

NetIQ eDirectory 9.0 Release Notes

January 2016



NetIQ eDirectory 9.0 includes new features and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the eDirectory Community Support Forums, our community Web site that also includes product notifications, blogs, and product user groups.

For a full list of all issues resolved in NetIQ eDirectory 9.x, including all patches and service packs, refer to [TID 7016794, "History of Issues Resolved in NetIQ eDirectory 9.x"](#).

For more information about this release and for the latest release notes, see the [Documentation](#) Web site. To download this product, see the [Product Upgrade](#) Web site.

1 What's New?

eDirectory 9.0 provides the following key features, enhancements, and fixes in this release:

1.1 New features

This release introduces the following new features:

- ♦ [Suite B Support](#)
- ♦ [Enhanced Background Authentication](#)
- ♦ [Federal Information Processing Standard 140-2 Certification](#)
- ♦ [Proxied Authorization Control](#)
- ♦ [Monitoring](#)
- ♦ [Container Readiness](#)
- ♦ [Enhanced Nested Groups](#)

1.1.1 Suite B Support

This release introduces support for configuring the eDirectory components to use the cryptographic algorithms that Suite B mandates. The Suite B algorithms ensure the security of classified and unclassified information passed through public networks. For more information, see [Configuring eDirectory in Suite B Mode](#) in the [NetIQ eDirectory Administration Guide](#).

IMPORTANT: Suite B standard is subject to change. Be aware that NSA (National Security Agency) may change their recommendations in future. Suite B support in eDirectory 9.0 is based on our interpretation of NSA recommendations.

1.1.2 Enhanced Background Authentication

This release introduces a standards-based background authentication mechanism called Enhanced Background Authentication (EBA) for single sign-on authentication with eDirectory. This mechanism enables you to overcome the limitations of proprietary background authentication material.

Using EBA, eDirectory issues users an X.509 certificate as the background authentication material and the background authentication protocol uses TLS version 1.2 for mutual authentication. EBA is disabled by default. To enable it, see [Enabling Enhanced Background Authentication](#) in the [NetIQ eDirectory Administration Guide](#).

1.1.3 Federal Information Processing Standard 140-2 Certification

eDirectory 9.0 leverages the Federal Information Processing Standards (FIPS) 140-2 compliant features to meet the security requirements of U.S. Federal agencies and customers with highly secure environments. For more information, see [Operating eDirectory in FIPS Mode](#) in the [NetIQ eDirectory Installation Guide](#).

1.1.4 Proxied Authorization Control

eDirectory now provides you the flexibility for controlling proxy authorization through the LDAP protocol as specified in [RFC 4370](#). The proxied authorization control allows a client to request that an operation be processed under a provided authorization identity instead of under the current authorization identity associated with the connection. The feature provides a mechanism for specifying an authorization identity on a per-operation basis, benefiting clients that need to perform operations efficiently on behalf of multiple users.

1.1.5 Monitoring

This release introduces an LDAP search method for retrieving the real time statistics for eDirectory subsystems and background processes such as Threadpool, Connection Table, Dclient, DS Agent, and LDAP Server. By using this common interface, you can monitor the status of eDirectory modules and operations. eDirectory supports this feature on LDAP protocol and only an LDAP client can place requests for monitoring data. For more information, see [Monitoring eDirectory](#) in the [NetIQ eDirectory Administration Guide](#).

1.1.6 Container Readiness

In past, if you searched for an eDirectory attribute whose automatic movement to Attribute Container was in progress, the LDAP search displayed a 6029 error for that attribute. While automatic containerization of attributes worked well for small deployments, it was time consuming for large deployments. eDirectory 9.0 provides you the flexibility of scheduling the attribute movement. You first view the attributes that are ready to be moved and then schedule their movement as per your convenience. For more information, see [FLAIM Attribute Containerization](#) in the [NetIQ eDirectory Tuning Guide](#).

