> 2009-06-14T17:14:30Z INFO NIDS Application: AM#500105009:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Executing
contract Name/Password - Form. </amLogEntry>

3. <amLogEntry> 2009-06-14T17:14:30Z INFO NIDS Application: AM#500105010:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Contract
Name/Password - Form requires additional interaction. </amLogEntry>

4. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500105015:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Processing
login request with TARGET = http://10.10.15.19:8080/nidp/app, saved TARGET = http://
/10.10.15.19:8080/nidp/app. </amLogEntry>

5. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500105009:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Executing
contract Name/Password - Form. </amLogEntry>

6. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500105014:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: Attempting
to authenticate user cn=bcf,o=novell with provided credentials. </amLogEntry>

7. <amLogEntry> 2009-06-14T17:14:39Z WARNING NIDS Application: Event Id: 3014666,
Target: cn=bcf,o=novell, Sub-Target: F35A3C7AD7F2EEDEB3D17F99EC3F39D1, Note 1:
Local, Note 2: This Identity Provider, Note 3: name/password/uri, Numeric 1: 0 </
amLogEntry>

8. <amLogEntry> 2009-06-14T17:14:39Z WARNING NIDS Application: Event Id: 3015456,
Note 1: F35A3C7AD7F2EEDEB3D17F99EC3F39D1, Note 2: Manager, Note 3:
Document=(ou=xpemplPEP,ou=mastercdn,ou=Content
PublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_Root,ou=accessManag
erContainer,o=novell:romaContentCollectionXMLDoc),Policy=(Manager),Rule=(1::RuleID
_1181251958207),Action=(AddRole::ActionID_1181252224665), Numeric 1: 0 </
amLogEntry>

9. <amLogEntry> 2009-06-14T17:14:39Z WARNING NIDS Application: Event Id: 3015456,
Note 1: F35A3C7AD7F2EEDEB3D17F99EC3F39D1, Note 2: authenticated, Note 3: system-
generated-action, Numeric 1: 0 </amLogEntry>

10. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500199050:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: IDP
RolesPep.evaluate(), policy trace:
~~RL~1~~~Rule Count: 1~~Success(67)
~~RU~RuleID_1181251958207~Manager~DNF~~1:1~~Success(67)
~~CS~1~~ANDs~~1~~True(69)
~~CO~1~LdapGroup(6645):no-param:hidden-value:~ldap-group-is-member-
of~SelectedLdapGroup(6645):hidden-param:hidden-value:~~~True(69)
~~PA~ActionID_1181252224665~~AddRole~Manager~~~Success(0)
~~PC~ActionID_1181252224665~~Document=(ou=xpemplPEP,ou=mastercdn,
```

```
ou=ContentPublisherContainer,ou=Partition,ou=PartitionsContainer,ou=VCDN_Root,ou=a
ccessManagerContainer,o=novell:romaContentCollectionXMLDoc),Policy=(Manager),Rule=
(1::RuleID_1181251958207),Action=(AddRole::ActionID_118125224665)~AdditionalRole(
6601):unknown():Manager:~~~Success(0)
</amLogEntry>
```

```
11. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500105013:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1:
Authenticated user cn=bcf,o=novell in User Store Local Directory with roles
Manager,authenticated. </amLogEntry>
```

```
12. <amLogEntry> 2009-06-14T17:14:39Z INFO NIDS Application: AM#500105017:
AMDEVICEID#9921459858EAAC29: AMAUTHID#F35A3C7AD7F2EEDEB3D17F99EC3F39D1: nLogin
succeeded, redirecting to http://10.10.15.19:8080/nidp/app. </amLogEntry>
```

**Table 5-3** Log Entry Descriptions for an Authentication Trace from an Identity Server

| Entry | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Indicates that a login request is in process. This is the first entry for a login request. The requester, even though login has not been successful, is assigned an authentication ID. You can use this ID to find the log entries related to this user. The entry also specifies the URL of the requested resource, in this case the /nidp/app resource called the End User Portal. The saved TARGET message does not contain a value, so this step will be repeated. |
| 2     | Specifies the contract that is being used to perform the login.                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3     | Indicates that the contract requires interaction with the user.                                                                                                                                                                                                                                                                                                                                                                                                        |
| 4     | Indicates that the a login request is in process. The saved TARGET message contains a value, so the required information has been gathered to start the authentication request. The AM# correlation tag is AM#500105015, which is the same value as the first log entry.                                                                                                                                                                                               |
| 5     | Indicates that an exchange is occurring between the client and the Identity Server to obtain the required credentials. Each contract requires a different exchange. The AM# correlation tag is AM#500105009, which is the same value as the second log entry.                                                                                                                                                                                                          |
| 6     | Provides the DN of the user attempting to log in and indicates that the user's credentials are being sent to the LDAP server for verification.                                                                                                                                                                                                                                                                                                                         |
| 7     | Provides information about an auditing event. If you have not enabled auditing or you have not selected the login events, this entry does not appear in your log file. This event contains information about who is logging in and the contract that is being used.                                                                                                                                                                                                    |
| 8     | Provides information about an auditing event. If you have not enabled auditing or you have not selected the login events, this entry does not appear in your log file. This event contains information about the Manager policy that is evaluated during login.                                                                                                                                                                                                        |
| 9     | Provides information about an auditing event. If you have not enabled auditing or you have not selected the login events, this entry does not appear in your log file.                                                                                                                                                                                                                                                                                                 |
| 10    | Contains the entry for processing a Role policy. When a user logs in, all Role policies are evaluated and the user is assigned any roles that the user has the qualifications for. For more information, see <a href="#">“Understanding Policy Evaluation Traces”</a> in the <i>NetIQ Access Manager Appliance 4.0 SP1 Policy Guide</i> .                                                                                                                              |
| 11    | Contains a summary of who logged in from which user store and the names of the Role policies that successfully assigned roles to the user.                                                                                                                                                                                                                                                                                                                             |
| 12    | Contains the final results of the login, with the URL that the request is redirected to.                                                                                                                                                                                                                                                                                                                                                                               |

## Protected Resource Authentication Trace

When a protected resource is configured to require authentication, both the Identity Server and the Embedded Service Provider of the Access Gateway generate log entries for the process. The following sections explain how to correlate the entries from the logs.

- ♦ [“Entries from an Identity Server Log” on page 79](#)
- ♦ [“Entries from an Access Gateway Log” on page 80](#)
- ♦ [“Correlating the Log Entries between the Identity Server and the Access Gateway” on page 80](#)

### Entries from an Identity Server Log

```
<amLogEntry> 2009-07-31T17:36:39Z INFO NIDS Application: AM#500105016:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Processing  
login resulting from Service Provider authentication request. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:39Z INFO NIDS Application: AM#500105009:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Executing  
contract Name/Password - Form. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:39Z INFO NIDS Application: AM#500105010:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Contract  
Name/Password - Form requires additional interaction. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105016:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Processing  
login resulting from Service Provider authentication request. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105009:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Executing  
contract Name/Password - Form. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105014:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Attempting  
to authenticate user cn=admin,o=novell with provided credentials. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105012:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67:  
Authenticated user cn=admin,o=novell in User Store Internal with no roles. </  
amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105018:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#83778AE09DCA5A35B57842D754A60D67: Responding  
to AuthnRequest with artifact AAMoz+rm2jQjDSHjea8U9zm3Td/U2ax0YZCo/  
qBNool8WkZiTct7N7Jx </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:36:49Z INFO NIDS Application: AM#500105019:  
AMDEVICEID#AA257DA77ED48DB0: AMAUTHID#C2D8D52704918AF2D5D62F6EDC2FFAC6: Sending  
AuthnResponse in response to artifact AAMoz+rm2jQjDSHjea8U9zm3Td/U2ax0YZCo/  
qBNool8WkZiTct7N7Jx </amLogEntry>
```

## Entries from an Access Gateway Log

```
<amLogEntry> 2009-07-31T17:35:05Z INFO NIDS Application: AM#500105005:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Processing proxy request for login using contract name/password/uri and return url
http://jwilson.provo.novell.com/ </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:35:05Z INFO NIDS Application: AM#500105015:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Processing login request with TARGET = http://jwilson.provo.novell.com/, saved
TARGET = . </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:35:05Z INFO NIDS Application: AM#500105009:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Executing contract IDP Select. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:35:05Z INFO NIDS Application: AM#500105010:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Contract IDP Select requires additional interaction. </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:35:15Z INFO NIDS Application: AM#500105020:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Received and processing artifact from IDP - AAMoz+rm2jQjDSHjea8U9zm3Td/U2ax0YZCo/
qBNool8WkZiTct7N7Jx </amLogEntry>
```

```
<amLogEntry> 2009-07-31T17:35:15Z INFO NIDS Application: AM#500105021:
AMDEVICEID#esp-2FA73CE1A376FD91: AMAUTHID#C6D119FD93EEBBEBEC50BEB27B9E2832:
Sending artifact AAMoz+rm2jQjDSHjea8U9zm3Td/U2ax0YZCo/qBNool8WkZiTct7N7Jx to URL
http://jwilson1.provo.novell.com:8080/nidp/idff/soap at IDP </amLogEntry>
```

## Correlating the Log Entries between the Identity Server and the Access Gateway

You can see that these two trace sequences are for the same authentication request because the artifact (AAMoz+rm2jQjDSHjea8U9zm3Td/U2ax0YZCo/qBNool8WkZiTct7N7Jx) that is exchanged is the same. You can use the AMAUTHID in each file to search for other requests that this user has made.

To associate a distinguished name with the AMAUTHID, use the catalina.out file of the Identity Server. Event AM#500105014 contains the DN of the user.



---

# 6 Changing the IP Address of an Access Manager Appliance

---

**NOTE:** Changing the primary IP Address of an Access Manager Appliance is not recommended. This may result in corruption of the configuration store. However, you can modify the Listening IP address of Reverse Proxy or the Outbound IP address used to communicate with the Web Server.

---

To modify the Listening IP Address or Outbound IP address, do the following:

- 1 In the Administration Console, click **Devices > Access Gateways** > Select the device > **New IP** > click **OK**.
- 2 Add the secondary IP address if applicable to the interfaces from **Network Settings > Adapter List**.
- 3 Configure the DNS from **Network Settings > DNS**.
- 4 Add the Host entries (if any) from **Network Settings > Hosts**.
- 5 Set up the routing (if any) from **Network Settings > Gateways**.
- 6 Under Services, click on **Reverse Proxy/Authentication**. In the Reverse Proxy List, click the proxy service name. Select the newly added cluster member and select the listening IP address for that service.
- 7 (Optional) If you want to specify the outbound connection to the Web server, click **Web Servers**, then click **TCP Connect Options**. Select the **Cluster Member** and select the IP address from the drop down list against **Make Outbound Connection Using** if you want to select the outbound IP address to communicate with the Web server.

To modify the IP address of the Audit Server:

- 1 In the Administration Console, click **Auditing > Novell Auditing**.
- 2 On the Novell Auditing page, change the IP address for the server and, if necessary, the port.
- 3 Click **OK**.
- 4 Update all Access Gateways.
- 5 Reboot all servers, including the Access Gateways, to use the new configuration.



---

# 7 Code Promotion

Code Promotion is an easy to use secure functionality to move the configuration data of Access Manager from one environment to another. It allows you to export the configuration data as a password-protected encrypted file. You can then import this file into another Access Manager system and seamlessly replicate the configuration into the target system.

The exported configuration data includes generic Identity Server cluster configuration and policy configuration. It is independent of the device specific data and network specific data. Hence, you can use the Code Promotion feature to promote configuration between two Access Manager systems that are in different networks, with different number of devices, and with different user stores. The Access Manager systems must be on the same platform.

- ♦ [Section 7.1, “How Code Promotion Helps?,” on page 83](#)
- ♦ [Section 7.2, “Use Cases,” on page 84](#)
- ♦ [Section 7.3, “Code Promotion Mechanism,” on page 84](#)
- ♦ [Section 7.4, “Sequence of Promoting the Configuration Data,” on page 85](#)
- ♦ [Section 7.5, “Prerequisites,” on page 85](#)
- ♦ [Section 7.6, “Limitations,” on page 86](#)
- ♦ [Section 7.7, “Exporting the Configuration Data by Using Code Promotion,” on page 86](#)
- ♦ [Section 7.8, “Importing the Configuration Data by Using Code Promotion,” on page 88](#)
- ♦ [Section 7.9, “Exporting the Access Gateway Configuration Data,” on page 90](#)
- ♦ [Section 7.10, “Importing the Access Gateway Configuration Data,” on page 90](#)
- ♦ [Section 7.11, “Troubleshooting,” on page 92](#)

## 7.1 How Code Promotion Helps?

Code Promotion addresses the following pain points associated with the following activities:

- ♦ **Managing Multiple Access Manager Setups:** Typically, multiple Access Manager setups are maintained to test configuration changes before applying them on production systems. For example, you can use the staging environment to deploy Access Manager, test various configurations and customizations, and apply these changes to the production environment. Earlier, there was no easy way to promote the tested and approved configuration data to the production environment. The configuration data had to be manually replicated in to another system. This was a time-consuming and error prone process. Code Promotion provides a mechanism to move the configuration data across environments. This increases efficiency, improves productivity, and in turn reduces costs of managing configurations across environments.
- ♦ **Different Administrators for Different Setups:** Different administrators can manage different Access Manager environments. Manually replicating the configuration to the different stages requires the maintenance of the precise list of all changes done on one system and this knowledge must be transferred among administrators. Hence, a mechanism is needed to ensure that all configuration changes are taken and moved correctly.

- ♦ **Replacing or Moving Physical Devices:** You may need to replace physical devices or you may need to move devices to a different network due to a business decision, such as, changing a network infrastructure vendor. Hence, a mechanism that is independent of these network changes is needed to transfer the configuration data.

## 7.2 Use Cases

Code Promotion simplifies promotion of the configuration data in the following scenarios:

- ♦ You want to test your configuration in a dedicated testing environment and then build a new production environment based on the tested configurations.
- ♦ You maintain multiple test environments and you want the configuration changes to pass through these stages before deploying the configuration data to an existing production environment.
- ♦ You want to move your application to another physical server.
- ♦ You want to move the application hardware to a different network infrastructure.

## 7.3 Code Promotion Mechanism

[Table 7-1](#) lists the configurations that you can promote to another environment and the corresponding promotion mechanism.

**Table 7-1** Configuration Promotion Mechanism

| Data                                      | Promotion Supported? | Mechanism                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identity Server configuration             | Yes                  | Use the Code Promotion feature.<br><br>For more information, see <a href="#">Section 7.7, “Exporting the Configuration Data by Using Code Promotion,” on page 86</a> and <a href="#">Section 7.8, “Importing the Configuration Data by Using Code Promotion,” on page 88</a> .                         |
| Policies configurations                   | Yes                  | Use the Code Promotion feature.<br><br>For more information, see <a href="#">Section 7.7, “Exporting the Configuration Data by Using Code Promotion,” on page 86</a> and <a href="#">Section 7.8, “Importing the Configuration Data by Using Code Promotion,” on page 88</a> .                         |
| Certificates and Keystores configurations | Yes                  | Use the Code Promotion feature.<br><br>For more information, see <a href="#">Section 7.7, “Exporting the Configuration Data by Using Code Promotion,” on page 86</a> and <a href="#">Section 7.8, “Importing the Configuration Data by Using Code Promotion,” on page 88</a> .                         |
| Access Gateway configurations             | Yes                  | Use the existing Access Gateway Export and Import Configuration feature.<br><br>For more information, see <a href="#">Section 7.9, “Exporting the Access Gateway Configuration Data,” on page 90</a> and <a href="#">Section 7.10, “Importing the Access Gateway Configuration Data,” on page 90</a> . |

| Data                  | Promotion Supported? | Mechanism                                                                                                                                           |
|-----------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Device customizations | No                   | Manually export and import the data.<br><br>For more information, see <a href="#">Section 7.8.3, “Post-Import Configuration Tasks,” on page 89.</a> |
| Device information    | No                   | Not applicable as devices are specific to a setup.                                                                                                  |

## 7.4 Sequence of Promoting the Configuration Data

You must promote the configuration data in the following sequence:

1. Identity Server configurations, policies configurations, and Certificates and Keystores configurations
2. Access Gateway configurations

Promoting the configuration data consists of the following steps:

1. Install Access Manager 4.0 or upgrade the prior version of Access Manager on your source and target systems.  
  
For more information about how to install Access Manager, see [NetIQ Access Manager Appliance 4.0 SP1 Installation Guide](#).  
  
For more information about how to upgrade and migrate Access Manager, see [NetIQ Access Manager 4.0 SP1 Migration and Upgrade Guide](#).
2. Export the Identity Server configuration and Policy configuration by using the Code Promotion feature from the source system.  
  
For more information, see [Section 7.7, “Exporting the Configuration Data by Using Code Promotion,” on page 86.](#)
3. Export the Access Gateway configuration from the source system.  
  
For more information, see [Section 7.9, “Exporting the Access Gateway Configuration Data,” on page 90.](#)
4. Import the Identity Server configuration and Policy configuration by using the Code Promotion feature on the target system.  
  
For more information, see [Section 7.8, “Importing the Configuration Data by Using Code Promotion,” on page 88.](#)
5. Import the Access Gateway configuration into the target system. For more information, see [Section 7.10, “Importing the Access Gateway Configuration Data,” on page 90.](#)

## 7.5 Prerequisites

- ♦ The source server and the target server must have Access Manager 4.0. If you want to export the configuration data from an earlier version of Access Manager into Access Manager 4.0, you must upgrade or migrate the existing setup to Access Manager 4.0. For more information about how to upgrade or migrate Access Manager, see the [NetIQ Access Manager 4.0 SP1 Migration and Upgrade Guide](#).
- ♦ The source server and the target server must run on the same operating system.

- ♦ The source server and the target server must have the same model; that is, both must be either Access Manager or Access Manager Appliance.
- ♦ Importing configuration data replaces the existing configuration data. Hence, use the backup option in the Import wizard to preserve a copy of the existing configuration before an import.

## 7.6 Limitations

- ♦ Code Promotion supports export and import of only the Identity Server configuration and policy configuration data.
- ♦ Code Promotion supports export and import of only the generic configuration data. It does not support exporting and importing the configuration data that vary from one system to another. For example, you can export and import network specific configuration, device specific configuration, configuration store, and its replica ring configuration.
- ♦ You can enable this feature only on the primary Administration Console.

## 7.7 Exporting the Configuration Data by Using Code Promotion

The Code Promotion page displays a list of all configuration files exported from that system. It displays the metadata of each exported configuration: date of export, configuration exported, name of user who exported, a link to download the exported file, and the comments.

You can download the previously exported configuration files from this page. These exported files are also saved on the primary Administration Console system at the following location:

