# NetIQ Access Manager 3.1 SP5 Readme

January 2013

This Readme describes the NetIQ Access Manager 3.1 SP5 release.

## 1 What's New

The following outline the version of the dependent component, as well as issues resolved in this release.

### 1.1 Dependent Component

This release updates the Platform Agent. The versions available for Linux and Windows platforms are as follows:

- Linux: Version 2.0.2-69
- Windows: Version 2.0.2-68

### 1.2 Issues Fixed

Access Manager 3.1 SP5 includes the following software fixes that resolve several previous issues.

For the list of software fixes and enhancements in previous releases, see the following readmes:

- For 3.1 SP4 IR1 readme, see 3.1 SP4 IR1.
- For 3.1 SP4 readme, see 3.1 SP4.

### 1.3 Issues Fixed in the Administration Console

This release of Access Manager resolves an issue where the Administration Console establishes a large number of LDAP connections to eDirectory resulting in performance issues. (Bug 761356)

### 1.4 Issues Fixed in the Identity Server

This release of Access Manager includes the following software fixes that resolve several previous issues for the Identity Server.

### 1.4.1 Error Logging in to the Identity Server

**Issue:** The Identity Server login fails with an error message when you log in with a username that contains a / character. (Bug 748435)

**Fix:** You can now access a protected resource by logging in to the Identity Server with a username that contains a / character.

### 1.4.2 Issues With Excessive Logging When Log Level is Set to Warning

**Issue:** Excessive logging occurs in the `catalina.out` file when *Logging* is enabled in the Identity Server. (Bug 750535)

**Fix:** Excessive logging no longer occurs when the log level is set to Warning.

### 1.4.3 User Session Times Out after Logging In to the Identity Server

**Issue:** When the *Limit user session* is enabled, the user session times out. For example if *Authentication Timeout* and *Default Timeout* are defined on the contract for five minutes, the system does not ask you to reauthenticate after five minutes elapse. (Bug 781763)

**Fix:** When the user session times out you will be asked for the user credentials when you open a new browser or when a new user logs in.

### 1.4.4 PasswordFetch Class Fails in a Federated Environment

**Issue:** When you provision a new user in a federated environment, the PasswordFetch Class that is part of post authentication method fails the first time and works without any issues when the newly provisioned user logs in subsequently. (Bug 782221)

**Fix:** The PasswordFetch Class fetches the password the first time you log in.

### 1.4.5 XML Signature Validation Issue in SAML 2.0

**Issue:** While validating the XML signature, federated authentication through SAML 2.0 fails and displays a signature validation message. For more information, see CVE-2012-3314. (Bug 787161)

**Fix:** The session authentication occurs without any XML signature validation issues and displays the error code messages `Signature Verification failed` and `invalid signatures`.

### 1.4.6 User Provisioning Issues

**Issue:** User provisioning issues occur when a user is created on one LDAP server and a request to modify an attribute is initiated on another LDAP server. For example, a user is created on LDAP server A and the attribute modify request is initiated on LDAP server B. When eDirectory synchronization occurs, the user account is not available on LDAP server B and this causes user provisioning issues. (Bugs 744295)

**Fix:** The user creation and LDAP attribute modify request now handled on the same LDAP server when more than one LDAP server replicas are configured for a user store.

## 1.5 Issues Fixed in the Access Gateway Service

This release of Access Manager includes the following software fixes that resolve several previous issues in the Access Gateway Service.

### 1.5.1 ActiveMQ Web Console Goes into a Non-Responding State due to Many Open Files

**Issue:** When *Auditing* is enabled, each child process of Apache requests ActiveMQ for creating a queue. ActiveMQ creates a queue depending on the process ID and assigns a queue ID. When Apache restarts, the child process again requests ActiveMQ to create the queue with the process ID. Over a period of time, ActiveMQ becomes non-responsive. (Bug 746349)

**Fix:** Each httpd child process does not request the ActiveMQ process to create queues.

### 1.5.2 Data Posted is Lost When the Size Exceeds Parking Limit

**Issue:** During the authentication process, if the data posted to the Access Gateway exceeds 50 KB, the data is lost. (Bug 756739, 786102)

**Fix:** The Access Gateway now accepts data up to 64 KB.

### 1.5.3 Extended Logging Cannot be Configured for Path-Based Proxies

**Issue:** Path based proxy service uses the log profile of the parent proxy and ignores the log profile assigned to it. (Bug 757251, 778471)

**Fix:** The Access Gateway now uses the log profile assigned to the path. The common and or extended logs are now created under `var/log/novell/reverse/` directory.