1.1.7 Enhanced Nested Groups

The Nested Groups feature is enhanced to allow a dynamic group or a nested group to be a member of another dynamic or a nested group to be nested to many levels. It is also possible to assign the ACL rights to the member objects of the nested groups.

1.2 Enhancements

This release introduces the following enhancements:

- ♦ [Section 1.2.1, “Performance Enhancement in Nested Groups,” on page 3](#)
- ♦ [Section 1.2.2, “Performance Enhancement in Data Replication,” on page 3](#)
- ♦ [Section 1.2.3, “Performance Enhancement in Rebuilding the Change Cache,” on page 3](#)
- ♦ [Section 1.2.4, “Improved Data Synchronization,” on page 3](#)
- ♦ [Section 1.2.5, “Optimized Janitor Thread for Inherited ACL Calculation,” on page 3](#)

1.2.1 Performance Enhancement in Nested Groups

This release improves the performance of searching large number of nested groups that do not have any nested group members associated with them.

1.2.2 Performance Enhancement in Data Replication

To communicate among various servers, eDirectory uses NetWare Core Protocol (NCP) as the communication protocol. In previous releases, NCP allowed maximum packet size of 64 KB, which limited the maximum throughput when data was transferred over NCP. This release improves the ability of NCP to handle packet size up to 1 MB, which enables eDirectory to synchronize up to 1 MB data in a single packet. eDirectory starts synchronizing with 64 KB packet size and increases the packet size based on the remaining data to be synchronized. This significantly improves the replication performance.

1.2.3 Performance Enhancement in Rebuilding the Change Cache

This release maximizes CPU utilization that significantly reduces the time taken by the change cache to rebuild.

1.2.4 Improved Data Synchronization

In previous releases of eDirectory, eDirectory accumulated data changes for five minutes or longer before data synchronization was scheduled. With eDirectory 9.0, data synchronization has been enhanced to schedule immediately after the data transaction completes successfully.

1.2.5 Optimized Janitor Thread for Inherited ACL Calculation

In this release, the Janitor thread is enhanced to process the ACLs sequentially from the partitions. This enables the Janitor thread to immediately release the DIB lock after processing the ACLs from a partition. When the DIB is optimally locked, it remains available for other operations resulting in improved performance. For more information about inherited ACLs, see [eDirectory Rights](#) in the [NetIQ eDirectory Administration Guide](#).

1.3 Fixed Issues

- ♦ [Section 1.3.1, “Login to iMonitor Needs eDirectory Restart,” on page 4](#)
- ♦ [Section 1.3.2, “Nested Members Are Excluded From the Dynamic Group Member Attribute,” on page 4](#)
- ♦ [Section 1.3.3, “SSL CertificateDNS Is Not Always Used for httpkeymaterialobject Attribute of the HTTP Server Object,” on page 4](#)

- [Section 1.3.4, “Unable To Configure Or Start eDirectory On SLES and RHEL Platforms When IPV6 Is Disabled,” on page 4](#)
- [Section 1.3.5, “Prolonged Member Search Time When baseDN Includes A Large Number Of Groups,” on page 5](#)
- [Section 1.3.6, “Simple Bind With No password Is Considered As Anonymous Bind,” on page 5](#)
- [Section 1.3.7, “Unable To Configure Character Limit For eDirectory Indexes,” on page 5](#)
- [Section 1.3.8, “eDirectory Crashes During Startup,” on page 5](#)
- [Section 1.3.9, “Wrong Value of IdapConfigVersion Attribute Causes eDirectory Upgrade Failure,” on page 5](#)
- [Section 1.3.10, “ndstrace Incorrectly Truncates Milliseconds in the Timestamp,” on page 5](#)
- [Section 1.3.11, “ndstrace with +LDAP Displays Error Message When LDAP Trace Options Are Set to Critical Error Messages,” on page 5](#)
- [Section 1.3.12, “XDAS Auditing Fails Over SSLv3 with Sentinel 7.3.1.0,” on page 6](#)

1.3.1 Login to iMonitor Needs eDirectory Restart

Issue: After changing the rights on the user object, the user is not able to log in to iMonitor without restarting eDirectory.

