Access Manager 3.2 Service Pack 2 Readme

June 2013

Access Manager 3.2 Service Pack 2 includes new features, improves usability, 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 Access Manager forum on Qmunity (http://community.netiq.com/forums/30.aspx), our community Web site that also includes product notifications, blogs, and product user groups.

For the list of software fixes and enhancements in previous releases, see Access Manager 3.2 Service Pack 1 IR1a Readme.

For more information about this release and for the latest release notes, see the Documentation (http://www.netiq.com/support) Web site. To download this product, see the Product Upgrade (http://www.netiq.com/products) Web site.

1 What’s New?

The following outline the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Updates for Dependent Components

This version provides the following updated components:

- Novell Audit Platform Agent for Linux 2.0.2.69
- iManager 2.7.6
- Java 1.7.0_04
- Tomcat 7-7.0.32-1

1.2 Creating an Inject JavaScript Policy

The Inject JavaScript policy adds the configured JavaScript to a protected resource page, when used in interactive mode. You can create a standalone Inject JavaScript policy. You can also use this policy with the Form Fill policy. For more information on creating the JavaScript policy, see “Creating an Inject JavaScript Policy” in the *NetIQ Access Manager 3.2 SP2 Policy Guide*.

1.3 Shared Secret Type

While creating policies from the Administration Console, the Shared Secret Type option allows you to choose how the value you specified in the HTML form should be stored in the shared secret store. For more information, see “Shared Secret Type: ” in the *NetIQ Access Manager 3.2 SP2 Policy Guide*.

1.4 Multiple Signing and Encryption Certificates

In the previous release, you were forced to use the same signing certificate for all configured service providers. The Identity Server is now enhanced to support multiple signing and encryption certificates.

In SLES, the *Add* and *Remove* options are available only for Encryption and Signing certificates. The *Replace* option allows you to replace only the default certificates.

For more information, see Configuring Communication Security for a SAML 2.0 Service Provider and Managing Certificates in a Keystore.

1.5 Protecting Kerberized Resources with Kerberos Constrained Delegation

Protecting kerberized resources with KCD on Windows enhancement is provided in this release. For more information, see Protecting Kerberized Resources with Kerberos Constrained Delegation.

1.6 Configuring an Inject Kerberos Ticket Policy

Enhancements for creating and configuring an Inject Kerberos Ticket policy procedure is provided in this release. For more information see, "Configuring an Inject Kerberos Ticket Policy" in *NetIQ Access Manager 3.2 SP2 Policy Guide*.

1.7 Inclusion of a Message after Authentication

The Access Gateway has been enabled to display a post-authentication message. Now, after authentication, the Access Gateway displays the message `Authentication successful, please wait while your requested page loads` before final redirect to the originally requested URL.

For more information see, "Enabling the Access Gateway to Display Post-Authentication Message" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*

1.8 Programmatic Access to the Identity Server and the Access Gateway Appliance Statistics

Access Manager now supports programmatic access to the Identity Server statistics. To use this enhancement, enable the REST API. Access Manager is also enhanced to support a programmatic method to retrieve the statistics from an Access Gateway Appliance server. For more information, see "Monitoring API for the Access Gateway Statistics" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide* and "Monitoring API for the Identity Server Statistics" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

1.9 Verification Before Removing the Access Gateway from a Cluster

A confirmation prompt is now added for removing an Access Gateway from the cluster.

1.10 Tracking Average Local (LDAP) Authentication Time

The Identity Server statistic is now added for tracking average local (LDAP) authentication time. This enhancement also includes showing a graph of this statistic over time.

1.11 Encryption Method Selection From Metadata

From Access Manager 3.2 Service Pack 2 onwards, encryption uses the method and algorithm specified in the metadata of the service provider for encrypting the assertion. For more information on encrypt assertions, see "Configuring Communication Security for a SAML 2.0 Service Provider " in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

1.12 Increased Flexibility of URL Mask on Pin List

While configuring a pin list, you can do the following:

- Provide file extensions with path. For example, `/picture/*.gif`
- Include asterisks (*) in file names and extension. For example, `/documents/sd*sd.gif and /abc*ed`

For more information, see "URL Mask" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.