### 1.5.4 Extended Logging Displays Incorrect Data

**Issue:** Incorrect data is displayed in the log data options. (Bug 765432)

**Fix:** The issue with data in the log data options is resolved.

### 1.5.5 Query String Injection Policy Corrupts Existing Parameter Values

**Issue:** The existing query parameter values are corrupted if a request to the Access Gateway Service from a browser has a query string that matches the data injected by the Identity Injection policy. (Bug 764475)

**Fix:** The existing query string does not get corrupted after the query string is injected.

### 1.5.6 LogoutSuccess Page is not Displayed

**Issue:** Linux Access Gateway does not display the LogoutSuccess page while accessing AGLogout with a third-party SAML 2.0 service provider. SAML 2.0 supports only front channel logout. (Bug 778971)

**Fix:** Linux Access Gateway now displays the LogoutSuccess page.

### 1.5.7 Configuration Changes on Access Gateway Service Leads to Apache Restart

**Issue:** Any configuration changes on the Access Gateway Service cause Apache services to restart. This causes service interruption. (Bug 778478)

**Fix:** Configuration changes made on the Access Gateway Service, do not cause service interruption.

### 1.5.8 302 Redirect Occurs after Updating the Configuration

**Issue:** ESP clears the cached session and failover details after each configuration request due to a change in the Access Gateway configuration. This results in 302 redirects for existing sessions. After the Identity Server configuration is updated, it results in a 302 error. (Bug 780133)

**Fix:** ESP does not clear the existing session details after updating the configuration.

### 1.5.9 Email Notifications Sent to All Profiles

**Issue:** The Access Gateway sends email notifications to all profiles even if the alert profile was not configured. (Bug 783350)

**Fix:** The email notifications are now sent only to profiles that are configured.

### 1.5.10 Page Redirection Error while Accessing a Resource

**Issue:** The following issues occur while accessing a resource: (Bug 786658)

- Mozilla Firefox: The Mozilla Firefox browser displays `The page isn't redirecting properly` error.
- Internet Explorer: In Internet Explorer, the redirection results in an infinite loop. This happens during the login process after the server submits credentials to the Identity Server.

**Fix:** Session information is updated in the Identity Server.

### 1.5.11 HTTP Log Rollover Issues

**Issue:** You cannot specify the time for *Roll Over Options* in a local time zone. (Bug 786692)

**Fix:** The local time zone specified for rollover is now accepted.

### 1.5.12 Navigation Page of Vibe Appears Intermittently

**Issue:** The header page of Vibe does not load, creating issues in displaying the Vibe navigation page. (Bug 786857)

**Fix:** The issue with memory pointers is resolved. The pages load without error.

### 1.5.13 Provide a Way to Cache More Than 1 MB

**Issue:** Apache does not cache a file if the file size is more than 1 MB. (Bug 786858)

**Fix:** The Access Gateway Server now provides the advanced option `CacheMaxFileSize` with a default value of 5 MB. For more information on this advanced option, see "Advanced Access Gateway Service Options" in the *Novell Access Manager 3.1 SP5 Access Gateway Guide*.

### 1.5.14 Empty Authentication Header Variable Causes HTTP 500 error

**Issue:** If you try to access a protected or public resource that has an Identity Injection policy assigned before the authentication process is completed, then the users get an HTTP 500 error. (Bug 769430)

**Fix:** Ensure that `NAGGlobalOptions RemoveEmptyHeaderValue` is set to `on`. For more information about this option, see "Advanced Access Gateway Service Options" in the *Novell Access Manager 3.1 SP5 Access Gateway Guide*.

### 1.5.15 The Identity Server Is Not Updated With User Session Details of the Access Gateway Service

**Issue:** The Identity Server is not updated with the user session details of the Access Gateway Service and this causes the Identity Server to time out. (Bugs 773018, 768997)

**Fix:** This issue has been fixed by modifying the time-to-live calculations.

### 1.5.16 Non-Redirected Login Is Not Working

**Issue:** An Identity Injection policy configured for a protected resource with Non-Redirected Login works the first time, but fails during subsequent requests. This issue occurs because the session cache does not have complete information for Non-Redirected Login. (Bug 786855)