Fix: This issue is resolved. Users can successfully log in to the iMonitor after rights are changed on the user objects.

1.3.2 Nested Members Are Excluded From the Dynamic Group Member Attribute

Issue: After creating a dynamic group, if you query a nested group, the nested members are not listed in the Member attribute of the dynamic group except those who have direct memberships to the nested group.

Fix: This release updates eDirectory to include the nested members in the Member attribute of the dynamic group.

1.3.3 SSL CertificateDNS Is Not Always Used for httpkeymaterialobject Attribute of the HTTP Server Object

Issue: SSL Certificate DNS is used as a default certificate for the httpkeymaterialobject attribute of the HTTP server object. However, this certificate is not always selected for the httpkeymaterialobject attribute of the HTTP server object during eDirectory installation.

Fix: This release resolves this issue. This certificate is automatically selected for the httpkeymaterialobject attribute during eDirectory installation.

1.3.4 Unable To Configure Or Start eDirectory On SLES and RHEL Platforms When IPV6 Is Disabled

Issue: You cannot configure eDirectory or start an already configured eDirectory on SLES and RHEL platforms if IPV6 is disabled through sysctl.

Fix: This release updates eDirectory to resolve this issue.

1.3.5 Prolonged Member Search Time When baseDN Includes A Large Number Of Groups

Issue: Querying for members takes more time than usual when baseDN includes large number of groups.

Fix: This issue is fixed. eDirectory is optimized to improve the performance of the member query.

1.3.6 Simple Bind With No password Is Considered As Anonymous Bind

Issue: eDirectory treats simple bind with no password as anonymous bind.

Fix: This release resolves this issue. eDirectory now differentiates between simple bind with no password and anonymous bind.

1.3.7 Unable To Configure Character Limit For eDirectory Indexes

Issue: eDirectory sets 32-bit limit on the length of the substring index and considers an underscore as a white space. When you query the substring index, the query does not return the desired result if an attribute has a value greater than 32-bit and has an underscore.

Fix: This release updates eDirectory to resolve this issue.

1.3.8 eDirectory Crashes During Startup

Issue: eDirectory crashes immediately after starting due to invalid entries in the `nds.conf` file.

Fix: This release updates eDirectory to start without crashing.

1.3.9 Wrong Value of ldapConfigVersion Attribute Causes eDirectory Upgrade Failure

Issue: eDirectory upgrade fails due to the wrong value in the `ldapConfigVersion` attribute.

Fix: This release resolves this issue. The `ldapConfigVersion` attribute now includes the correct value and eDirectory upgrades successfully.

1.3.10 ndstrace Incorrectly Truncates Milliseconds in the Timestamp

Issue: `ndstrace` truncates the milliseconds in the timestamp when the first digit of the milliseconds in the time stamp is a zero. It does not print the zero.

Fix: This issue is fixed. `ndstrace` no longer truncates milliseconds in the timestamp.

1.3.11 ndstrace with +LDAP Displays Error Message When LDAP Trace Options Are Set to Critical Error Messages

Issue: `ndstrace` with `+LDAP` displays non-critical messages when LDAP Trace options are set to display critical error messages.

Fix: This release resolves this issue. `ndstrace` is enhanced to display error messages according to the specified trace options.

1.3.12 XDAS Auditing Fails Over SSLv3 with Sentinel 7.3.1.0

Issue: XDAS auditing fails over SSLv3 with Sentinel 7.3.1.0. This issue occurs because this version of Sentinel no longer supports SSLv2 and SSLv3.

Fix: This issue is fixed. XDAS is updated to use SSLv23 to audits events to Sentinel 7.3.1.0.