1.13 Change in Behavior of Protected Resource Path Matching

This release changes how Access Manager matches the configuration of a protected resource. If you have a protected resource configured with /path/portal/*, it will not match request URL with /path/portal. This behavioral change may cause SSO failure to backend Web server.

For example, let us assume you have Protected Resource (PR1) configured with `/path/portal/*` with Identity Injection policy for initiating an SSO to the backend Web server and you send the following requests:

1. (https://www.domain.com/path/portal)
2. (https://www.domain.com/path/portal/bob)

Prior to this release, both the requests matched PR1. With this release, request 1 does not match PR1 and hence SSO may fail if it requires an Identity Injection policy. To make it work, add an additional path in PR1 as `/path/portal` or you can modify `/path/portal/*` to `/path/portal*`. For more information, see TID 7012584.

1.14 Upgrading Kernel to the Latest Security Patch

The Access Manager Appliance installs a customized version of SLES 11. If you want to install the latest patches as they become available, see Upgrading Kernel to the Latest Security Patch in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1.15 Software Fixes for the Administration Console

Access Manager 3.2 Service Pack 2 includes software fixes that resolve several previous issues in the Administration Console.

- Section 1.15.1, “Cannot Add or Configure a Port to the Web Server Host Name,” on page 4

1.15.1 Cannot Add or Configure a Port to the Web Server Host Name

Issue: You cannot add or configure a port number along with the Web Server Host Name. (Bug 787378)

Fix: You can now append the port number to the Web Server Host Name field. For example, *<web server hostname>:<web server port number>*.

1.16 Software Fixes for the Identity Server

Access Manager 3.2 Service Pack 2 includes software fixes that resolve several previous issues in the Identity Server.

- Section 1.16.1, “Kerberos Fall Back to Basic Authentication Class Triggered After Fall back to Form Fails,” on page 5
- Section 1.16.2, “LDAP Unbind Request and Authentication Fails,” on page 5
- Section 1.16.3, “RADIUS Authentication Checks LDAP Password Before Token Validation,” on page 5
- Section 1.16.4, “PasswordFetchClass User Lookup Fails,” on page 5
- Section 1.16.5, “SAML ECP Profile is not Working for Office365,” on page 5
- Section 1.16.6, “The Identity Server Fails to Respond,” on page 5

1.16.1 Kerberos Fall Back to Basic Authentication Class Triggered After Fall back to Form Fails

Issue: When you configure a Kerberos contract with FALLBACK_AUTHCLASS by editing the Identity Server Cluster, it displays the default form-based authentication before the basic authentication UI is displayed. (Bug 790909)

Fix: To configure the basic authentication as a fall back authentication class, add any one of the following property:

Property Name: FALLBACK_AUTHCLASS

Property Value: Basic or com.novell.nidp.authentication.local.BasicClass

1.16.2 LDAP Unbind Request and Authentication Fails

When you submit a token after 15 seconds of the initial LDAP bind, the Identity server issues an LDAP unbind request and authentication fails. For more information, see TID 7012564. (Bug 794290)

1.16.3 RADIUS Authentication Checks LDAP Password Before Token Validation

When you enable the RADIUS token-based authentication on the Identity Server, it verifies the LDAP password before verifying the token. (Bug 794495)

1.16.4 PasswordFetchClass User Lookup Fails

Issue: PasswordFetchClass user lookup into iplanet Directory fails. (Bug 799701)

Fix: Password fetch will work if DN uses UID instead of CN for user look up in the LDAP directory.

1.16.5 SAML ECP Profile is not Working for Office365

Issue: The Identity Server is not setting the IDPEmail attribute, which is configured as an attribute to send, in the SAML 2.0 token. (Bug 807382)

Fix: The ECP URL for Office365 is https://IDP/nidp/saml2/soap.