**Fix:** The session cache is now updated with Liberty ID and this is subsequently used in ESP policies.

## 1.6 Issues Fixed in the Linux Access Gateway Appliance

### 1.6.1 Failure to Rewrite AJAX Location Header

**Issue:** The system fails to rewrite the AJAX location header causing broken links. (Bug 727755)

**Fix:** The AJAX location header is now rewritten with the published DNS name.

### 1.6.2 Unmasking of Data does not Occur during Form Fill

**Issue:** When the data in the form you submit is sent to the Web server, the data values are masked instead of being displayed. (Bug 748657)

**Fix:** When the Access Gateway submits the data to the Web server, the masked values are displayed.

### 1.6.3 Client-Initiated Renegotiation Issues and Browser Exploit Against SSL/TLS Attacks

**Issue:** Client-initiated renegotiation issues and Browser Exploit Against SSL/TLS attack occur during SSL communication. (Bugs 763598, 765154)

**Fix:** To disable client renegotiation completely, use the `.disableClientRenego` touch file. To avoid Browser Exploit Against SSL/TLS attacks, configure the cipher setting in the `sslsettings.conf` file. For more information on these touch files see .disableClientRenego and Browser Exploit Against SSL/TLS Attack During SSL Communication in the *Novell Access Manager 3.1 SP5 Access Gateway Guide*. For more information on this vulnerability, see CVE-2011-3389.

### 1.6.4 Issues During Form Fill Process

**Issue:** During form fill, the following issues occur:

- If the data posted contains a `&` character, the Linux Access Gateway form fill process fails.
- If the data posted contains a space, it is encoded as a `+` character instead of `%20` character. The Linux Access Gateway form fill process fails. (Bug 766104)

**Fix:** The data is posted without any issues during form fill.

### 1.6.5 Linux Access Gateway Users Experience Downtime

**Issue:** If the audit events are enabled and the audit server is not reachable, Linux Access Gateway users experience downtime. (Bug 771341)

**Fix:** This downtime issue has been resolved.

### 1.6.6 Restart Issue with the ics_dyn Process

**Issue:** The 3.1.4 Linux Access Gateway channel to the Administration Console causes the ics_dyn process to restart. (Bug 777948)

**Fix:** The ics_dyn process issue is now resolved.

### 1.6.7 Form Fill Issues When Some Characters are Specified in the Password

**Issue:** Characters such as `"`, `$`, `#`, `&` specified in the password leads to form fill issues. (Bug 770889)

**Fix:** The password now accepts the specified characters and form fill occurs without any issues.

## 1.7 Issues Fixed in SSL VPN

This release of Access Manager resolves an issue where `Stunnel` does not start when you update the `libopenssl` security package. For more information, see TID 7010536. (Bug 773755)

# 2 Upgrading or Migrating to Access Manager 3.1 SP5

After you have obtained the Access Manager license, log in to the Novell Customer Center. Follow the link that allows you to download the software. Ensure that you are on Access Manager 3.1 SP4 or later before upgrading to Access Manager 3.1 SP5. You can migrate Access Manager 3.1 SP5 to Access Manager 3.2 SP1 IR1. For more information, see Section 2.2, “Migration Instructions,” on page 7.

The following files are available:

| Filename | Description |
|---|---|
| `AM_31_SP5_IdentityServer_Linux32.tar.gz` | Contains the Linux Identity Server the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN server. |
| `AM_31_SP5_IdentityServer_Win32.exe` | Contains the Windows Identity Server and Windows Administration Console for Window 2003. |
| `AM_31_SP5_IdentityServer_Win64.exe` | Contains the Windows Identity Server and Windows Administration Console for Windows 2008. |
| `AM_31_SP5_AccessGatewayAppliance_Linux_SLES11.iso` | Contains CD image for the SUSE Linux Enterprise Server (SLES) 11 version of the Access Gateway Appliance and the Traditional SSL VPN Server. Can be used only for installation. |
| `AM_31_SP5_AccessGatewayAppliance_Linux_SLES11.tar.gz` | Contains the upgrade RPMs for SLES 11 version of the Access Gateway Appliance and the traditional SSL VPN server. |
| `AM_31_SP4_AccessGatewayAppliance_Linux_SLES9.tar.gz` | Contains the upgrade RPMs for SLES 9 version of the Access Gateway Appliance and the Traditional SSL VPN server. |
| `AM_31_SP5_AccessGatewayService_Win64.exe` | Contains the Access Gateway Service for Windows Server 2008 R2 for a 64-bit operating system. |
| `AM_31_SP5_AccessGatewayService_Linux_64.bin` | Contains the Access Gateway Service for SLES 11 for a 64-bit operating system. |
| `AM_31_SP5_ApplicationServerAgents_AIX.bin` | Contains the Agents Service for AIX platform. |
| `AM_31_SP5_ApplicationServerAgents_Linux.bin` | Contains the Agents Service for Linux platform. |
| `AM_31_SP5_ApplicationServerAgents_Solaris.bin` | Contains the Agents Service for Solaris platform. |

| Filename | Description |
|---|---|
| `AM_31_SP5_ApplicationServerAgents_Windows.exe` | Contains the Agents Service for Windows platform. |