1.4 System Requirements

For information about prerequisites, hardware requirements, and supported operating systems, see the [NetIQ eDirectory Installation Guide](#).

IMPORTANT: eDirectory 9.0 does not support Identity Manager 4.5.x.

1.5 Supported Upgrade Paths

To upgrade to eDirectory 9.0, you need to be either on eDirectory 8.8 or higher. For more information on upgrading eDirectory, see the [NetIQ eDirectory Installation Guide](#).

2 Installing eDirectory 9.0

Log in to the [NetIQ Downloads](#) page and follow the link that allows you to download the software. The following files are available:

Table 1 Files Available for eDirectory 9.0

Filename	Description
eDirectory_900_Linux_x86_64.tar.gz	Contains the eDirectory tar file for Linux platforms.
eDirectory_900_Windows_x86_64.exe	Contains the eDirectory executable file for Windows platforms.
eDir_IMANPlugins.npm	Contains the iManager plug-in npm. Install the NPM as directed in the NetIQ iManager Installation Guide .

3 Known Issues

The following sections provide information on known issues at the time of the product release.

3.1 Known Issues on Linux

- [Section 3.1.1, “eDirectory Dumps the Core on Loading xdasauditds When the Syslog Appender Is Disabled,” on page 7](#)
- [Section 3.1.2, “SNMP Fails on RHEL 6.6 and Above Platforms,” on page 7](#)
- [Section 3.1.3, “Identity Manager Fails to Start When Updated with Non Root eDirectory 9.0,” on page 7](#)
- [Section 3.1.4, “eDirectory Configuration Fails on SLES 12 and RHEL 7 If the Configuration File Path Contains a Hyphen,” on page 7](#)
- [Section 3.1.5, “eDirectory Utilities Require Users to Authenticate Using NDS Password,” on page 7](#)

- [Section 3.1.6, “Non-Root User is Not Supported on RHEL 7 Platform,” on page 7](#)
- [Section 3.1.7, “SLPD Provided with SLES 12 and RHEL 7 Platforms Does Not Work,” on page 8](#)
- [Section 3.1.8, “Executing the ndspath Script from a Directory Containing opt May Export Wrong Paths,” on page 8](#)
- [Section 3.1.9, “Duplicate Files Are Created after Upgrading from eDirectory 8.8 SP8 to eDirectory 9.0,” on page 8](#)
- [Section 3.1.10, “Localhost Issues in /etc/hosts,” on page 8](#)
- [Section 3.1.11, “LDAP, TCP, and TLS Ports Issue with Large DIBs,” on page 8](#)
- [Section 3.1.12, “Uninstallation Fails if Installation Was Not Successfully Completed,” on page 9](#)

3.1.1 eDirectory Dumps the Core on Loading xdasauditds When the Syslog Appender Is Disabled

Issue: ndsd dumps the core when it attempts to load the `xdasconfig.properties` file in which the layout definition for Syslog is not defined correctly.

Workaround: There is no workaround at this time.

3.1.2 SNMP Fails on RHEL 6.6 and Above Platforms

Issue: This occurs because of an issue with the SNMP modules that RedHat provides.

Workaround: Install the latest RHEL patch from the Red Hat update service. For more information about this workaround, see [TID 7011659 \(https://www.netiq.com/support/kb/doc.php?id=7011659\)](https://www.netiq.com/support/kb/doc.php?id=7011659).

3.1.3 Identity Manager Fails to Start When Updated with Non Root eDirectory 9.0

Issue: The non-root installation of eDirectory 9.0 contains an empty `<eDirectory install path>/sbin/pre_ndsd_start`. The paths for Identity Manager are not set and, therefore, the Identity Manager fails to start.

Workaround: For more information about this workaround, see [TID 7016136 \(https://www.netiq.com/support/kb/doc.php?id=7016136\)](https://www.netiq.com/support/kb/doc.php?id=7016136).