1.16.6 The Identity Server Fails to Respond

There are issues authenticating to the Identity Server accessing Liberty or SAML metadata. The Identity Server fails to report to the Administration Console as the SSL connection fails to timeout. For more information, see TID 7012562. (Bug 792738)

1.16.7 Vulnerability Issue for Cross-Site Scripting in the Identity Server

Issue: Access Manager does not validate a JSP file if you have customized the file, such as customizing the login, logout, or error pages. If you modify JSP files you must sanitize the JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks and TID 7012486. (Bug 817557)

Fix: Sanitized the JSP file to prevent cross-site scripting attacks.

1.16.8 The Identity Server Inserts Only One Value in SAML 2.0 Assertion

Issue: The Identity Server inserts only one value in a SAML 2.0 assertion, when there are multiple attributes with the same name. (Bug 800580)

Fix: The Identity Server now includes a remote attribute in the string to be encoded so that you get a unique encoded value for each constant value that you add.

1.17 Software Fixes for the Access Gateway Service

Access Manager 3.2 Service Pack 2 includes software fixes that resolve several previous issues in the Access Gateway Service.

1.17.1 Increased Flexibility of Configuring Protected Resources Using Wild Characters

Issue: 403 error occurs while accessing protected resources after upgrading to version 3.2 for the URL paths configured as `/path/path_*`. (Bug 774381)

Fix: Implemented regular expressions in URL path matching for protected resources which allows flexibility in configuring the protected resources using wild characters.

1.17.2 TCP Tunnel Connections are Active Even After Idle Timeout

Issue: The TCP tunnel connections remain active even after the idle timeout for the proxy is reached. (Bug 810717)

Fix: The TCP connections are getting closed based on the timeout values set.

1.17.3 Logout Page Does Not Execute With the Customizations You Made

Issue: When you have both Liberty and SAML 2.0 sessions running on the Identity Server and you log out of the Access Gateway, the `logoutsuccess.jsp` page does not execute with the customizations you have made to the logout page. You will be able to log out of the Access Gateway but the customizations you made are lost.

If the `logutSuccess.jsp` file is not loaded in a frame, the banner will not be displayed, and the Access Gateway will comment out the content in the logoutSuccess.jsp file. For more information on customizing the Access Gateway logout page, see "Customizing the Access Gateway Logout Page" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide* (Bug 792560)

Fix: Add the following line after the <body> tag in the logoutSuccess.jsp file:

```
<!-- BANNER LOADS IF THIS PAGE IS NOT LOADED IN REGULAR FRAME -->

<%@include file="logoutHeader.jsp"%>
```

1.17.4 Form Fill Posts the Page When None of the Input Fields Match

Issue: The Form Fill Policy posts the page even if none of the input fields match. (Bug 804229)

Fix: The form is not automatically submitted and will be available for you in interactive mode.

1.17.5 Web Server Health Check Fails to Check Status

The Web server health check fails to check the status of the back end Web servers with a message `Worker connectivity not checked`. For more information, see TID 7012561. (Bug 794482)

1.17.6 Proxy Configuration Updates Are Not Occurring Until You Restart Apache

Issue: Changes you make to an existing policy are not reflected unless you restart Apache manually. For more information, refer to TID 7012560. (Bug 803525)

Fix: Proxy Configuration Updates are reflected without restarting Apache manually.

1.17.7 Changes in the Access Gateway Configuration Cause Service Interruption

Issue: When updates are applied to the proxy servers, the Apache service on that device is restarted. This stops the existing httpd processes on the Access Gateway and causes Service Interruption. For more information, see TID 7012560. (Bug 778475)

Fix: Service is not interrupted as graceful restart is now supported in the Access Gateway.

1.17.8 The Access Gateway Fails Abruptly While Processing 302 Redirect Responses

Issue: Access Gateway fails abruptly while processing 302 redirect responses from Web server without a trailing / after hostname. For more information, see TID 7012558. (Bug 806978)

Fix: This release changes the Web server redirects to include the trailing / character sent with the 302 redirect.