```
/var/opt/novell/novlwww/namconfig
```

You as an administrator can delete or back up these files if needed. If these files are deleted from the disk, they will no longer be listed on the Code Promotion page.

| Access Manager ▼                            | Devices ▼                    | Policies ▼        | Auditing ▼               | Security                                        |
|---------------------------------------------|------------------------------|-------------------|--------------------------|-------------------------------------------------|
| <b>Code Promotion</b>                       |                              |                   |                          |                                                 |
| Code Promotion                              |                              |                   |                          |                                                 |
| Export Configuration   Import Configuration |                              |                   |                          |                                                 |
| Date of Export                              | Configuration Exported       | Exported By       | Action                   | Comments                                        |
| <b>Configuration Exports</b>                |                              |                   |                          |                                                 |
| Oct 21, 2013 10:41 AM                       | 2 Identity Provider Clusters | cn=admin,o=novell | <a href="#">Download</a> | Auto backup created during configuration import |
| Oct 18, 2013 09:52 AM                       | 1 Identity Provider Cluster  | cn=admin,o=novell | <a href="#">Download</a> | Auto backup created during configuration import |
| Close                                       |                              |                   |                          |                                                 |

The exported configuration data includes:

- ♦ Identity Server configuration
  - ♦ Cluster configuration
  - ♦ Shared Settings

- ♦ Keystores
- ♦ Trusted roots
- ♦ Policy configuration
  - ♦ All policy containers
  - ♦ All policy definitions
  - ♦ Policy extensions

Perform the following steps to export the configuration data:

- 1 Log in to the Administration Console from where you want to export the configuration data.
- 2 In the Administration Console, click **Access Manager > Code Promotion**.
- 3 In the Code Promotion page, click **Export Configuration**.

### Export Configuration

#### Configuration to Export

- ☒ Identity Server Configurations [All Clusters and Shared Settings]
- ☒ Policy Configurations [All IDP policies, AG policies and All Policy Containers]

#### Export Settings

Specify a password to encrypt the exported configuration file (optional)

Encryption Password:

Confirm Encryption Password:

Comments:

OK

Cancel

- 4 Based on your requirements, select the configuration to export:

**Identity Provider Configuration:** This will export all clusters, shared settings, keystores, and trust stores.

**Policy Configuration:** This will export all the policy containers, policy definitions, and policy extensions.

- 5 Specify a password to encrypt the archived configuration data file.

You require this password to decrypt the ZIP file while importing configuration data into another environment.

- 6 Add an appropriate comment for this export in **Comments**. This can be helpful to identify the exported configuration.

For example, Configuration export after UAT completion.

- 7 Click **OK** and save the file at your preferred location on your local system.

## 7.8 Importing the Configuration Data by Using Code Promotion

Import the configuration data only on the primary Administration Console.

Perform the following procedure to import configuration data:

- 1 Ensure that the ZIP file containing the configuration data that you want to import is accessible.
- 2 Log in to the Administration Console from where you want to import the configuration data.
- 3 In the Administration Console, click **Access Manager > Code Promotion**.
- 4 In the Code Promotion page, click **Import Configuration**.

Import Configuration

Step 1 of 3: Upload configuration file to import

Configuration

File To Import:

Browse...

Decryption Password:

Import Settings

☒ Import Identity Server Configuration

☒ Import Policies

☒ Import Identity Server Policies Only

☐ Import All Policy Containers and All Policies

Backup Settings

Always enable the configuration backup option. This will help in rolling back the changes if needed.

☒ Backup current configuration before import

(Note: Backed up configuration will be encrypted using the password specified above.)

<< Back

Next >>

Cancel

### 7.8.1 Upload Configuration File to Import

Perform the following steps to upload the configuration file to import.

- 1 Click **Browse** to import the configuration file.
- 2 In **Decryption Password**, specify the password that you used to encrypt the configuration data file. You need this password to extract the contents of the configuration file.
- 3 (Optional) Select **Backup current configuration before import**. This backup helps to roll back your changes if needed. The backup file is encrypted with the same password that is used for decryption in [Step 2](#). You can download this backup file from the Code Promotion page.



- 4 Under **Import Settings**, select the desired options based on your requirements.

---

**NOTE:** Importing Identity Server Configuration overwrites the existing Shared Settings on the system with new Shared Settings. However, these will not be deleted.

---

The following table lists examples with Attribute Sets illustrating the import action:

| Imported Attribute Sets    | Existing Attribute Sets                       | Import Action                                                               |
|----------------------------|-----------------------------------------------|-----------------------------------------------------------------------------|
| OIOSAML with five mappings | OIOSAML with two mappings                     | OIOSAML set is replaced with the imported one. Hence, it has five mappings. |
| AttrSet1                   | Not available                                 | AttrSet1 is added.                                                          |
| No import                  | AttrSet2 is defined only in the target system | AttrSet2 remains unchanged.                                                 |

- 5 Click **Next**. Go to [Section 7.8.2, “Configuring Identity Server Clusters to Import,”](#) on page 89.

## 7.8.2 Configuring Identity Server Clusters to Import

If you selected **Import Identity Provider Clusters** in [Step 4](#), the Import Identity Provider Clusters page allows you to specify the import action for each cluster found in the imported configuration.

Perform the following steps to configure the IDP clusters to import.

- 1 Select a cluster to configure import settings in **Clusters To Import**.
- 2 Select an action for the selected cluster from **Import Action**. The following options may be available:

**Import As New Cluster:** Select this option if you want to import the cluster as a new cluster. Specify **New Cluster Name** and **New Cluster URL**. Ensure that the new cluster name is different from the existing cluster names defined on that system.

**Overwrite Existing Cluster:** Select this option if you want to overwrite the existing cluster with the selected cluster. Specify which **Cluster To Overwrite**.

---

**NOTE:** You need to configure import action for each cluster separately. If the cluster you want to import has only one user store, it will be mapped to the default user store of the existing cluster. If the cluster you are importing has multiple user stores, then you must specify how to map them to the user stores of the existing cluster.

---

- 3 Click **Next**. Go to [Section 7.8.3, “Post-Import Configuration Tasks,”](#) on page 89.

## 7.8.3 Post-Import Configuration Tasks

When import is done, the final page displays the status of the import operation. After importing the Identity Server configuration data, you must perform configurations that are specific to the target system and that are not part of the exported data.

- ♦ After the import process is complete, the system displays a list of certificates that you need to create manually. Identity Server key stores are imported, but you must create the certificates referenced in them on the server where you have imported the configuration data. The new

certificate name must exactly match with the names listed. For more information about how to create certificates, see “[Creating Certificates](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Administration Console Guide*.

- ♦ Configure user stores for the newly added clusters. After the import process is complete, the system displays a list of Identity Server clusters for which you need to configure user stores. A place holder user store entry will be created. You must enter the IP address, search context, and the password for the target system user stores. For more information, see “[Configuring Identity User Stores](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.
- ♦ Distribute the policy extension JARs to devices in the Administration Console under **Policy > Extensions**. For more information, see “[Distributing a Policy Extension](#)” in the *NetIQ Access Manager Appliance 4.0 SP1 Policy Guide*.
- ♦ Update service providers with the new metadata. (Conditional)  
The identity provider certificate is different in the exported and imported systems. Hence, you must re-import the identity provider metadata to all service providers in that cluster for federation to work. For more information, see “[Viewing and Reimporting a Trusted Provider’s Metadata](#)” in the *NetIQ Access Manager Appliance 4.0 Identity Server Guide*.
- ♦ Copy customization files from the exported setup into the devices in this setup. This includes the Identity Server custom Authorization classes, custom JSP files, and so forth.
- ♦ Persistent federation identities and shared secrets are not imported. These are to be shared between the Identity Servers in your exported setup and service providers only. They do not apply to the Identity Servers in the imported system. You must configure these on the server after you import the configuration data.
- ♦ Update Identity Server devices in the modified clusters. Go to **Auditing > Troubleshooting > Certificates** and click **Re-push certificates** and then update all devices in the cluster.

## 7.9 Exporting the Access Gateway Configuration Data

- 1 In the Administration Console, click **Devices > Access Gateway > [Name of Access Gateway]**.
- 2 Click **Configuration > Export**.
- 3 (Conditional) If you want to encrypt the file, specify the following details:  
**Password protect:** Select this option to encrypt the file.  
**Password:** Specify a password to encrypt the file. You require the same password during decrypting the file on the target system.
- 4 Click **OK**, then select to save the configuration to a file.  
The filename is the name of the Access Gateway with an `.xml` extension.
- 5 Click **Export** and modify the proposed filename if needed.
- 6 Copy the Access Gateway configuration file to a place accessible by the target system.

## 7.10 Importing the Access Gateway Configuration Data

- 1 Verify that the Access Gateway meets the conditions for an import:
  - ♦ The Access Gateway should not be a member of a cluster. If it is a member of a cluster, remove it from the cluster before continuing.  
In the Administration Console, click **Devices > Access Gateways**, select the Access Gateway, then click **Actions > Remove from Cluster**.

You can create a cluster and add this machine to the cluster as the primary server after you have completed the import.

- ♦ Delete reverse proxies if any configured.

In the Administration Console, click **Devices > Access Gateways > Edit > Reverse Proxies / Authentication**. In the **Reverse Proxy List**, select **Name**, then click **Delete**. Update the Access Gateway and the Identity Server.

- 2 Click **Access Gateways > [Name of Access Gateway] > Configuration > Import**.
- 3 Browse to the location of the configuration file, select the file, enter the password if you specified while exporting the configuration, then click **OK**.
- 4 When the configuration import has finished, verify the configuration for your reverse proxies.
  - 4a Click **Access Gateways > Edit > [Name of Reverse Proxy]**.
  - 4b Verify the listening address.

This is important if your Access Gateway has multiple network adapters. By default, the IP address of eth0 is always selected as the listening address.
  - 4c Verify the certificates assigned to the reverse proxy.

The Subject Name of the certificate should match the published DNS name of the primary proxy service in the **Proxy Service List**.
  - 4d Verify the Web Server configuration. In the **Proxy Service List**, click the **Web Server Addresses** link. Check the following values:
    - ♦ **Web Server Host Name**: If this name has a staging prefix or suffix, remove it.
    - ♦ **IP addresses in the Web Server List**: If the IP addresses in the production area are different from the IP addresses in the staging area, modify the IP addresses to match the production area.
    - ♦ **Certificates**: If you have configured SSL or mutual SSL between the proxy service and the Web servers, configure the **Web Server Trusted Root** and **SSL Mutual Certificate** options. The export and import configuration option does not export and import certificates.
  - 4e Click **OK > OK**.
- 5 (Conditional) If you have multiple reverse proxies, repeat [Step 4](#) for each proxy service.
- 6 On the Configuration page, click **Reverse Proxy / Authentication**, then select the **Identity Server Cluster** configuration.
- 7 If you have multiple reverse proxies, verify that the Reverse Proxy value in the **Embedded Service Provider** section is the reverse proxy you want to use for authentication, then click **OK** twice.
- 8 Click **Access Gateways > Update**.
- 9 Click **Identity Servers > Update**.

If your Identity Server does not prompt you for an update, complete the following steps to trigger the update:

  - 9a In the Administration Console, click **Devices > Access Gateways > Edit > Reverse Proxy / Authentication**.
  - 9b Set the **Identity Server Cluster** field to **None**, then click **OK**.
  - 9c Click **Reverse Proxy / Authentication**.
  - 9d Set the **Identity Server Cluster** field to the correct value, then click **OK**.
  - 9e Update the Access Gateway.
  - 9f Update the Identity Server.

**10** Configure the keystores for the Access Gateway.

If you have configured the Access Gateway for SSL between the Identity Server and the Access Gateway and between the Access Gateway and the browsers, verify that the trust stores and the keystores contain the correct certificates.

**10a** In the Administration Console, click **Security > Certificates**.

**10b** Find the certificate for the Access Gateway.

The subject name of this certificate should match the DNS name of the Access Gateway. If this certificate is not in the list, you need to create it or import it.

This certificate should be in use by the ESP Mutual SSL and Proxy Key Store of the Access Gateway.

**10c** If the certificate is not in use by the required keystores, select the certificate, then click **Actions > Add Certificate to Keystores**.

**10d** Click the **Select Keystore** icon, select **ESP Mutual SSL** and **Proxy Key Store of the Access Gateway**, then click **OK** twice.

**11** Configure the trust stores for the Access Gateway.

**11a** In the Administration Console, click **Security > Certificates > Trusted Roots**.

The trusted root certificate of the CA that signed the Access Gateway certificate needs to be in the NIDP-truststore.

The trusted root certificate of the CA that signed the Identity Server certificate, needs to be in the ESP Trust Store of the Access Gateway.

**11b** If you need to add a trusted root to a trust store, select the trusted root, click **Add Trusted Roots to Trust Stores**.

**11c** Click the **Trust Store** icon, select the required trust store, then click **OK** twice.

**12** If you made any keystore or trust store modifications, update the Access Gateway and the Identity Server.

**13** (Optional) Create a cluster configuration and add this server as the primary server.

## 7.11 Troubleshooting

### Importing Configuration Fails

**Explanation:** While importing the configuration data, the Import Configuration wizard displays the `Configuration Import Failed` message.

**Action:** See the details of the failure the Administration Console tomcat logs at the following location:

```
/opt/novell/nam/adminconsole/logs/catalina.out
```

Collect the error details and contact the Technical Support team.

To restore your system, go to **Access Manager > Code Promotion**. You will find the backup file that was created as part of import. Download the file and then click **Import Configuration** on the same page. Re-import this backup configuration to restore to the previous configuration.

---

# 8 Troubleshooting the Administration Console

This section provides information about general troubleshooting issues found in the Administration Console:

- ♦ [Section 8.1, “Global Troubleshooting Options,” on page 93](#)
- ♦ [Section 8.2, “Logging,” on page 100](#)
- ♦ [Section 8.3, “Event Codes,” on page 100](#)
- ♦ [Section 8.4, “Restoring a Failed Secondary Console,” on page 100](#)
- ♦ [Section 8.5, “Converting a Secondary Access Manager Appliance into a Primary Appliance,” on page 101](#)
- ♦ [Section 8.6, “Repairing the Configuration Datastore,” on page 107](#)
- ♦ [Section 8.7, “Session Conflicts,” on page 107](#)
- ♦ [Section 8.8, “Unable to Log In to the Administration Console,” on page 107](#)
- ♦ [Section 8.9, “Exception Processing IdentityService\\_ServerPage.JSP,” on page 108](#)
- ♦ [Section 8.10, “Backup and Restore Failure Because of Special Characters in Passwords,” on page 108](#)
- ♦ [Section 8.11, “Unable to Install NMAS SAML Method,” on page 108](#)
- ♦ [Section 8.12, “Incorrect Audit Configuration,” on page 109](#)
- ♦ [Section 8.13, “Unable to Update the Access gateway Listening IP Address in the Administration Console Reverse Proxy,” on page 109](#)
- ♦ [Section 8.14, “During Access Manager Appliance Installation Any Error Message Should Not Display Successful Status,” on page 111](#)
- ♦ [Section 8.15, “Incorrect Health Is Reported on the Access Gateway,” on page 111](#)
- ♦ [Section 8.16, “Administration Console Does Not Refresh the Command Status Automatically,” on page 111](#)
- ♦ [Section 8.17, “SSL Communication Fails,” on page 112](#)
- ♦ [Section 8.18, “Error: Tomcat did not stop in time. PID file was not removed,” on page 112](#)
- ♦ [Section 8.19, “An IP Address for the Other Known Device Manager List is Missing in the Troubleshooting Page,” on page 112](#)
- ♦ [Section 8.20, “View Objects Do Not Function Properly in Internet Explorer 10 Default Mode,” on page 112](#)

## 8.1 Global Troubleshooting Options

The following options allow you to view the status of multiple devices and identify the devices that are not healthy.

- ♦ [Section 8.1.1, “Checking for Potential Configuration Problems,” on page 94](#)
- ♦ [Section 8.1.2, “Checking for Invalid Policies,” on page 95](#)

- [Section 8.1.3, “Checking for Version Conflicts,” on page 96](#)
- [Section 8.1.4, “Checking and Terminating User Sessions,” on page 96](#)
- [Section 8.1.5, “Checking for Invalid Policies,” on page 96](#)
- [Section 8.1.6, “Viewing Device Health,” on page 96](#)
- [Section 8.1.7, “Viewing Health by Using the Hardware IP Address,” on page 97](#)
- [Section 8.1.8, “Using the Dashboard,” on page 97](#)
- [Section 8.1.9, “Viewing System Alerts,” on page 100](#)

## 8.1.1 Checking for Potential Configuration Problems

If your Access Manager Appliance components are not behaving in the way you have configured them to run, you might want to check the system to see if any of the components have configuration or network problems.

- 1 In the Administration Console, click **Auditing > Troubleshooting > Configuration**.
- 2 All of the options should be empty, except the **Cached Access Gateway Configurations** option (see [Step 4](#)) and the **Current Access Gateway Configurations** option (see [Step 5](#)). If an option contains an entry, you need to clear it. Select the appropriate action from the following table:

| Option                                                        | Description and Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device Pending with No Commands</b>                        | If you have a device that remains in the pending state, even when all commands have successfully executed, that device appears in this list. Before deleting the device from this list, check its Command Status. If the device has any commands listed, select the commands, then delete them. Wait a few minutes. If the device remains in a pending state, return to this troubleshooting page. Find the device in the list, then click <b>Remove</b> . The Administration Console clears the pending state.                                                                                                          |
| <b>Other Known Device Manager Servers</b>                     | If a secondary Administration Console is in a non-reporting state, perhaps caused by hardware failure, its configuration needs to be removed from the primary Administration Console. As long as it is part of the configuration, other Access Manager devices try to contact it. If you cannot remove it by running the uninstall script on the secondary Administration Console, you can remove it by using this troubleshooting page. Click <b>Remove</b> next to the console that is in the non-reporting state. All references to the secondary Administration Console are removed from the configuration database. |
| <b>Access Gateways with Corrupt Protected Resource Data</b>   | If you modify the configuration for a protected resource, update the Access Gateway with the changes, then review the configuration for the protected resource and the changes have not been applied, the configuration for the protected resource is corrupted. Click <b>Repair</b> next to the protected resource that has a corrupted configuration. You should then be able to modify its configuration, and when you update the Access Gateway, the changes should be applied and saved.                                                                                                                            |
| <b>Access Gateways with Duplicate Protected Resource Data</b> | After an upgrade, if you get errors related to invalid content for policy enforcement lists, you need to correct them. The invalid elements that do not have an associated resource data element are listed in this section. Click <b>Repair</b> .                                                                                                                                                                                                                                                                                                                                                                       |

| Option                                                                           | Description and Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Gateways with Protected Resources Referencing Nonexistent Policies</b> | Protected resources have problems when policies are deleted before their references to the protected resources are removed. If you have protected resources in this condition, they are listed in this section. Click the <b>Repair</b> button to remove these references. Then verify that your protected resources have the correct policies enabled. Click <b>Access Gateways &gt; Edit &gt; [Name of Reverse Proxy] &gt; [Name of Proxy Service] &gt; Protected Resources</b> , then change to the <b>Policy View</b> .                                                                                    |
| <b>Access Gateways with Invalid Alert Profile References</b>                     | You can create XML validation errors on your Access Gateway Appliance if you start to create an alert profile (click <b>Access Gateways &gt; Edit &gt; Alerts &gt; New</b> ), but you do not finish the process. The incomplete alert profile does not appear in the configuration for the Access Gateway, so you cannot delete it. If such a profile exists, it appears in the <b>Access Gateways with Invalid Alert Profile References</b> list. Click <b>Remove</b> . You should then be able to modify its configuration, and when you update the Access Gateway, the changes should be applied and saved. |
| <b>Devices with Corrupt Data Store Entries</b>                                   | If an empty value is written to an XML attribute, the device with this invalid configuration appears in this list.<br><br>Click <b>Repair</b> to rewrite the invalid attribute values.                                                                                                                                                                                                                                                                                                                                                                                                                         |

- 3 When you have finished repairing or deleting invalid Access Gateway configurations, click the **Access Gateways** link, then click **Update > OK**.
- 4 (Optional) Verify that all members of an Access Gateway cluster have the same configuration in cache:
  - 4a Click **Auditing > Troubleshooting > Configuration**.
  - 4b Scroll to the **Cached Access Gateway Configuration** option.
  - 4c Click **View** next to the cluster configuration or next to an individual Access Gateway.  
 This option allows you to view the Access Gateway configuration that is currently residing in browser cache. If the Access Gateway belongs to a cluster, you can view the cached configuration for the cluster as well as the cached configuration for each member. The + and - buttons allow you to expand and collapse individual configurations. The configuration is displayed in XML format  
 To search for particular configuration parameters, you need to copy and paste the text into a text editor.
- 5 (Conditional) After viewing the Access Gateway configuration (see [Step 4](#)) and discovering that an Access Gateway does not have the current configuration, select the Access Gateway in the **Current Access Gateway Configurations** section, then click **Re-push Current Configuration**.

## 8.1.2 Checking for Invalid Policies

The Policies page displays the policies that are in an unusable state because of configuration errors.

- 1 In the Administration Console, click **Auditing > Troubleshooting > Policies**.  
If you have configured a policy without defining a valid rule for it, the policy appears in this list.
- 2 Select the policy, then click **Remove**.



## 8.1.3 Checking for Version Conflicts

The Version page displays all the installed components along with their currently running version. Use this page to verify that you have updated all components to the latest compatible versions. There are two steps to ensuring that your Access Manager Appliance components are running compatible versions:

To view the current version of all Access Manager Appliance devices:

- 1 In the Administration Console, click **Auditing > Troubleshooting**.
- 2 Click **Version**.

A list of the devices with their version information is displayed. If a device also has an Embedded Service Provider, the version of the Embedded Service Provider is also displayed.

## 8.1.4 Checking and Terminating User Sessions

The User Sessions page helps you to find users logged into your system and also helps to terminate their sessions if required. It displays the active user details for each Identity Server. You can search for a user with the user ID and terminate the session(s).

- 1 In the Administration Console, click **Auditing > User Sessions**.
- 2 Specify the user ID and click **Search**. If a match is found, it lists the IP address of the Identity Server and its sessions.
- 3 Click **Terminate Sessions** to terminate the sessions of the specific user.

---

**NOTE:** User details are fetched once per administration session. The last updated date is displayed. To refresh the data, click on **Refresh**.

---

For more information about user sessions, see [“Terminating an Existing Authenticated User from the Identity Server”](#) in the [NetIQ Access Manager Appliance 4.0 Identity Server Guide](#).

## 8.1.5 Checking for Invalid Policies

The Policies page displays the policies that are in an unusable state because of configuration errors.

- 1 In the Administration Console, click **Auditing > Troubleshooting > Policies**.  
If you have configured a policy without defining a valid rule for it, the policy appears in this list.
- 2 Select the policy, then click **Remove**.

## 8.1.6 Viewing Device Health

You can monitor all of the devices hosted by a server and quickly isolate and correct server issues. The system displays a status (green, yellow, white, or red) for the server.

- 1 In the Administration Console, click **Auditing > Device Health**.  
The Device Health page shows the health status by IP address of the server and lists all the devices installed on the server. The health of the least healthy device is used for the status of the server.
- 2 To view more information about the health of each device, click the IP address of the machine.



Health information can also be viewed at the following locations:

- ♦ **Access Manager > Dashboard**

The Dashboard page shows the health status at the device level. The status displayed is the status of the least healthy device.

- ♦ **Devices > [Component] > Servers**

The Servers page for each component provides a health status for each device.

## 8.1.7 Viewing Health by Using the Hardware IP Address

The Hardware IP Address page allows you to view the devices and agents managed through the selected IP address. You can monitor all of the devices hosted by a server and quickly isolate and correct server issues. The system displays statuses (green, yellow, white, or red) for the Access Manager devices.

- 1 In the Administration Console, click **Access Manager > Auditing > Device Health**.
- 2 To view information about the health of each installed device, click an IP address.
- 3 Select one of the following actions:
  - ♦ To return to the Device Health page, click **Close**.
  - ♦ To edit the details of a device, click the server name.
  - ♦ To view health details, click the **Health** icon.
  - ♦ To view the alerts, click the alerts link.
  - ♦ To view device statistics, click the statistics link.
  - ♦ To view or configure audit events for the device, click the **Edit Events** link.

## 8.1.8 Using the Dashboard

The Dashboard page is the starting point and central place to monitor and manage all product components and policies. The status of each device is available, with colored warnings or alert conditions.

- 1 In the Administration Console, click **Access Manager > Dashboard**.
- 2 Click a box to view a component or click the link to view the alerts:
  - ♦ [Identity Servers](#)
  - ♦ [Access Gateways](#)
  - ♦ [SSL VPNs](#)
  - ♦ [Policies](#)
  - ♦ [Alerts](#)

For conventions that apply to all pages in the interface, see [Section 1.2.5, “Understanding the Administration Console Conventions,”](#) on page 20.

## Identity Servers

The Identity Server is the central authentication and identity access point for all Access Manager Appliance devices. The Identity Server is responsible for authenticating users and distributing role information to facilitate authorization decisions. It also provides the Liberty Alliance Web Service Framework to distribute identity information.

An Identity Server always operates as an identity provider and can optionally be configured to run as an identity consumer (also known as a service provider), using either Liberty, SAML 1.1, or SAML 2.0 protocols. As an identity provider, the Identity Server is the central store for a user's identity information and is the heart of the user's identity federations or account linkage information. As an authentication authority, the identity provider is viewed by internal and external service providers as a trusted identity store.

In an Access Manager Appliance configuration, the Identity Server is responsible for managing the following:

- ♦ **Authentication:** Verifies user identities through various forms of authentication, both local (user supplied) and indirect (supplied by external providers). The identity information can be some characteristic attribute of the user, such as a role, e-mail address, name, or job description.
- ♦ **Identity Stores:** Stores user identities in eDirectory, Microsoft Active Directory, and Sun ONE Directory Server.
- ♦ **Identity Federation:** Enables user identity federation and provides access to Liberty-enabled services.
- ♦ **Account Provisioning:** Enables service provider account provisioning when federating, which automatically creates user accounts.
- ♦ **Custom Attribute Mapping:** Allows you to define custom attributes by mapping Liberty Alliance keywords to LDAP-accessible data, in addition to the available Liberty Alliance Employee and Person profiles.
- ♦ **SAML Assertions:** Processes and generates SAML assertions. Using SAML assertions in each Access Manager Appliance component protects confidential information by removing the need to pass user credentials between the components to handle session management.
- ♦ **Single Sign-on and Log-out:** Enables users to log in only once to gain access to multiple applications and platforms. Single sign-on and single log-out are primary features of Access Manager Appliance and are achieved after the federation and trust model is configured among trusted providers and the components of Access Manager Appliance.
- ♦ **Embedded Service Providers:** Provides authentication and identity services for the other Access Manager Appliance components. The Access Gateways and the SSL VPN server include an Embedded Service Provider that sets up a trusted relationship with the Identity Server.
- ♦ **Roles:** Provides RBAC (role-based access control) management. RBAC is used to provide a convenient way to assign a user to a particular job function or set of permissions within an enterprise to control access. The Identity Server establishes the active set of roles for a user session each time the user is authenticated. Roles can be assigned to subsets of users based on constraints outlined in a role policy. The established role can then be used in authorization policies to form the basis for granting and restricting access to particular Web resources.
- ♦ **Clustering:** Adds capacity and failover management. An Identity Server can be a member of a cluster of Identity Servers that is configured to act as a single server.

## Access Gateways

An Access Gateway provides secure access to HTTP-based Web servers by hiding the IP addresses and DNS names of the Web servers. It provides the typical security services (authorization, single sign-on, and data encryption) previously provided by Novell iChain, and is integrated with the new identity and policy services of Access Manager.

An Access Gateway works with the Identity Server to enable existing Web services for the Liberty and SAML protocols. It provides single sign-on to Web servers through Identity Injection policies that supply required user information and Form Fill policies that automatically fill in requested form information. If your Web servers have not been configured to enforce authentication and authorization, you can configure an Access Gateway to provide these services. Authentication contracts and authorization policies can be assigned so that they protect the entire Web server, a single page, or somewhere in between.

An Access Gateway can also be configured so that it caches requested pages. When the user meets the authentication and authorization requirements, the user is sent the page from cache rather than requesting it from the Web server.

An Access Gateway can be installed as a soft appliance (includes both the operating system and the Access Gateway software) and as a service (includes just the Access Gateway software).

## SSL VPNs

You configure the SSL VPN when you need to protect non-HTTP and Java applications. The SSL VPN component provides secure access to such applications as an e-mail server, an FTP client, or Telnet service. The SSL VPN is a Linux-based service as a protected resource of an Access Gateway, which allows it to share session information with the Access Gateway.

The requests are delivered in the form of a servlet. An ActiveX plug-in or Java applet is delivered to the client on successful authentication. Roles and policies determine authorization decisions for back-end applications. Client integrity checking is available to ensure the existence of approved firewall and virus scanning software, before the SSL VPN session is established.

## Policies

Policies provide the authorization component of Access Manager Appliance. The administrator of the Identity Server uses policies to define how properties of a user's authenticated identity map to the set of active roles for the user. This role definition serves as the starting point for role-based authorization policies of the Access Gateway. Additionally, authorization policies can be defined for the Access Gateway that control access to protected resources based on user and system attributes other than assigned roles.

The flexibility built into the policy component is nearly unlimited. You can, for example:

- ♦ Set up a URL-based policy that permits or denies users access to a protected Web site, depending on their roles, such as employee or manager.
- ♦ Specify whether an administrator has access to the policy management component of the Access Manager Administration Console. The administrator could create, edit, and manage policies that are assigned to specific components.

Each Access Gateway includes an Embedded Service Provider agent that interacts with the Identity Server to provide authentication, policy decision, and enforcement.

## 8.1.9 Viewing System Alerts

The System Alerts page displays how many unacknowledged alerts have been generated for all the devices imported into this Administration Console.

- 1 In the Administration Console, click **Access Manager > Dashboard > Alerts**.
- 2 To acknowledge and clear the alerts for a device, select the name of the server, then click **Acknowledge Alerts**.

The following columns display information about the alerts for each server.

| Column               | Description                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server Name</b>   | Specifies the name of the server receiving alerts. Click the server name to view more information about an alert before acknowledging it. |
| <b>Severe</b>        | Indicates how many severe alerts have been sent to the server.                                                                            |
| <b>Warning</b>       | Indicates how many warning alerts have been sent to the server.                                                                           |
| <b>Informational</b> | Indicates how many informational alerts have been sent to the server.                                                                     |

## 8.2 Logging

You can troubleshoot by configuring component logging. In the Administration Console, click **Devices > Identity Server > Edit > Logging**.

For more information, see [Section 5.3, “Using the Log Files for Troubleshooting,” on page 73](#).

## 8.3 Event Codes

Descriptions of the Access Manager event codes are available in [NetIQ Access Manager Appliance 4.0 SP1 Event Codes](#).

## 8.4 Restoring a Failed Secondary Console

If a secondary console fails, you need to remove its configuration from the primary console before installing a new secondary console. If the failed console is part of the configuration, other Access Manager Appliance devices try to contact it.

- 1 On the primary console, click **Auditing > Troubleshooting**.
- 2 In the **Other Known Device Manager Servers** section, click **Remove** next to the secondary console that is failed.
- 3 Remove traces of the secondary console from the configuration datastore:
  - 3a In the NetIQ Access Manager menu bar, select **View Objects**.



- 3b In the Tree view, select **novell**.

**3c** Delete all objects that reference the failed secondary console.

You should find the following types of objects:

- ♦ SAS Service object with the hostname of the secondary console
- ♦ An object that starts with the last octet of the IP address of the secondary console
- ♦ DNS AG object with the hostname of the secondary console
- ♦ DNS IP object with the hostname of the secondary console
- ♦ SSL CertificateDNS with the hostname of the secondary console
- ♦ SSL CertificateIP with the hostname of the secondary console

**4** Install a new secondary console. For installation instructions, see [“Installing Secondary Versions of Access Manager Appliance”](#) in the *NetIQ Access Manager Appliance 4.0 SP1 Setup Guide*.

## 8.5 Converting a Secondary Access Manager Appliance into a Primary Appliance

To convert a secondary Access Manager Appliance into a primary Access Manager Appliance, a recent backup of Access Manager Appliance must be available. For information about how to perform a backup, see [Section 2.2, “Backing Up the Access Manager Appliance Configuration,” on page 34](#). A backup is necessary to restore the certificate authority (CA).

If the failed server holds a master replica of any partition, you must use `ndsrepair` to designate a new master replica on a different server in the replica list.

This conversion includes the following tasks:

- ♦ [Section 8.5.1, “Shutting Down the Primary Access Manager Appliance,” on page 101](#)
- ♦ [Section 8.5.2, “Changing the Master Replica,” on page 101](#)
- ♦ [Section 8.5.3, “Restoring CA Certificates,” on page 102](#)
- ♦ [Section 8.5.4, “Verifying the vcdn.conf File,” on page 103](#)
- ♦ [Section 8.5.5, “Deleting Objects from the eDirectory Configuration Store,” on page 103](#)
- ♦ [Section 8.5.6, “Performing Component-Specific Procedures,” on page 104](#)
- ♦ [Section 8.5.7, “Enabling Backup on the New Primary Appliance,” on page 106](#)

### 8.5.1 Shutting Down the Primary Access Manager Appliance

If your primary Access Manager Appliance is running, you must log in as the administrator and shut down the service.

Start YaST, click **System > System Services (Runlevel)**, then select to stop the `ndsd` service.

### 8.5.2 Changing the Master Replica

Changing the master replica to reside on the new primary Access Manager Appliance makes this Access Manager Appliance into the certificate authority for Access Manager. You need to first designate the replica on the new primary Access Manager Appliance as the master replica. Then you need to remove the old primary Access Manager Appliance from the replica ring.

## Secondary Administration Console

- 1 At the secondary Access Manager Appliance, log in as `root`.
- 2 Change to the `/opt/novell/eDirectory/bin` directory.
- 3 Run DSRRepair with the following options:  