3.1.4 eDirectory Configuration Fails on SLES 12 and RHEL 7 If the Configuration File Path Contains a Hyphen

Issue: eDirectory configuration fails if the configuration file path contains a hyphen.

Workaround: There is no workaround at this time.

3.1.5 eDirectory Utilities Require Users to Authenticate Using NDS Password

Issue: eDirectory utilities require users to authenticate through NDS password.

Workaround: If Universal Password is being used, synced it with the `NDS password` for all eDirectory command line tools to authenticate.

3.1.6 Non-Root User is Not Supported on RHEL 7 Platform

Issue: RHEL 7 does not allow starting services for a non-root user. So eDirectory does not support a non-root user on this platform.

Workaround: There is no workaround at this time.

3.1.7 SLPD Provided with SLES 12 and RHEL 7 Platforms Does Not Work

Issue: SLPD provided with SLES 12 and RHEL 7 platforms does not work after installing eDirectory on these platforms.

Workaround: To get the SLPD working, either build your own version of SLPD after downloading it from the [OpenSLP website \(http://www.openslp.org/\)](http://www.openslp.org/) on your platform or contact NTS for further assistance.

3.1.8 Executing the ndspath Script from a Directory Containing opt May Export Wrong Paths

Issue: If you run the ndspath script from a directory containing opt, sometimes the script does not export the correct paths.

Workaround: To export the correct paths, run the script from the binary location.

3.1.9 Duplicate Files Are Created after Upgrading from eDirectory 8.8 SP8 to eDirectory 9.0

Issue: After upgrading eDirectory, the new configuration files have a `.new` extension.

Workaround: If there are any changes to the configuration files, merge them with the new files.

3.1.10 Localhost Issues in /etc/hosts

If you have a loopback address alias to the hostname of the system in an `/etc/hosts` entry, it must be changed to the hostname or IP address. That is, if you have an entry similar to the one below in your `/etc/hosts` file, it needs to be changed to the correct entry given in second example below.

The following example has problems when any utility tries to resolve to the ndsd server:

```
127.0.0.1 test-system localhost.localdomain localhost
```

The following is a correct example entry in `/etc/hosts`:

```
127.0.0.1 localhost.localdomain localhost
10.77.11.10 test-system
```

If any third-party tool or utility resolves through localhost, it needs to be changed to resolve through a hostname or IP address and not through the localhost address.

3.1.11 LDAP, TCP, and TLS Ports Issue with Large DIBs

When the DIB is large, the DS takes time to come up and wrongly displays the following errors:

```
LDAP TCP Port is not listening
```

```
LDAP TLS Port is not listening
```

In this scenario, the ports are not disabled but eDirectory services are slow to come up. To check the status of LDAP, refer to the `ndsd.log` file or enter the following command and grep for the LDAP TCP/TLS ports:

```
netstat -na
```


3.1.12 Uninstallation Fails if Installation Was Not Successfully Completed

Issue: If eDirectory installation fails, nds-uninstall cannot remove eDirectory.

Workaround: Install eDirectory again in the same location and then uninstall it.

3.2 Known Issues on Windows

- ♦ [Section 3.2.1, “Manually Extending the Schema Before Installation,” on page 9](#)
- ♦ [Section 3.2.2, “Removing the Novell Client after eDirectory Installation,” on page 9](#)
- ♦ [Section 3.2.3, “Specifying eDirectory Information During the Installation,” on page 9](#)
- ♦ [Section 3.2.4, “Help Files Are Not Launched for Some Utilities,” on page 10](#)
- ♦ [Section 3.2.5, “Login Fails During Installation of the Secondary Server,” on page 10](#)
- ♦ [Section 3.2.6, “eDirectory Installation Fails From a Path Containing Non-ASCII Characters,” on page 10](#)
- ♦ [Section 3.2.7, “Missing rt.jar File Causes eDirectory Installation to Fail,” on page 10](#)
- ♦ [Section 3.2.8, “Installing eDirectory Stops SNMP,” on page 10](#)
- ♦ [Section 3.2.9, “eDirectory Upgrade Fails with an Error,” on page 10](#)
- ♦ [Section 3.2.10, “Issue while Invoking NDS Utilities,” on page 11](#)
- ♦ [Section 3.2.11, “eMBox Does Not Handle Double-Byte Characters,” on page 11](#)
- ♦ [Section 3.2.12, “Issues with Dsclusterconfig.exe Utility,” on page 11](#)