## 2.1 Upgrade Instructions

To upgrade to 3.1 SP5, ensure that you are using Access Manager 3.1 SP4 or later. For instructions on upgrading see "Upgrading Access Manager Components" in the *NetIQ Access Manager 3.1 SP5 Installation Guide*.

## 2.2 Migration Instructions

Complete the following steps to migrate Access Manager 3.1 SP5 to 3.2 SP1 IR1:

1. Migrate the Administration Console from 3.1.5 to 3.2 SP1. For more information, see Migrating Access Manager on SLES.
2. Upgrade the 3.2 SP1 Administration Console to 3.2 SP1 IR1. For more information, see Upgrading from Access Manager 3.2 SP1 to 3.2 SP1 IR1.
3. Migrate the other Access Manager components after upgrading the Administration Console to 3.2 SP1 IR1. For more information, see Migrating Access Manager on SLES.

## 2.3 Installation Instructions

For installation instructions of the Access Manager Administration Console, the Identity Server, the Access Gateway Appliance, the Access Gateway Service, and the SSL VPN server, see the *NetIQ Access Manager 3.1 SP5 Installation Guide*.

## 2.4 Verifying Version Numbers Before Upgrading

Before upgrading or migrating to Access Manager 3.1 SP5, ensure that you have upgraded all the components to Access Manager 3.1 SP4 or later.

To determine the existing version, complete the following steps:

**1** In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.

**2** Examine the value in the *Version* field. The following table indicates the versions that can be upgraded to 3.1 SP5.

| Component | 3.1 SP4 | 3.1 SP4 IR1 |
|---|---|---|
| Administration Console | `3.1.4.27` | `3.1.4.57` |
| Identity Server | `3.1.4.27` | `3.1.4.57` |
| Linux Access Gateway | `3.1.4.27` | `3.1.4.57` |
| Access Gateway Services | `3.1.4.27` | `3.1.4.57` |
| SSL VPN | `3.1.4.27` | `3.1.4.57` |

## 2.5 Verifying Version Numbers After Upgrading

After upgrading all the Access Manager components, verify the version as follows:

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version.*
2. Examine the value in the *Version* field to verify that the component has been upgraded to 3.1 SP5.

| Component | Version |
|---|---|
| Administration Console | 3.1.5.42 |
| Identity Server | 3.1.5.42 |
| Access Gateway Appliance | 3.1.5.42 |
| Access Gateway Services | 3.1.5.42 |
| SSL VPN | 3.1.5.42 |

# 3 Known Issues

The following table lists the known issues and workaround in Access Manager 3.1 SP5:

| Issue | Workaround |
|---|---|
| The lcache process (Novell Nsure Audit Platform agent) runs as a root user. But after the lcache process crashes, it runs as a non-root user. (Bug 770032) | For information on resolving this issue, see TID 7010978. |
| When you perform an LDAP query to the user store, the PasswordFetch class fails. (Bug 776183) | None. |
| An LDAP photo attribute is not injected into the HTTP custom header. (Bug 780739) | None. |
| When an alternate hostname is configured the first time, Access Gateway rewrites the referer header to the back-end Web server. During subsequent attempts, Access Gateway does not rewrite the referer header. (Bug 786086) | None. |
| When lcache runs out of memory or loses connection to the logging server, the health page does not display the health status. (Bug 786695) | None. |
| An un-authenticated user is not redirected to the login page while accessing the protected URL that contains the # character. (Bug 791063) | When the # character is replaced with `%23`, redirection works. |
| Authentication fails if a user bind request to the user store takes more than 15 seconds. (Bug 794290) | None. |
| The Access Gateway health check fails to check status of some of the back-end Web servers. (Bug 794482) | None. |

# 4 Documentation

The following sources provide information about Access Manager:

- Documentation Web Site.
- Access Manager Support. For TIDs and Cool Solutions articles, select *Access Manager* for the *Product* and *Articles / Tips* in the *Advanced Search* options.
- Novell Access Manager Product Site.

# 5 Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/).

All third-party trademarks are the property of their respective owners.