```
./ndsrepair -P -Ad
```
- 4 Select the one available replica.
- 5 Select **Designate this server as the new master replica**.
- 6 Run `ndsrepair -P -Ad` again.
- 7 Select the one available replica.
- 8 Select **View replica ring**.
- 9 Select the name of the failed primary server.
- 10 Select **Remove this server from replica ring**.
- 11 Specify the DN of the admin user in leading dot notation. For example:  
`.admin.novell`
- 12 Specify password.
- 13 Type `I Agree` when prompted.
- 14 Continue with [Section 8.5.3, “Restoring CA Certificates,” on page 102](#).

### 8.5.3 Restoring CA Certificates

The following steps are performed on the machine that you are promoting to be a primary Appliance.

- 1 Copy your most recent Access Manager Appliance backup files to your new primary Access Manager Appliance.
- 2 Change to the backup `bin` directory:  

```
/opt/novell/devman/bin
```
- 3 Verify the IP address in the backup file. The `IP_Address` parameter value should be the IP address of the new Primary Administration Console.
  - 3a Open the backup file:  

```
defbkparm.sh
```
  - 3b Verify that the value in the `IP_Address` parameter is the IP address of your new primary console.
  - 3c Save the file.
- 4 Run the certificate restore script:  

```
sh aminst-certs.sh
```
- 5 When prompted, specify the administrator's password and location of the backup files.
- 6 Continue with [Section 8.5.4, “Verifying the vcdn.conf File,” on page 103](#).

## 8.5.4 Verifying the vcdn.conf File

Verify whether the `vcn.conf` file contains IP address of the new Administration Console. If it contains IP address of the failed primary Administration Console, replace it with the new IP address.

- 1 Change to the Appliance configuration directory:

```
opt/novell/devman/share/conf
```

- 2 Run the following command in the command line interface to restart Access Manager Appliance:

```
/etc/init.d/novell-ac restart OR rcnovell-ac restart
```

- 3 Continue with [Section 8.5.5, “Deleting Objects from the eDirectory Configuration Store,”](#) on page 103.

## 8.5.5 Deleting Objects from the eDirectory Configuration Store

Objects representing the failed primary Access Manager Appliance in the configuration store must be deleted.

- 1 Log in to the new Administration Console, then click **Access Gateways**.
- 2 If the failed primary Appliance's Access Gateway is the primary server (has the red icon next to it), then change the primary Access Gateway server.

- 2a Click **[Access Gateway cluster name] > Edit**.

- 2b Select a different primary Access Gateway > click **Ok** > click **Close**.

Ignore any trust store related warnings.

- 2c Click **Update All**.

Wait until the status becomes current for all except the failed primary Appliance.

- 3 Click **Auditing > Troubleshooting**.
- 4 In the **Other Known Device Manager Servers** section, select the old primary Appliance, then click **Remove**.

- 5 Remove traces of the failed primary Access Manager Appliance from the configuration datastore:

- 5a In the NetIQ Access Manager menu bar, select **View Objects**.

- 5b In the Tree view, select **novell**.

- 5c Delete all objects that reference the failed primary Access Manager Appliance.

You should find the following types of objects:

- ♦ SAS Service object with the hostname of the failed primary console
- ♦ An object that starts with the last octet of the IP address of the failed primary console
- ♦ DNS AG object with the hostname of the failed primary console
- ♦ DNS IP object with the hostname of the failed primary console
- ♦ SSL CertificateDNS with the hostname of the failed primary console
- ♦ SSL CertificateIP with the hostname of the failed primary console

- 6 Continue with [Section 8.5.6, “Performing Component-Specific Procedures,”](#) on page 104.

## 8.5.6 Performing Component-Specific Procedures

If you have installed the following components, perform the cleanup steps for the component:

- ♦ “Third Access Manager Appliance” on page 104
- ♦ “Access Gateway Services” on page 104
- ♦ “SSL VPN” on page 105

### Third Access Manager Appliance

If you installed a third Appliance used for failover, you must manually perform the following steps on that server:

- 1 Open the `vcdn.conf` file.  
`/opt/novell/devman/share/conf`
- 2 In the file, look for the line that is similar to the following:  
`<vcdnPrimaryAddress>10.1.1.1</vcdnPrimaryAddress>`  
In this line, 10.1.1.1 represents the failed primary Appliance IP address.
- 3 Change this IP address to the IP address of the new primary Appliance.
- 4 Restart the Access Manager Appliance by entering the following command from the command line interface:  
`/etc/init.d/novell-ac restart` OR `rcnovell-ac restart`

### Access Gateway Services

For each Access Gateway Service imported into the Administration Console, edit the `settings.properties` file on the Access Gateway if the primary Administration Console was not configured as the Audit Server.

If the primary Administration Console was configured as an Audit Server, you must edit the `config.xml` file and the `settings.properties` file on the Access Gateway and edit the `CurrentConfig` and `WorkingConfig` XML documents in the configuration store on the new primary Administration Console.

- 1 At the Access Gateway Service, log in as the `root` or the `Administrator` user.
- 2 Shut down all Access Gateway Services.  
`/etc/init.d/novell-appliance stop` OR `rcnovell-appliance stop`
- 3 (Conditional) If your audit server was on the primary Administration Console, edit the `config.xml` file:
  - 3a Change to the directory and open the file.  
`/opt/novell/nam/adminconsole/webapps/agm/WEB-INF/config/current`
  - 3b Find the `NsureAuditSetting` entry.  
In the `IPv4Address` field, change the IP address from the failed Administration Console to the new primary Appliance address.
  - 3c Save and exit.
- 4 Edit the `settings.properties` file:
  - 4a Change to the directory and open the file.  
`/opt/novell/devman/jcc/conf`



- 4b Change the IP address in the `remotemgmtip` list from the IP address of the failed Appliance to the address of the new primary Appliance.
- 4c Save and exit.
- 5 At the Access Gateway Service, start all services by entering the following command:  
`/etc/init.d/novell-appliance start` OR `rcnovell-appliance start`
- 6 (Conditional) Repeat this process for each Access Gateway Service that has been imported into the Administration Console.

## SSL VPN

For each SSL VPN component imported into the Administration Console, you must edit the `config.xml` file and the `settings.properties` file on the SSL VPN server and edit the current config and working config XML documents in the configuration store on the new primary Appliance.

- 1 Log in as the `root` user.
- 2 Open a terminal window and shut down all services by entering the following commands:
  - ♦ `/etc/init.d/novell-jcc stop` OR `rcnovell-jcc stop`
  - ♦ `/etc/init.d/novell-sslvpn stop` OR `rcnovell-sslvpn stop`
- 3 Edit the `config.xml` file:
  - 3a Enter: `vi /etc/opt/novell/sslvpn/config.xml`
  - 3b Enter `/DeviceManagerAddress`, then press Enter.
  - 3c Change the IP address to that of the new primary Appliance.
  - 3d Enter `:wq!` to save and exit.
- 4 At the new primary Appliance, open an LDAP browser and edit the `CurrentConfig` object of the SSL VPN.

---

**IMPORTANT:** You should use an LDAP browser for the following steps, rather than iManager. iManager is slow at saving large files, and your iManager connection might time out before your modifications are saved.

---

- 4a Browse to the following container: `novell > accessManagerContainer > VCDN_Root > PartitionsContainer > Partition > AppliancesContainer`.  
 A list of devices appears. SSL VPN devices have an `sslvpn` prefix.
- 4b Expand an SSL VPN container, then select the `CurrentConfig` object.
- 4c Select the `romaSSLVPNConfigurationXMLDoc` attribute and open it.
- 4d Copy the contents of the attribute to a text editor.
- 4e Search for the `<DeviceManagerAddress>` element.
- 4f Change the IP address of the `<DeviceManagerAddress>` element so that it matches the IP address of the new primary Administration Console.
- 4g Copy the modified document in the text editor to the value field of the `romaSSLVPNConfigurationXMLDoc` attribute.
- 4h Save your changes.
- 5 At the new primary Appliance, edit the `WorkingConfig` object of the SSL VPN container:

Use an LDAP browser for these steps.

- 5a Browse to the SSL VPN object by expanding the following containers: novell > accessManagerContainer > VCDN\_Root > PartitionsContainer > Partition > AppliancesContainer.  
A list of devices appears.
- 5b Expand the SSL VPN container, then select the WorkingConfig object.
- 5c Select the romaSSLVPNConfigurationXMLDoc attribute and open it.
- 5d Copy the contents of the attribute to a text editor.
- 5e Search for the <DeviceManagerAddress> element.
- 5f Change the IP address of the <DeviceManagerAddress> element so that it matches the IP address of the new primary Administration Console.
- 5g Copy the modified document in the text editor to the value field of the romaSSLVPNConfigurationXMLDoc attribute.
- 5h Save your changes.
- 6 Start all services by entering the following commands:
  - ♦ `/etc/init.d/novell-jcc start` OR `rcnovell-jcc start`
  - ♦ `/etc/init.d/novell-sslvpn start` OR `rcnovell-sslvpn start`
- 7 (Conditional) If the SSL VPN server is still not functioning, restart the Linux server by entering `reboot`.
- 8 (Conditional) Repeat this process for each SSL VPN server that has been imported into the Administration Console.

## 8.5.7 Enabling Backup on the New Primary Appliance

- 1 On the new primary Appliance, change to the `/opt/novell/devman/bin` directory.
- 2 Open the `defbkparm.sh` file and find the following lines:

```
EDIR TREE=<tree_name>
EDIR CA=<CA name>
```

These lines contain values using the hostname of the Appliance you are on.

- 3 Modify these lines to use the hostname of the failed Appliance.

When you install the primary Appliance, the EDIR TREE parameter is set to the hostname of the server with `_tree` appended to it. The EDIR CA parameter is set to the hostname of the server with `_tree CA` appended to it.

If the failed Appliance had `amlab` as its hostname, you would change these lines to have the following values:

```
EDIR TREE="amlab_tree"
EDIR CA="amlab_tree CA"
```

- 4 Save your changes.
- 5 Take a backup from your new primary Appliance.

---

**WARNING:** After configuring the secondary Appliance to be the new primary Appliance and performing all the cleanup steps, you cannot restore an old backup from the primary Appliance. Take a new backup as soon as your new primary Appliance is functional.

---

## 8.6 Repairing the Configuration Datastore

The configuration datastore is an embedded version of eDirectory 8.8. If it becomes corrupted, you can run DSRepair to fix it. Or, you can restore a recent backup. To restore a backup, see [Section 2.3, “Restoring the Access Manager Appliance Configuration,” on page 35](#).

To run DSRepair:

- 1 In a browser, enter the following URL.

```
http://<ip_address>:8028/nds
```

Replace <ip\_address> with the IP address of your Administration Console.

- 2 At the login prompt, enter the username and password of the admin user for the Administration Console.

The NDS iMonitor application is launched. For more information, see [Accessing iMonitor \(http://www.novell.com/documentation/edir88/edir88/data/a6l60f7.html\)](http://www.novell.com/documentation/edir88/edir88/data/a6l60f7.html).

- 3 In the **View** bar, select the **Repair** icon.

For more information about DSRepair, see the following:

- ♦ Click the **Help** icon.
- ♦ [Using NdsRepair \(http://www.novell.com/documentation/edir88/edir88tshoot/data/bq0gv5l.html\)](http://www.novell.com/documentation/edir88/edir88tshoot/data/bq0gv5l.html)

## 8.7 Session Conflicts

Do not use two instances of the same browser to simultaneously access the same Administration Console. Browser sessions share settings, which can result in problems when you apply changes to configuration settings. However, you can use two different brands of browsers simultaneously, such as Internet Explorer and Firefox to avoid the session conflicts.

## 8.8 Unable to Log In to the Administration Console

If you experience problems logging in to the Administration Console, you might need to restart Tomcat.

- 1 Restart Tomcat by running this command:

```
/etc/init.d/novell-ac restart OR rcnovell-ac restart
```

- 2 If this does not solve the problem, check the log file:

```
/opt/novell/nam/adminconsole/logs/catalina.out
```

- 3 Check for the following error:

```
Error Starting up core services.  
Application manager is Shutting down the Device Manager suite.  
Shutting down Device Manager suite.
```

- 4 If you see this error, check the status of eDirectory:

- 4a Enter the following command:

```
/etc/init.d/nds status
```

If the status command returns nothing, start eDirectory manually.

- 4b Enter the following command:

```
/etc/init.d/ndsd start
```

4c Restart Tomcat.

## 8.9 Exception Processing IdentityService\_ServerPage.JSP

If you see the message `Exception processing IdentityService_ServerPage.jsp` on the Administration Console, it is an indication that the system has run out of available file handles. You need to use the command line to increase the `ulimit` value (`ulimit -n [new limit]`), which sets the number of open file descriptors allowed.

To set this value permanently, you can create the `/etc/profile.local` file with the `ulimit` value, such as:

```
ulimit -n 4096
```

You can make changes to `/etc/security/limits.conf` file with a line just to change the limit for a specific user. In this case: `novlwwuser`. Add the following line:

```
novlwww soft nofile [new limit]
```

## 8.10 Backup and Restore Failure Because of Special Characters in Passwords

Administration passwords with special characters such as dollar signs might cause the `ambkup` utility to fail. The `ambkup` utility creates a command line for the `ICE` utility, and the special characters might be interpreted by it. If you must use special characters, and this issue arises, modify the `defbkparm` file so that the special characters are escaped.

For example, if the administrator's password is `mi$$le`, then the field `DS_ADMIN_PWD` should be `mi\$\$le`.

This file is located in the following directory:

```
/opt/novell/devman/bin/defbkparm.sh
```

## 8.11 Unable to Install NMAS SAML Method

When you try to create an Identity Server cluster configuration with an eDirectory user store and with the **Install NMAS SAML method** option enabled and you have not installed the dependent packages, the following error message is displayed:

```
Warning: Failed to create SAML Affiliate Object  
com.novell.security.japi.nmas.LoginMethodModel.getLsmWINNNTStatus()I
```

One of the installation requirements for the Administration Console is to install the `compat` and the `libstdc++` packages. On SLES 11, the `compat` package contains the `libstdc++` library. The Identity Server also requires the `compat` package. For more information about installing these packages, see [TID 7004701: iManager: Certificate Server Plugin Errors \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT\\_TID\\_1\\_1&dialogID=68926420&statId=0%200%20130264119\)](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&statId=0%200%20130264119).

## 8.12 Incorrect Audit Configuration

If the Audit Events from Access Gateway behind NAT are not seen in the Audit Server, do the following:

Click **Auditing** in the Administration Console and verify if values are provided for the **Server Listening IP Address**, **Server Public NAT IP Address**, and **Port Numbers** fields.

### Scenario 1:

- 1 If the values are not provided for the **Server Listening IP Address**, **Server Public NAT IP Address**, and **Port Numbers** fields, enter the values, then click **Apply**.
- 2 If you change the existing values and click **Apply**, an information window displays the following messages:

All Access Gateways need to be updated.

All servers need to be rebooted to start using the new configuration.

- 3 Click **OK**.
- 4 Update the Access Gateway whose events are not seen.
- 5 Restart the Access Gateway.

### Scenario 2:

- 1 If Server Listening IP Address, Server Public NAT IP Address and Port Numbers are valid and still have problems, repush the configuration.
- 2 Change the port number to some invalid port number, then click **Apply**.

---

**NOTE:** Do not update or restart the Access Gateway as the message indicates.

---

- 3 Change the invalid port number again to the valid port number, then click **Apply**.  
The configuration is repushed and works successfully.
- 4 Update the Access Gateway whose events are not seen.
- 5 Restart the Access Gateway.

## 8.13 Unable to Update the Access gateway Listening IP Address in the Administration Console Reverse Proxy

The Administration Console fails to change the Access Gateway listening IP address of the Reverse Proxy. The health status of the Access Gateway on Administration Console displays failure to start the protected resource with old Listening IP address. However, when protected resource is viewed

(**Devices > Access Gateways > Access Gateway or Access Gateway Cluster > Proxy**), the Administration Console displays the new IP Address has been selected as listening IP address of the Reverse Proxy.

To workaround this issue:

- 1 In the Administration Console, click **Devices > Access Gateways**.
  - 1a Click the **Health** icon of the Access Gateway that has the problem.
  - 1b Note the Reverse Proxies that have the problem.
- 2 In the Administration Console, click **Devices > Access Gateways**.
- 3 Click the **Edit** link for the cluster that has problem.
- 4 For each of the Reverse Proxies that have the problem, do the following:
  - 4a Click **Reverse Proxy**.
  - 4b Select the cluster member from the list.
  - 4c Select the new IP address on which the proxy service will listen to.
  - 4d Unselect the old IP address on which proxy service was listening to.
  - 4e Click **OK**.
  - 4f An alert is displayed as "Select at least one listening address for the service."
  - 4g Click **OK**.
  - 4h Again select the **Listening IP Address** check box.
  - 4i Click **OK**.
- 5 If the update link is enabled, click on it. If not, do the following:
  - 5a Click **Edit** for the cluster that has problem.
  - 5b Click the **Proxy** name link.
  - 5c Click **Proxy service name** in the **Proxy Service** list.
  - 5d Enter the description.
  - 5e Click **OK**.

The **Update** link will be enabled.
  - 5f Click **Update**.

After the device command status moves to Succeeded, verify the health status of the Access Gateway.

## 8.14 During Access Manager Appliance Installation Any Error Message Should Not Display Successful Status

Even after successful installation or upgrade of Access Gateway, the health shows failure in starting ESP. After a fresh import of Access Manager Appliance in the Administration Console, the Access Gateway Health displays “*ESP Failed to initialize : Unable to read <keystorefilelocation>*”. The keystore file can be Connector, Signing, Encryption or Truststore.

To workaround this issue:

- 1 On the Access Gateway, go to the <keystorefilelocation> location as specified in the health error message.
- 2 Delete the files indicated in the ESP error message.
- 3 In the Administration Console, click **Auditing > Troubleshooting > Certificates**.
- 4 Enable the device that has been deleted in the Access Manager Appliance and it needs to be re-pushed.
- 5 Click **Re-Push Certificate**.
- 6 Restart server provider of the Access Gateway.

## 8.15 Incorrect Health Is Reported on the Access Gateway

In the Administration Console, if the **Stop Service on Audit Server Failure** option is enabled, the Access Gateway services are stopped and show the Health status reports services as down when the Audit server is not functioning or reachable,.

If the **Stop Service on Audit Server Failure** option is disabled, the Access Gateway Service comes up but the related Health status still reports the services as being down.

To workaround this issue restart Tomcat.

## 8.16 Administration Console Does Not Refresh the Command Status Automatically

The automatic refresh feature to retrieve device health is disabled when total number of the Access Gateway devices imported to an Administration Console page is more than 20. This feature is disabled to prevent the performance overhead in getting the health of 20 or more devices simultaneously.

To workaround this issue an administrator can manually refresh the page to get the health status of the devices.

## 8.17 SSL Communication Fails

From 3.2 onwards, Access Manger supports only the 128-bit SSL communication among the Administration Console, Identity Server, SSL VPN, and browsers.

If you want to enable the weak ciphers (not recommended), see [Section 1.1.4, “Configuring the SSL Communication,” on page 15](#).

## 8.18 Error: Tomcat did not stop in time. PID file was not removed

While stopping Tomcat for the Administration Console, Access Gateway, Identity Server, or SSL VPN, you may get this error message:

```
Tomcat did not stop in time. PID file was not removed.
```

Ignore this message. Tomcat will be forcibly stopped if it does not stop normally.

## 8.19 An IP Address for the Other Known Device Manager List is Missing in the Troubleshooting Page

If the Administration Console is down, the IP address for that console is not seen. To bring up that Administration Console, follow these steps:

- 1 Run the `sntp -P no -r PRIMARY_IP` command.
- 2 Run the `/etc/init.d/novell-ac restart` OR `rcnovell-ac restart` command.

If the Administration Console is still not available, follow these steps:

- 1 Run the `/etc/init.d/ndsd restart` command.
- 2 Run the `/etc/init.d/novell-ac restart` OR `rcnovell-ac restart` command.

## 8.20 View Objects Do Not Function Properly in Internet Explorer 10 Default Mode

When you click **View Objects**, you cannot perform any popup related operations in **Tree**, **Browse**, and **Search** tabs.

To workaround this issue, launch Internet Explorer 10 in the compatibility mode.

---

**NOTE:** This is an iManager issue. See [Operations Under the View Objects do not function properly in Internet Explorer 10 Default Mode](#) in the [iManager 2.7.6 Readme](#).

---



---

# 9 Troubleshooting Certificate Issues

- ♦ Section 9.1, “Resolving Certificate Import Issues,” on page 113
- ♦ Section 9.2, “Mutual SSL with X.509 Produces Untrusted Chain Messages,” on page 115
- ♦ Section 9.3, “Certificate Command Failure,” on page 115
- ♦ Section 9.4, “A Device Reports Certificate Errors,” on page 115
- ♦ Section 9.5, “Issue while Adding the Access Gateway in a Cluster,” on page 116
- ♦ Section 9.6, “Renewing the expired eDirectory certificates,” on page 116

## 9.1 Resolving Certificate Import Issues

Use the following sections to resolve issues created when a full certificate chain is not imported in to Access Manager Appliance:

- ♦ Section 9.1.1, “Importing an External Certificate Key Pair,” on page 113
- ♦ Section 9.1.2, “Resolving a -1226 PKI Error,” on page 114
- ♦ Section 9.1.3, “When the Full Certificate Chain Is Not Returned During an Automatic Import of the Trusted Root,” on page 114
- ♦ Section 9.1.4, “Using Internet Explorer to Add a Trusted Root Chain,” on page 114

### 9.1.1 Importing an External Certificate Key Pair

The Access Manager Certificate Authority requires that all certificate key pairs in `.pfx` format contain the complete certificate chain. If a key pair was created with multiple CAs and the exported certificate does not contain the complete certificate chain, the file cannot be imported into Access Manager. When you try to import such a certificate, the following error message is displayed:

```
"Error importing certificate key pair: Error: Error: -1403
```

When exporting the certificate key pair, ensure that you include all the certificates in the certification path.

To ensure that your certificate contains all the intermediate certificates and contains them in the right order, import the certificate into Internet Explorer or Firefox.

- ♦ For Internet Explorer, click **Tools > Internet Options > Content > Certificates > Personal > Import**.
- ♦ For Firefox, click **Tools > Options > Advanced > Encryption > View Certificates > Your Certificates > Import**.

Make sure the browser contains the public key for all the intermediate CAs. Then select the certificate and export the certificate in `.pfx` format. In Internet Explorer, you must select to include all the certificates in the chain. In Firefox, all the certificates in the chain are automatically included.

If you receive an error when importing the certificate, the error comes from either NICI or PKI. For a description of these error codes, see [Novell Certificate Server Error Codes and Novell International Cryptographic Infrastructure](http://www.novell.com/documentation/nwec/index.html) (<http://www.novell.com/documentation/nwec/index.html>).

## 9.1.2 Resolving a -1226 PKI Error

When you create a certificate signing request, send it to a third-party issuer to be signed, and receive the server certificate from the third-party issuer. You sometimes receive a -1226 error when you try to import the signed certificate. You receive this error when the issuer does not send the trusted roots required to validate the issuer of the server certificate.

Use one of the following options to resolve this issue:

- ♦ If the issuer included the trusted root and any intermediate certificates in a separate file or files, specify these files during the import by clicking the + character that allows you to add a trusted root or an intermediate certificate.
- ♦ If the issuer did not send you any additional files, you can go to the issuer's Web site, download them, then specify these files during the import by clicking the + character that allows you to add a trusted root or an intermediate certificate.
- ♦ You can try importing the certificate into Internet Explorer, which has the trusted roots from all major CAs, then export the certificate with the required chain of trusted roots. See [Section 9.1.4, "Using Internet Explorer to Add a Trusted Root Chain,"](#) on page 114.

## 9.1.3 When the Full Certificate Chain Is Not Returned During an Automatic Import of the Trusted Root

Access Manager Appliance allows you to automatically import the trusted root under the following conditions:

- ♦ When enabling SSL communication between the Access Gateway and the Web server, you can automatically import the root CA from the Web server.
- ♦ When setting up the user stores for the Identity Server and adding the server replicas, you can automatically import the root CA of the LDAP server.

If there are multiple certificates in the chain, sometimes the server does not send all the certificates in the chain. When this happens, the following message is displayed:

```
The root CA certificate was not returned by the server. It might be necessary
to manually import the root CA certificate and possible intermediate CA
certificates in order to complete the chain.
```

To correct this problem, you need to manually import the missing entries. The easiest method to obtain all the certificates in the chain, including the root CA, is to import the server certificate into Internet Explorer, then export the chain and import it into Access Manager. If Access Manager already has some of the certificates, it skips their import and imports only the missing certificates.

For instructions on this process, see [Section 9.1.4, "Using Internet Explorer to Add a Trusted Root Chain,"](#) on page 114.

## 9.1.4 Using Internet Explorer to Add a Trusted Root Chain

The following procedure works only when Internet Explorer contains the trusted root certificate of the issuer of your certificate.

- 1 In Internet Explorer, click **Tools > Internet Options > Content > Certificates**.
- 2 Click **Import** and import your server certificate into the **Other People** tab.
- 3 Click **Other People**, then double-click your certificate.

- 4 Click **Certification Path**.
  - ♦ If the **Certification Path** shows that the certificate is OK, you now have the full certificate chain available for export. Click **OK**, then continue with [Step 5](#).
  - ♦ If the **Certification Path** is not OK, you cannot use this method. Click **OK**, then contact your issuer for the certificate chain.
- 5 Select the certificate, then click **Export > Next**.
- 6 Select **Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)** as the format and select **Include all certificates in the certification path if possible** to include the certificate chain.
- 7 Click **Next**, then specify a filename and path for the file.
- 8 Click **Next > Finish**.
- 9 Use this P7B file to import your server certificate into Access Manager.

## 9.2 Mutual SSL with X.509 Produces Untrusted Chain Messages

When you set up an X.509 contract for mutual SSL authentication, you must ensure that the Identity Server trust store (NIDP-truststore) contains the trusted root from each CA that has signed the client certificates. If a client has a certificate signed by a CA that is not in the Identity Server Trust Store, authentication fails.

To add a certificate to the Identity Server Trust Store:

- 1 In the Administration Console, click **Devices > Identity Servers > Edit > Security > NIDP Trust Store**.
- 2 Click either **Add** or **Auto-Import From Server** and follow the prompts.

## 9.3 Certificate Command Failure

Certificate commands are generated when you upgrade the Administration Console. Ensure that they have completed successfully.

- 1 To determine whether a certificate command has failed, click **Security > Command Status**.
- 2 Note the destination trust store or keystore of the failed command.
- 3 Click **Auditing > Troubleshooting > Certificates**.

The Certificates page displays all the keystores and trust stores configured for Access Manager.
- 4 Select the store, then click **Re-push certificates**.

This sends all assigned certificates to Access Manager Appliance.

## 9.4 A Device Reports Certificate Errors

After you restore a device, especially the Administration Console, the device might report certificate errors. To fix these errors, you need to re-push the certificates from the Administration Console to the device:

- 1 Click **Auditing > Troubleshooting > Certificates**.
- 2 Select the store that is reporting errors, then click **Re-push certificates**.

You can select multiple stores at the same time.

- 3 (Optional) To verify that the re-push of the certificates was successful, click **Security > Command Status**.

## 9.5 Issue while Adding the Access Gateway in a Cluster

You may get the following error while adding the Access Gateway in a cluster:

Unable to read keystore: /opt/novell/devman/jcc/certs/esp/4C06F0AE2EFAED18/signing.keystore

To workaround this issue:

- 1 Click **Auditing > Troubleshooting > Certificates**.
- 2 Select the store that is reporting errors, then click **Re-push certificates**.  
You can select multiple stores at the same time.
- 3 (Optional) To verify that the re-push of the certificates was successful, click **Security > Command Status**.

## 9.6 Renewing the expired eDirectory certificates

The Secondary Administration Console stops working when the eDirectory certificates expire.

To workaround this issue manually renew the eDirectory certificates. For more information, see [renewing the certificates](#).

---

# A Certificates Terminology

Access Manager Appliance uses certificates to provide secure communication between devices, encrypt sensitive information, facilitate single sign-on, and to verify that the user sending the message is who he or she claims to be. The following is a list of certificate terminology used in Access Manager Appliance:

**certificate authority (CA):** An entity that issues digital certificates attesting to the authenticity of the information in the certificate.

**certificate:** Information attached to an electronic message. It is used to verify that the sender is who he or she claims to be. A certificate is signed. The signer of the certificate (a CA), if trusted, verifies the accuracy of the information in the certificate.

**certificate chain:** In addition to identifying a user, server, or computer, certificates can validate the identity and trustworthiness of other certificates. A certificate that asserts an identity is signed by a certificate that trusts the contents of the certificate it is signing. The signing certificate in turn can be signed by another certificate, which can be signed by another certificate, and so forth, thus forming a certificate chain. The last certificate in the certificate chain is referred to as the root certificate and is a self-signed certificate.

When a certificate or certificate chain is sent from one computer to another, the receiving computer examines the certificate chain to determine if it can be trusted. To verify certificate trust in a chain, the receiving computer examines its own configuration store to see if it contains a CA certificate that matches the root certificate of the certificate chain. If so, the receiver compares its copy of the certificate with the chain's root certificate to verify its authenticity.

**certificate signing request (CSR):** Requesting a signed certificate is accomplished by sending a CSR to the CA. A CSR is created with information about the person or organization that desires the signed certificate. A public key is also generated and included in the CSR. A private key is also generated, but not included in the CSR.

When the CA receives the CSR, the CA uses it in combination with the CA's guidelines and practices to establish that the person or organization represented by the CSR is properly identified and authorized as the owner of the information in CSR. The CA creates and signs a certificate that the requesting person or organization can use. The signature of the CA in the certificate identifies that the entity is who it claims to be. The signed certificate is delivered to its owner, who adds it to the keystore (usually the same keystore where the private key created with the original CSR resides).

**issuer:** The CA that issues a certificate.

**intermediate certificate:** A subordinate certificate issued by the trusted root specifically for end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, proceeds through the intermediate certificate, and ends with the SSL certificate issued to you. Using intermediate certificates adds more levels of security, but does not cause performance, installation, or compatibility issues.

**key:** A string or variable value used for encrypting and decrypting information.

**key pair:** Public and private keys generated by a cryptography system and used in combination with each other.

**keystore:** A storage file containing keys, certificates, and trusted roots. Access Manager Appliance agents can access keystores to retrieve certificates, keys, and trusted roots as needed.

**local CA:** The CA of the Administration Console's instance of eDirectory. Also known as the Organizational CA.

**private key:** The unpublished key in a security system that uses two keys. It is used for authentication, data encryption/decryption, digital signing, and secure e-mail. One of the most common uses is sending and receiving digitally signed and encrypted e-mail by using the S/MIME standard.

The public and private keys have the following relationships:

- ♦ Data encrypted with the public key can be decrypted with the private key only.
- ♦ Data signed with the private key can be verified with the public key only.
- ♦ Exposing a public key does not expose the corresponding private key.

**public key:** The publicly distributed key in a security system that uses two keys.

**root CA:** The issuing authority for the root certificate.

**root certificate:** The last certificate in a certificate chain.

**self-signed certificate:** A certificate whose issuer is itself.

**SSL connections:** When two computers connect and need to establish trust and a secure connection, certificates are exchanged and an encryption algorithm is established. Public keys shared in the exchanged certificates, as well as the associated private keys (which are not exchanged) are used as part of the encryption algorithm. After security is established, a secure SSL session is established and the two computers are able to communicate securely.

**trusted certificate:** The certificate of a known CA. These certificates are self-signed and are recognized as representing a CA that is trusted.

**trusted root:** The same as a trusted certificate. A trusted root provides the basis for trust in public key cryptography. Trusted roots enable security for SSL, secure e-mail, and certificate-based authentication. These certificates are for root CAs, so they are called "trusted roots."

**trust store:** A keystore containing only trusted roots. Intermediate CAs and end entity public certificates can be part of a trust store.

---

# B Access Manager Audit Events and Data

The sections contains all the Novell audit events logged by Access Manager Appliance. Each event has EventID, Description, Originator Title, Target Title, Subtarget Title, Text1 Title, Text2 Title, Text3 Title, Value1 Title, Value1 Type, Group Title, Data Length, and Data Type values stored. Each field contains a single character token (such as B, U, Y, and so on) that represent the data fields of the audit event, with each letter representing a different data field. The mapping of the character tokens to data fields is found in the `nids_en.lsc` and `sslvpn_en.lsc` files.

**Access Manager** is listed among the log applications on the **General** tab on the Logging Server Options page (**Auditing and Logging > Logging Server Options**). You can view events on the Event list page in **Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**.

When you run an SQL query (**Auditing and Logging > Queries > [Name] > Run**), the system displays the results on the Query Results page. The **EventID** column displays the description of the event. Below, the event ID is listed with the description, to help you quickly locate the data for each audit event.

This section discusses the following audit events:

- [Section B.1, “NIDS: Sent a Federate Request \(002e0001\),” on page 121](#)
- [Section B.2, “NIDS: Received a Federate Request \(002e0002\),” on page 122](#)
- [Section B.3, “NIDS: Sent a Defederate Request \(002e0003\),” on page 122](#)
- [Section B.4, “NIDS: Received a Defederate Request \(002e0004\),” on page 123](#)
- [Section B.5, “NIDS: Sent a Register Name Request \(002e0005\),” on page 123](#)
- [Section B.6, “NIDS: Received a Register Name Request \(002e0006\),” on page 124](#)
- [Section B.7, “NIDS: Logged Out an Authentication that Was Provided to a Remote Consumer \(002e0007\),” on page 124](#)
- [Section B.8, “NIDS: Logged out a Local Authentication \(002e0008\),” on page 125](#)
- [Section B.9, “NIDS: Provided an Authentication to a Remote Consumer \(002e0009\),” on page 125](#)
- [Section B.10, “NIDS: User Session Was Authenticated \(002e000a\),” on page 126](#)
- [Section B.11, “NIDS: Failed to Provide an Authentication to a Remote Consumer \(002e000b\),” on page 126](#)
- [Section B.12, “NIDS: User Session Authentication Failed \(002e000c\),” on page 127](#)
- [Section B.13, “NIDS: Received an Attribute Query Request \(002e000d\),” on page 128](#)
- [Section B.14, “NIDS: User Account Provisioned \(002e000e\),” on page 128](#)
- [Section B.15, “NIDS: Failed to Provision a User Account \(002e000f\),” on page 129](#)
- [Section B.16, “NIDS: Web Service Query \(002e0010\),” on page 129](#)
- [Section B.17, “NIDS: Web Service Modify \(002e0011\),” on page 130](#)
- [Section B.18, “NIDS: Connection to User Store Replica Lost \(002e0012\),” on page 131](#)

- ◆ Section B.19, “NIDS: Connection to User Store Replica Reestablished (002e0013),” on page 131
- ◆ Section B.20, “NIDS: Server Started (002e0014),” on page 132
- ◆ Section B.21, “NIDS: Server Stopped (002e0015),” on page 132
- ◆ Section B.22, “NIDS: Server Refreshed (002e0016),” on page 133
- ◆ Section B.23, “NIDS: Intruder Lockout (002e0017),” on page 133
- ◆ Section B.24, “NIDS: Severe Component Log Entry (002e0018),” on page 134
- ◆ Section B.25, “NIDS: Warning Component Log Entry (002e0019),” on page 134
- ◆ Section B.26, “NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider as Identity Provider and Service Provider Are not in Same Group (002E001A),” on page 135
- ◆ Section B.27, “NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider Because a Policy Evaluated to Deny (002E001B),” on page 136
- ◆ Section B.28, “NIDS: Brokered an Authentication from Identity Provider to Service Provider (002E001C),” on page 136
- ◆ Section B.29, “NIDS: Roles PEP Configured (002e0300),” on page 137
- ◆ Section B.30, “Access Gateway: PEP Configured (002e0301),” on page 137
- ◆ Section B.31, “Roles Assignment Policy Evaluation (002e0320),” on page 138
- ◆ Section B.32, “Access Gateway: Authorization Policy Evaluation (002e0321),” on page 138
- ◆ Section B.33, “Access Gateway: Form Fill Policy Evaluation (002e0322),” on page 139
- ◆ Section B.34, “Access Gateway: Identity Injection Policy Evaluation (002e0323),” on page 139
- ◆ Section B.35, “Access Gateway: Access Denied (0x002e0505),” on page 140
- ◆ Section B.36, “Access Gateway: URL Not Found (0x002e0508),” on page 140
- ◆ Section B.37, “Access Gateway: System Started (0x002e0509),” on page 141
- ◆ Section B.38, “Access Gateway: System Shutdown (0x002e050a),” on page 142
- ◆ Section B.39, “Access Gateway: Identity Injection Parameters (0x002e050c),” on page 142
- ◆ Section B.40, “Access Gateway: Identity Injection Failed (0x002e050d),” on page 143
- ◆ Section B.41, “Access Gateway: Form Fill Authentication (0x002e050e),” on page 144
- ◆ Section B.42, “Access Gateway: Form Fill Authentication Failed (0x002e050f),” on page 144
- ◆ Section B.43, “Access Gateway: URL Accessed (0x002e0512),” on page 145
- ◆ Section B.44, “Access Gateway: IP Access Attempted (0x002e0513),” on page 146
- ◆ Section B.45, “Access Gateway: Webserver Down (0x002e0515),” on page 147
- ◆ Section B.46, “Access Gateway: All WebServers for a Service is Down (0x002e0516),” on page 147
- ◆ Section B.47, “Management Communication Channel: Health Change (0x002e0601),” on page 148
- ◆ Section B.48, “Management Communication Channel: Device Imported (0x002e0602),” on page 148
- ◆ Section B.49, “Management Communication Channel: Device Deleted (0x002e0603),” on page 149
- ◆ Section B.50, “Management Communication Channel: Device Configuration Changed (0x002e0604),” on page 150
- ◆ Section B.51, “Management Communication Channel: Device Alert (0x002e0605),” on page 150



- [Section B.52, “SSL VPN: Common Logs \(002e0701\),” on page 151](#)
- [Section B.53, “SSL VPN: Extended Logs \(002e0702\),” on page 151](#)
- [Section B.54, “SSL VPN: Servlet Status \(002e0706\),” on page 152](#)
- [Section B.55, “SSL VPN: Servlet Connection Added \(002e0707\),” on page 152](#)
- [Section B.56, “SSL VPN: Servlet Connection Failed \(002e0708\),” on page 153](#)
- [Section B.57, “SSL VPN: Servlet Connection Removed \(002e0709\),” on page 153](#)
- [Section B.58, “SSL VPN: Cluster Node Status \(002e070A\),” on page 154](#)
- [Section B.59, “SSL VPN: Servlet New Session Created \(002e070B\),” on page 154](#)
- [Section B.60, “SSL VPN: Servlet Session Replicated \(002e070C\),” on page 155](#)
- [Section B.61, “SSL VPN: Servlet Session Removed \(002e070D\),” on page 155](#)
- [Section B.62, “SSL VPN: Servlet State Transfer Started \(002e0710\),” on page 156](#)
- [Section B.63, “SSL VPN: Servlet State Transfer Completed \(002e0711\),” on page 156](#)
- [Section B.64, “SSL VPN: Servlet Cluster Node Is Down \(002e0712\),” on page 157](#)
- [Section B.65, “SSL VPN: Servlet Cluster Node Is Restarted \(002e0713\),” on page 157](#)
- [Section B.66, “SSL VPN: Servlet Cluster Error with Reason \(002e0714\),” on page 158](#)
- [Section B.67, “SSL VPN: Servlet Service Provider Authenticated User \(002e0715\),” on page 158](#)
- [Section B.68, “SSL VPN: Servlet New Authenticated Connection Received \(002e0716\),” on page 159](#)
- [Section B.69, “SSL VPN: Servlet Service Provider Re-authenticated User \(002e0717\),” on page 159](#)

## B.1 NIDS: Sent a Federate Request (002e0001)

This event is generated when you select the **Federation Request Sent** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Sent a federate request.

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.2 NIDS: Received a Federate Request (002e0002)

This event is generated when you select the **Federation Request Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Received a federate request.

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier; Data Description: Service Provider ID

**Text2 (T):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.3 NIDS: Sent a Defederate Request (002e0003)

This event is generated when you select the **Defederation Request Sent** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Sent a defederate request.

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier; Data Description: Service Provider ID

**Text2 (T):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.4 NIDS: Received a Defederate Request (002e0004)

This event is generated when you select the **Defederation Request Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Received a defederate request

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier

Data Description: Service Provider ID

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.5 NIDS: Sent a Register Name Request (002e0005)

**Description:** NIDS: Sent a register name request

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.6 NIDS: Received a Register Name Request (002e0006)

This event is generated when you select the **Register Name Request Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Received a register name request

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.7 NIDS: Logged Out an Authentication that Was Provided to a Remote Consumer (002e0007)

This event is generated when you select the **Logout Provided** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Logged out an authentication that was provided to a remote consumer

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier

Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** Schema Title: Timed Out

Data Description: 0 = other reason

1 = timed out

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.8 NIDS: Logged out a Local Authentication (002e0008)

This event is generated when you select the **Logout Local** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Logged out a local authentication

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: LDAP Auth: User DN

Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier

Data Description: IDP Session ID (AMAUTHID#auth\_id:

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** Schema Title: Timed Out

Data Description: 0 = other reason

1 = timed out

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.9 NIDS: Provided an Authentication to a Remote Consumer (002e0009)

This event is generated when you select the **Login Consumed** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Provided an authentication to a remote consumer

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: User DN

**SubTarget (Y):** Schema Title: Authentication Identifier

Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text1 (S):** Schema Title: Authentication Type

Data Description: Authentication Profile

**Text2 (T):** Schema Title: Authentication Entity Name  
Data Description: Authentication Source

**Text3 (F):** Schema Title: Contract Class or Method Name  
Data Description: Authentication Contract URI

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** Schema Title: Client IP Address Description: IP Address of the host from which the authentication succeeded.

## **B.10 NIDS: User Session Was Authenticated (002e000a)**

This event is generated when you select the **Login Provided** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: User session was authenticated

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier  
Data Description: User DN

**SubTarget (Y):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text1 (S):** Schema Title: Authentication Type  
Data Description: Authentication Profile

**Text2 (T):** Schema Title: Authentication Entity Name  
Data Description: Authentication Source

**Text3 (F):** Schema Title: Contract Class or Method Name  
Data Description: Authentication Contract URI

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** Schema Title: Client IP Address Description: IP Address of the host from which the authentication succeeded.

## **B.11 NIDS: Failed to Provide an Authentication to a Remote Consumer (002e000b)**

This event is generated when you select the **Login Consumed Failure** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Failed to provide an authentication to a remote consumer

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier  
Data Description: User DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Provider Identifier  
Data Description: Service Provider ID

**Text3 (F):** Schema Title: Reason  
Data Description: Reason Message

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.12 NIDS: User Session Authentication Failed (002e000c)

This event is generated when you select the **Login Provided Failure** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration. Use the **Description** field and the **Text3 (F)** field to determine whether the failure came from a contract, SAML 1.1, SAML 2.0, or Liberty.

**Description:** NIDS: User session authentication failed. This string plus one of the following phrases: for a contract failure, `Contract Execution`; for a SAML 1.1 failure, `SAML Assertion`; for a SAML 2.0 failure, `SAML2 SSO`; for a Liberty failure, `Liberty SSO`.

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Authentication Contract Name  
Data Description: Contract URI

**SubTarget (Y):** Schema Title: User Identifier Data Description: User DN

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Reason  
Data Description: Reason Message

**Text3 (F):** Schema Title: Authentication Source  
Data Description: For a contract, contains the authentication method name; for Liberty, contains the service provider IP; for SAML 1.1, contains the SAML assertion issuer; for SAML 2.0, contains the service provider IP.

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** Schema Title: Client IP Address Description: IP Address of the host from which the authentication failed.

## B.13 NIDS: Received an Attribute Query Request (002e000d)

This event is generated when you select the **Attribute Query Request Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Received an attribute query request

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier  
Data Description: LDAP Auth: User DN  
Other Auth: User GUID

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier  
Data Description: Service Provider ID

**Text2 (T):** Schema Title: Attribute Names  
Data Description: Requested Attributes

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.14 NIDS: User Account Provisioned (002e000e)

This event is generated when you select the **User Account Provisioned** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: User account provisioned

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Store Identifier  
Data Description: Displayable user name

**SubTarget (Y):** null

**Text1 (S):** Schema Title: User Identifier  
Data Description: Authentication User Name

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)



**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.15 NIDS: Failed to Provision a User Account (002e000f)

This event is generated when you select the **User Account Provisioned Failure** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Failed to provision a user account

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Store Identifier

Data Description: Displayable User Name

**SubTarget (Y):** null

**Text1 (S):** Schema Title: User Identifier

Data Description: Authentication User Name

**Text2 (T):** Schema Title: Reason

Data Description: Reason Message

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.16 NIDS: Web Service Query (002e0010)

This event is generated when you select the **Web Service Query Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration. The Identity Server uses this event for two types of Web service queries:

- ♦ **Discovery:** This is a query to discover a service. For this type of query, the **Group (G)** field is not used. For a remote query, the **Data Description** of the **Value1** field is set to 0. For a local query, the **Data Description** of the **Value1** field is set to 1.
- ♦ **Profile:** This is a query to get attributes for a user from a profile (personal, credential, etc.). For this type of query, the **Group (G)** field contains a GroupingID for all attributes selected in the request. A separate event is generated for each attribute select list in the request. For a remote query, the **Data Description** of the **Value1** field is set to 0. For a local query, the **Data Description** of the **Value1** field is set to 1.

**Description:** NIDS: Web Service query

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: User DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier

Data Description: Requesting Provider ID

**Text2 (T):** Schema Title: Select String

Data Description: Requested attributes; select string

**Text3 (F):** Schema Title: Service Identifier

Data Description: Web Service URI

**Value1 (1):** Schema Title: Local

Data Description: 0 – Remote

1 – Local

**Group (G):** Schema Title: Query Group

Data Description: If this is a profile query, it contains the grouping ID for all attributes selected in this request. Otherwise, this field is not used in the event.

**Data Length (X):** 0

**Data (D):** null

## B.17 NIDS: Web Service Modify (002e0011)

This event is generated when you select the **Web Service Modify Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration. The Identity Server uses this event for two types of Web service modify requests:

- ♦ **Discovery:** This is a request to discover a service to modify. For this type of request, the **Group (G)** field is not used. For a remote request, the **Data Description** of the **Value1** field is set to 0. For a local request, the **Data Description** of the **Value1** field is set to 1.
- ♦ **Profile:** This is a request to modify the attributes of a user in a profile (personal, credential, etc.). For this type of request, the **Group (G)** field contains a GroupingID for all attributes selected in the request. A separate event is generated for each attribute select list in the modify request. For a remote request, the **Data Description** of the **Value1** field is set to 0. For a local request, the **Data Description** of the **Value1** field is set to 1.

**Description:** NIDS: Web Service modify

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier

Data Description: User DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Provider Identifier

Data Description: Requesting Provider ID

**Text2 (T):** Schema Title: Select String  
Data Description: Modified attributes select string

**Text3 (F):** Schema Title: Service Identifier  
Data Description: Web Service URI

**Value1 (1):** Schema Title: Local  
Data Description: 0 – Remote; 1 – Local

**Group (G):** Schema Title: Modify Group  
Data Description: If this is a profile modify, it contains the grouping ID for each attribute select list in the request. Otherwise, this field is not used in the event.

**Data Length (X):** 0

**Data (D):** null

## **B.18 NIDS: Connection to User Store Replica Lost (002e0012)**

This event is generated when you select the **LDAP Connection Lost** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Connection to user store replica lost

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Store Replica Name  
Data Description: Replica name

**SubTarget (Y):** null

**Text1 (S):** Schema Title: User Store Replica Host  
Data Description: IP Address of User Store replica server

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.19 NIDS: Connection to User Store Replica Reestablished (002e0013)**

This event is generated when you select the **LDAP Connection Reestablished** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Connection to user store replica reestablished

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Store Replica Name  
Data Description: Replica name

**SubTarget (Y):** null

**Text1 (S):** Schema Title: User Store Replica Host  
Data Description: IP Address of User Store replica server

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.20 NIDS: Server Started (002e0014)

This event is generated when you select the **Server Started** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Server started

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Configuration Identifier  
Data Description: Configuration Object DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Server Identifier  
Data Description: Unique server ID also used to create Liberty and SAML artifacts

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.21 NIDS: Server Stopped (002e0015)

This event is generated when you select the **Server Stopped** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Server stopped

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Configuration Identifier  
Data Description: Configuration object DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Server Identifier  
Data Description: Unique server ID also used to create Liberty and SAML artifacts

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.22 NIDS: Server Refreshed (002e0016)

This event is generated when you select the **Server Refreshed** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Server Refreshed

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Configuration Identifier  
Data Description: Configuration Object DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Server Identifier  
Data Description: Unique server ID also used to create Liberty and SAML artifacts

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.23 NIDS: Intruder Lockout (002e0017)

This event is generated when you select the **Intruder Lockout Detected** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Intruder Lockout

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier  
Data Description: User DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Server Identifier  
Data Description: IP address of the User Store replica server

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.24 NIDS: Severe Component Log Entry (002e0018)

This event is generated when you select the **Component Log Severe Messages** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Severe Component Log Entry

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Log Text  
Data Description: Server Error Text

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.25 NIDS: Warning Component Log Entry (002e0019)

This event is generated when you select the **Component Log Warning Messages** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Warning Component Log Entry

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Log Text  
Data Description: Warning Error Text

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.26 NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider as Identity Provider and Service Provider Are not in Same Group (002E001A)**

This event is generated when you select the **Brokering Across Groups Denied** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Failed to broker an authentication from identity provider to service provider as identity provider and service provider are not in same group

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier Data Description: User DN

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Identity Provider Identifier

Description : Identity Provider ID

**Text2 (T):** Schema Title: Service Provider Identifier

Description: Service Provider ID

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** Schema Title: Target URL Length Description: Byte length of the target URL

**Data (D):** Schema Title: Target URL Description: Target URL

## B.27 NIDS: Failed to Broker an Authentication from Identity Provider to Service Provider Because a Policy Evaluated to Deny (002E001B)

This event is generated when you select the **Brokering Rule Evaluated to Deny** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Failed to broker an authentication from identity provider to service provider because a policy evaluated to deny

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier Data Description: User DN

**SubTarget (Y):** Schema Title: Broker Group Name Description: Name of the Brokering Group

**Text1 (S):** Schema Title: Identity Provider Identifier

Description: Identity Provider ID

**Text2 (T):** Schema Title: Service Provider Identifier

Description: Service Provider ID

**Text3 (F):** Schema Title: Broker Policy Description: Name of the Broker Policy that evaluated to deny

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** Schema Title: Target URL Length Description: Byte length of the target URL

**Data (D):** Schema Title: Target URL Description: Target URL

## B.28 NIDS: Brokered an Authentication from Identity Provider to Service Provider (002E001C)

This event is generated when you select the **Brokering Handled** option under **Novell Audit Logging** on the Logging page of an Identity Server configuration.

**Description:** NIDS: Brokered an authentication from identity provider to service provider

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: User Identifier Data Description: User DN

**SubTarget (Y):** Schema Title: Broker Group Name Description: Name of the Brokering Group

**Text1 (S):** Schema Title: Identity Provider Identifier

Description: Identity Provider ID

**Text2 (T):** Schema Title: Service Provider Identifier

Description: Service Provider ID

**Text3 (F):** null



**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** Schema Title: Target URL Length Description: Byte length of the target URL

**Data (D):** Schema Title: Target URL Description: Target URL

## B.29 NIDS: Roles PEP Configured (002e0300)

This event is generated for Identity Server roles.

**Description:** NIDS: Roles PEP Configured

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** Schema Title: Policy Enforcement List Length

Data Description: Byte length of PEL

**Data (D):** Schema Title: Policy Enforcement List

Data Description: Policy Enforcement List (PEL) data

## B.30 Access Gateway: PEP Configured (002e0301)

This event is generated when you enable auditing.

**Description:** Access Gateway: policy enforcement point (PEP) configured

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Event Identifier

Data Description: Event Tracking Identifier

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** Schema Title: Audit Enabled

Data Description: 0 = No; 1 = Yes

**Group (G):** 0

**Data Length (X):** Schema Title: Policy Enforcement List Length  
Data Description: Byte length of PEL

**Data (D):** Schema Title: Policy Enforcement List  
Data Description: Policy Enforcement List (PEL) data

## B.31 Roles Assignment Policy Evaluation (002e0320)

This event is generated when you enable auditing.

**Description:** Roles assignment policy evaluation

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Assigned Roles  
Data Description: Assigned Role or error message

**Text3 (F):** Schema Title: Policy Action  
Data Description: Policy Action FDN

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.32 Access Gateway: Authorization Policy Evaluation (002e0321)

This event is generated when you enable auditing.

**Description:** Access Gateway: Authorization policy evaluation

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Text3 (F):** Schema Title: Policy Action  
Data Description: Policy Action FDN

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.33 Access Gateway: Form Fill Policy Evaluation (002e0322)**

This event is generated when you enable auditing.

**Description:** Access Gateway: Form Fill policy evaluation

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Text3 (F):** Schema Title: Policy Action  
Data Description: Policy Action FDN

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.34 Access Gateway: Identity Injection Policy Evaluation (002e0323)**

This event is generated when you enable auditing.

**Description:** Access Gateway: Identity Injection policy evaluation

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text2 (T):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Text3 (F):** Schema Title: Policy Action  
Data Description: Policy Action FDN

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.35 Access Gateway: Access Denied (0x002e0505)

This event is generated when you select the **Access Denied** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: Access Denied

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0505

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Protected Resource Name  
Data Description: Configured Name of Protected Resource

**SubTarget (Y):** Schema Title: Protected Resource URL  
Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier  
Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Source IP Address  
Data Description: User IP address (numeric format – host order)

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.36 Access Gateway: URL Not Found (0x002e0508)

This event is generated when you select the **URL Not Found** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: URL Not Found

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0508

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** Schema Title: Protected Resource URL

Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier

Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier

Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier

Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Source IP Address

Data Description: User IP address (numeric format – host order)

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.37 Access Gateway: System Started (0x002e0509)**

This event is generated when you select the **System Started** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: System Started

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0509

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.38 Access Gateway: System Shutdown (0x002e050a)

This event is generated when you select the **System Shutdown** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: System Shutdown

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e050a

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** null

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.39 Access Gateway: Identity Injection Parameters (0x002e050c)

This event is generated when you select the **Identity Injection Parameters** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: Identity Injection Parameters

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e050c

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** Schema Title: Protected Resource URL  
Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier  
Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Injection Location  
Data Description: 2710 – Auth Header 2720 – Custom Header  
2730 – Query Parameters

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.40 Access Gateway: Identity Injection Failed (0x002e050d)

This event is generated when you select the **Identity Injection Failed** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: Identity Injection Failed

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e050d

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** Schema Title: Protected Resource URL  
Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier  
Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Injection Location  
Data Description: 2710 – Auth Header 2720 – Custom Header  
2730 – Query Parameters

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.41 Access Gateway: Form Fill Authentication (0x002e050e)

This event is generated when you select the **Form Fill Success** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: Form Fill Authentication

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e050e

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Protected Resource Name  
Data Description: Configured name of protected resource

**SubTarget (Y):** Schema Title: Protected Resource URL  
Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier  
Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.42 Access Gateway: Form Fill Authentication Failed (0x002e050f)

This event is generated when you select the **Form Fill Failed** option on the Novell Audit page of an Access Gateway.



**Description:** Access Gateway: Form Fill Authentication Failed

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e050f

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** Schema Title: Protected Resource Name

Data Description: Configured name of protected resource

**SubTarget (Y):** Schema Title: Protected Resource URL

Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier

Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier

Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier

Data Description: Event Tracking Identifier

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.43 Access Gateway: URL Accessed (0x002e0512)

This event is generated when you select the **URL Accessed** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: URL Accessed

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0512

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** Schema Title: Protected Resource URL

Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier

Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Source IP Address  
Data Description: User IP address (numeric format – host order)

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.44 Access Gateway: IP Access Attempted (0x002e0513)

This event is generated when you select the **IP Access Attempted** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: IP Access Attempted

In the Event list (**Auditing and Logging** > **Logging Server Options** > **[Name of Novell Audit Secure Logging Server]** > **Novell Access Manager** > **Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0513

**Originator (B):** Schema Title: Originator  
Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** Schema Title: Protected Resource URL  
Data Description: Protected Resource URL

**Text1 (S):** Schema Title: User Identifier  
Data Description: User DN

**Text2 (T):** Schema Title: Authentication Identifier  
Data Description: IDP Session ID (AMAUTHID#auth\_id:)

**Text3 (F):** Schema Title: Event Identifier  
Data Description: Event Tracking Identifier

**Value1 (1):** Schema Title: Source IP Address  
Data Description: User IP address (numeric format – host order)

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.45 Access Gateway: Webserver Down (0x002e0515)

This event is generated when you select the **IP Access Attempted** option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: One of the Web servers is not reachable

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0515

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** WebServer hostname

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** WebServer IP Address

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.46 Access Gateway: All WebServers for a Service is Down (0x002e0516)

This event is generated when you select the IP Access Attempted option on the Novell Audit page of an Access Gateway.

**Description:** Access Gateway: All Web servers for a service are down

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0516

**Originator (B):** Schema Title: Originator

Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** WebServer Hostname

**Text2 (T):** null

**Text3 (F):** null

**Value1 (1):** WebServer IP address

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.47 Management Communication Channel: Health Change (0x002e0601)

This event is generated when you select the **Health Changes** option on the Access Manager Auditing page.

**Description:** Management Communication Channel: Health Change

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0601

**Originator (B):** Schema Title: Originator

Data Description: "devmanagement" (AMDEVICEID#devmanagement:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Changed Device

Data Description: IP address and device type of the changed device

**Text2 (T):** Schema Title: Old State

Data Description: Old State

**Text3 (F):** Schema Title: New State

Data Description: New State

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.48 Management Communication Channel: Device Imported (0x002e0602)

This event is generated when you select the **Server Imports** option on the Access Manager Auditing page.

**Description:** Management Communication Channel: Device Imported

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0602

**Originator (B):** Schema Title: Originator

Data Description: "devmanagement" (AMDEVICEID#devmanagement:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Device

Data Description: IP address and device type of the changed device

**Text2 (T):** blank string

**Text3 (F):** blank string

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.49 Management Communication Channel: Device Deleted (0x002e0603)

This event is generated when you select the **Server Deletes** option on the Access Manager Auditing page.

**Description:** Management Communication Channel: Device Deleted

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0603

**Originator (B):** Schema Title: Originator

Data Description: "devmanagement" (AMDEVICEID#devmanagement:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Device

Data Description: IP address and device type of the changed device

**Text2 (T):** Schema Title: Administrator

Data Description: DN of the administrator deleting the device

**Text3 (F):** blank string

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.50 Management Communication Channel: Device Configuration Changed (0x002e0604)

This event is generated when you select the **Configuration Changes** option on the Access Manager Auditing page.

**Description:** Management Communication Channel: Device Configuration Changed

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0604

**Originator (B):** Schema Title: Originator

Data Description: "devmanagement" (AMDEVICEID#devmanagement:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Device

Data Description: IP address and device type of the changed device

**Text2 (T):** Schema Title: Administrator

Data Description: DN of the administrator invoking the configuration change

**Text3 (F):** blank string

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.51 Management Communication Channel: Device Alert (0x002e0605)

This event is generated when you enable auditing.

**Description:** Management Communication Channel: Device Alert

In the Event list (**Auditing and Logging > Logging Server Options > [Name of Novell Audit Secure Logging Server] > Novell Access Manager > Events**), this column is called **Event Name**.

In a query, this column is called **EventID**.

**Event ID:** 0x002e0605

**Originator (B):** Schema Title: Originator  
Data Description: "devmanagement" (AMDEVICEID#devmanagement:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Device  
Data Description: IP address of the device generating the alert

**Text2 (T):** Schema Title: Alert Message  
Data Description: alert message string

**Text3 (F):** blank string

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.52 SSL VPN: Common Logs (002e0701)

This event is generated when you enable **Command Line Interface Debug Logs, Connection Manager Logs, Certificate Management Debug Logs, Command Line Interface Logs, Certificate Management Logs** or **SSL VPN Incoming Connections Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Common logs

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.53 SSL VPN: Extended Logs (002e0702)

This event is generated when you enable **Authentication Logs, SSL VPN Incoming Connections Debug Logs, Cluster Logs, Servlet Communications Logs** or **Other SSL VPN Gateway Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Extended logs

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.54 SSL VPN: Servlet Status (002e0706)

This event is generated when SSL VPN Servlet starts. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet status

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.55 SSL VPN: Servlet Connection Added (002e0707)

This event is generated when a new user session is added to the Connection Manager. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet connection added

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)



**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.56 SSL VPN: Servlet Connection Failed (002e0708)

This event is generated when adding a new user session to the Connection Manager fails. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet connection failed

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.57 SSL VPN: Servlet Connection Removed (002e0709)

This event is generated when a user session is removed from the Connection Manager. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet connection removed

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.58 SSL VPN: Cluster Node Status (002e070A)

This event is generated when a node connects to other members in the cluster. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Cluster node status

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.59 SSL VPN: Servlet New Session Created (002e070B)

This event is generated when a new Tomcat session is created. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet new session created

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.60 SSL VPN: Servlet Session Replicated (002e070C)

This event is generated when a Tomcat session is shared among other members of the cluster. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet new session replicated

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.61 SSL VPN: Servlet Session Removed (002e070D)

This event is generated when a Tomcat session is removed from other members of the cluster. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet session removed

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.62 **SSL VPN: Servlet State Transfer Started (002e0710)**

This event is generated when duplicating a Tomcat session from other members of the cluster is started. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet state transfer started

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## B.63 **SSL VPN: Servlet State Transfer Completed (002e0711)**

This event is generated when duplicating a Tomcat session from other members of the cluster is complete. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet state transfer completed

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.64 SSL VPN: Servlet Cluster Node Is Down (002e0712)**

This event is generated when a Servlet cluster node is down. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet Cluster node is down

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.65 SSL VPN: Servlet Cluster Node Is Restarted (002e0713)**

This event is generated when a Servlet cluster node is restarted. To enable logging of this event, select **Cluster Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet Cluster node is restarted

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.66 SSL VPN: Servlet Cluster Error with Reason (002e0714)**

This event is generated when an error occurs during authenticating a user. To enable logging of this event, select **Authentication Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet cluster error with reason

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.67 SSL VPN: Servlet Service Provider Authenticated User (002e0715)**

This event is generated when a user session is authenticated. To enable logging of this event, select **Authentication Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet service provider authenticated user

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.68 SSL VPN: Servlet New Authenticated Connection Received (002e0716)**

This event is generated when an authenticated Access Gateway user session is received. To enable logging of this event, select **Authentication Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet new authenticated connection received

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null

## **B.69 SSL VPN: Servlet Service Provider Re-authenticated User (002e0717)**

This event is generated when a user session is re-authenticated. To enable logging of this event, select **Authentication Logs** on the Novell Audit Settings page for a SSL VPN.

**Description:** SSL VPN: Servlet service provider re-authenticated user

**Originator (B):** Schema Title: Originator Data Description: JCC Device ID (AMDEVICEID#device\_id:)

**Target (U):** null

**SubTarget (Y):** null

**Text1 (S):** Schema Title: Component Description: SSL VPN SERLET (SSL VPN Component)

**Text2 (T):** Schema Title: Message Description: Audit Event Message String

**Text3 (F):** null

**Value1 (1):** 0

**Group (G):** 0

**Data Length (X):** 0

**Data (D):** null