3.2.1 Manually Extending the Schema Before Installation

In some cases, schema extensions do not synchronize fast enough to the lower levels of a tree where the first new eDirectory 9.0 server is being installed, so some features are not completely installed.

Workaround: Extend the schema manually in your tree before you install eDirectory 9.0, using the eDirectory 9.0 schema files located in the `<Unzip Location>\Novell\NDS\x64` folder.

For more information on extending the schema, see [“Extending the Schema on Windows”](#) in the *NetIQ eDirectory Administration Guide*.

3.2.2 Removing the Novell Client after eDirectory Installation

When eDirectory 9.0 is installed on a Windows computer already containing the Novell Client, eDirectory installs an SLP service, but sets the service to manual mode so that it does not run when the server is booted. eDirectory then uses the SLP service from the Novell Client. If the Novell Client is removed, leaving no SLP service for eDirectory to use, you must manually start the SLP service, or change it to start automatically when the server boots.

3.2.3 Specifying eDirectory Information During the Installation

When specifying the eDirectory information during the installation, if an invalid Server object container type is specified, the installation does not detect the error until later, and the eDirectory installation fails with a -611 or -634 error.

The valid Server object container types are:

- ♦ Organization (O)

- ♦ Organizational Unit (OU)
- ♦ Domain (DC)

3.2.4 Help Files Are Not Launched for Some Utilities

This is observed for utilities such as DSRepair, DSMerge, and DSBrowse.

Workaround: To view the help files for these utilities, navigate to the folder where the files are located. Double-click the files to open the files. For example, `C:/Novell/NDS/NLS/Nihongo` for the Japanese help file.

3.2.5 Login Fails During Installation of the Secondary Server

If the login fails during the secondary server installation, click the **Browse** button next to the **Administrator Login Name** dialog box. After this, you might see an error message and a dialog box prompting you to enter an IP address. Enter the IP address of any server in the tree, preferably the Master server of the partition to which the server is being added.

If the server is running on a port number other than 524, enter the port number as well such as `1.2.3.4:1524`. This connects to the server, displays the tree name, and prompts for a login name and password. Follow the dialog boxes to continue with the installation. Ensure that the time between the primary and secondary servers is synchronized.

3.2.6 eDirectory Installation Fails From a Path Containing Non-ASCII Characters

eDirectory installation fails when the install files are run from a path that contains double-byte or extended ASCII characters.

3.2.7 Missing rt.jar File Causes eDirectory Installation to Fail

The installer fails to find the correct path to load the `rt.jar` file.

Workaround: This issue does not occur if the eDirectory installation folder has a relatively short path. For example, eDirectory installation can fail if the length of the folder path is more than 115 characters.

3.2.8 Installing eDirectory Stops SNMP

SNMP stops working after installing eDirectory and displays the following error message:

```
SNMP subagent error -672
```

Workaround:

- 1 Install and configure SNMP service after eDirectory is installed.
- 2 Run the `dssnmppsupport.exe` on your eDirectory server.

NOTE: Apply `dssnmppsupport.exe` only if `MpsSvc` service is running on the eDirectory server.

3.2.9 eDirectory Upgrade Fails with an Error

Issue: While upgrading eDirectory, the installer displays the following error:

```
Admin user does not have enough rights to modify the tree schema.
```

Workaround:

- 1 From the Administrator Login page of eDirectory installation, browse to and select the admin user.
- 2 Specify the password, then click *Next* to continue.

3.2.10 Issue while Invoking NDS Utilities

Issue: When you invoke any of the eDirectory utilities except DSTrace and DSRepair, the Interactive dialog box appears.

To launch and continue using the invoked utility, click *Show me the message* in the Interactive dialog box.

Windows Server 2012 and Windows Server 2012 R2 do not allow interactive services by default.

Workaround: To allow interactive services, go to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows and change
NoInteractiveServices from 1 to 0. Reboot the computer to start the interactive services detection service.

NOTE: When configuring the Directory Agent for eDirectory module (ds.dlm), ensure that you exit the ds.dlm dialog box to continue using the eDirectory services.

3.2.11 eMBox Does Not Handle Double-Byte Characters

Issue: The NetIQ eDirectory Management Toolbox (eMBox) does not handle double-byte characters for setting a roll-forward directory through the eMBox client and iManager.

Workaround: Use DSBK for setting a roll-forward directory.

3.2.12 Issues with Dsclusterconfig.exe Utility

- ♦ [Section 3.2.12.1, "Dsclusterconfig.exe Utility Does Not Accept All Terminal Options in French," on page 11](#)
- ♦ [Section 3.2.12.2, "Dsclusterconfig.exe Utility Does Not Support Japanese Locale," on page 11](#)

3.2.12.1 Dsclusterconfig.exe Utility Does Not Accept All Terminal Options in French

Issue: In a French localized Windows environment, if you try to run the utility for configuring eDirectory on a cluster (dsclusterconfig.exe), the localized o option does not work.

Workaround: Provide the corresponding English y option to run the utility.

3.2.12.2 Dsclusterconfig.exe Utility Does Not Support Japanese Locale

Issue: If you use the dsclusterconfig.exe utility in a Japanese localized Windows environment, the utility displays corrupted Japanese characters in the Windows terminal.

Workaround: Change the localization settings to English in the utility.

3.3 Common Issues on Linux and Windows

- ♦ [Section 3.3.1, "eDirectory Does Not Log an Event For a Failed Login," on page 12](#)
- ♦ [Section 3.3.2, "Symantec Network Threat Protection Conflicts with IPv6," on page 12](#)

- [Section 3.3.3, “Instrumentation Upgrade Issues While Upgrading eDirectory,” on page 12](#)
- [Section 3.3.4, “Default Listeners for New Network Interface,” on page 12](#)
- [Section 3.3.5, “Using eDirectory 9.0 with a Firewall Enabled,” on page 12](#)
- [Section 3.3.6, “Passwords Stored in ndspassstore Do Not Work after Upgrade,” on page 13](#)
- [Section 3.3.7, “Some Utilities Do Not Connect To LDAPS Port Over IPv6,” on page 13](#)
- [Section 3.3.8, “EBA Is Not Functional After Renaming an eDirectory Tree,” on page 13](#)
- [Section 3.3.9, “EBA Enabled Servers Use Secure NCP Channel for Encrypted Replication,” on page 13](#)
- [Section 3.3.10, “Switching Between Tabs in the DHost Console Does Not Refresh the DLMs,” on page 13](#)

3.3.1 eDirectory Does Not Log an Event For a Failed Login

Issue: By default, eDirectory disables logging for a failed login event.

Workaround: Configure the Nsure Audit settings for eDirectory to log the Add Value events in the NCP server object. You also need to enable the intruder detection on containers where auditing of these events is required. For more information, see [TID 7017208](#).

3.3.2 Symantec Network Threat Protection Conflicts with IPv6

Issue: Symantec network threat protection conflicts with IPv6 addresses.

Workaround: If you want to use IPv6 addresses in iManager 3.0, and your computer is running Network Threat Protection process, you must disable this process.

3.3.3 Instrumentation Upgrade Issues While Upgrading eDirectory

Issue: If you upgrade an eDirectory server on which the eDirectory instrumentation is also installed, the eDirectory instrumentation files are not upgraded automatically.

Workaround: Upgrade the eDirectory instrumentation files manually.

NOTE: eDirectory instrumentation is automatically installed with Identity Manager 4.0.

For more information on upgrading the instrumentation, refer to the [NetIQ eDirectory Installation Guide](#).

3.3.4 Default Listeners for New Network Interface

Issue: eDirectory listens on all interfaces configured on the computer for NCP, HTTP, HTTPS, LDAP and LDAPS by default.

Workaround: Adding a new network interface address to the computer, and restarting eDirectory will make it start listening on that address automatically and have referrals also added correspondingly.

3.3.5 Using eDirectory 9.0 with a Firewall Enabled

Issue: When you try to add an eDirectory 9.0 server from a computer to an existing tree running on a different computer, it might fail if the firewall is enabled.

Workaround: There is no workaround at this time.

3.3.6 Passwords Stored in ndspassstore Do Not Work after Upgrade

Issue: After upgrading eDirectory to version 9.0, the passwords stored in ndspassstore do not work.

Workaround: Execute the ndspassstore command for the specific user after upgrading eDirectory. This overwrites the passwords making them usable.

3.3.7 Some Utilities Do Not Connect To LDAPS Port Over IPv6

Issue: ndsindex, nmashotpcnf, and krbLdapConfig utilities do not connect to LDAPS port over IPv6 after configuring with a certificate file.

Workaround: There is no workaround at this time.

3.3.8 EBA Is Not Functional After Renaming an eDirectory Tree

Issue: Renaming a tree after installing eDirectory and configuring an EBA-enabled server on the tree leaves EBA non-functional. eDirectory displays the following error message:

Download of EBA CA certificate failed. Error: -2109(UAP_ERR_NMAS_API_INIT_FAILED)

Workaround: Rename the tree to its original name. This restores the EBA functionality.

3.3.9 EBA Enabled Servers Use Secure NCP Channel for Encrypted Replication

Issue: By default, the EBA-enabled eDirectory servers use the traditional authentication method for encrypted replication.

Workaround: To use the EBA authentication, restart the servers. This establishes the EBA authentication.

3.3.10 Switching Between Tabs in the DHost Console Does Not Refresh the DLMs

Issue: If you switch between the Services and the Connections tab in the DHost console, the DLMs are not refreshed in the console. Switching the tabs eventually removes all the DLM's from the console.

Workaround: There is no workaround at this time.

4 Changes to Documentation

- ♦ [Section 4.1, "Revamped Documentation," on page 13](#)
- ♦ [Section 4.2, "iManager," on page 14](#)
- ♦ [Section 4.3, "Novell International Cryptographic Infrastructure \(NICI\)," on page 14](#)
- ♦ [Section 4.4, "eDirectory Issues on Open Enterprise Server \(UNIX only\)," on page 14](#)

4.1 Revamped Documentation

The eDirectory documentation has been revamped. Content from NMAS Administration Guide, Password Management Guide, and Certificate Server Guide is now part of the [eDirectory Administration Guide](#). Use the following links to access these chapters in the eDirectory Administration Guide:

- ♦ [NMAS](#)

- ♦ [Password Management](#)
- ♦ [Certificate Server](#)

4.2 iManager

For iManager information, refer to the [iManager online documentation](#).

4.3 Novell International Cryptographic Infrastructure (NICI)

The NICI Administration Guide is included in the [eDirectory documentation page](#).

4.4 eDirectory Issues on Open Enterprise Server (UNIX only)

For more information on eDirectory issues on Open Enterprise Server (OES), see [OES Readme \(http://www.novell.com/documentation/oes2/\)](#).

5 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.