1.17.9 Cannot Inject a Photo into HTTP Headers

Issue: You can use the jpegPhoto LDAP attribute to store your photo in JPEG format. This LDAP attribute does not inject the image into a custom HTTP header and returns a 400 Bad Request error. (Bug 780739)

Fix: Edit the `index.php` file and add the following line:

```
<img src="....Base64 value got from custom
header......."/>
```

1.17.10 Issue with Importing or Renewing Certificates

Issue: Access Manager is unable to import certificates with different certificate file formats. (Bug 815696)

Fix: Access Manager is now able to import certificates in DER, PEM and PKCS7 format along with different format certificates together.

1.17.11 Issues With nproduct.log File Growing and Audit Events Are Not Sent to NSure Audit Server

Issue: The `nproduct.log` file keeps growing even though audit is not enabled. Another issue is that no audit events are sent to the NSure Audit server running on the Administration Console. (Bug 796294)

Fix: The issue with the log file has been resolved.

1.18 Software Fixes for the SSL VPN

1.18.1 Expired SSL VPN Signing Certificate

Issue: SSL VPN signing certificate has expired and the `nidp.jar` file contains an expired certificate. (Bug 816698)

Fix: No expired certificate related messages are now observed in the jar file.

2 Installing or Upgrading

After you purchased Access Manager 3.2 Service Pack 2, log in to the Novell Downloads page and follow the link that allows you to download the software. The following files are available:

Table 1 *Files Available for Access Manager Service Pack 2.*

Filename	Description
`AM_32_SP2_AccessManagerService_Linux64.tar.gz`	Contains the Access Manager Service for Linux.
`AM_32_SP2_AccessManagerService_Win64.exe`	Contains the Access Manager Service for Windows Server 2008.
`AM_32_SP2_AccessGatewayAppliance_Linux_SLES11_64.iso`	Contains the Access Gateway Appliance.
`AM_32_SP2_AccessGatewayAppliance_Linux_SLES11_64.tar.gz`	Contains all patches from 3.2 to 3.2 SP2 for the Access Gateway Appliance.
`AM_32_SP2_AccessGatewayService_Win64.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008.
`AM_32_SP2_AccessGatewayService_Linux_64.tar.gz`	Contains the Access Gateway Service for SLES 11 and RHEL 6.2 or 6.3.
`AM_32_SP2_ApplicationServerAgents_AIX.bin`	Contains the Agents service for AIX platform.
`AM_32_SP2_ApplicationServerAgents_Linux.bin`	Contains the Agents service for Linux platform.

Filename	Description
AM_32_SP2_ApplicationServerAgents_Solaris.bin	Contains the Agents service for Solaris platform.
AM_32_SP2_ApplicationServerAgents_Windows.exe	Contains the Agents service for Windows platform.

If you have purchased a previous release of Access Manager (3.2 IR1, 3.2 SP1, 3.2 SP1 IR1a,) and need to move to 3.2 Service Pack 2, download the patch files from Novell Downloads page.

To install or upgrade Access Manager 3.2 Service Pack 2, see the Access Manager 3.2 SP2 Installation GuideAccess Manager Appliance 3.2 SP2 Installation Guide.

For the supported upgrade/migration paths for 3.2 SP2 see the following table. For more information on upgrading/migrating Access Manager 3.2 SP2, see *NetIQ Access Manager 3.2 SP2 Migration and Upgrade Guide*.

Table 2 *Supported Upgrade Paths for 3.2 SP2*

Source	Destination
3.2 IR1	3.2 SP2
3.2 SP1	3.2 SP2
3.2 SP1 IR1a	3.2 SP2

Table 3 *Supported Migrate Paths for 3.2 SP2*

Source	Destination
3.1 SP4	3.2 SP2
3.1.5	3.2 SP2

2.1 Verifying Version Numbers

It is important to verify the version number of existing Access Manager components before you upgrade or migrate to 3.2 SP2. This ensures that you have the correct version of files on your system.

2.1.1 Verifying Version Number Before Upgrading to 3.2 SP2

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Examine the value of the Version field to see if it displays a version that is eligible for upgrading to 3.2 SP2.

Components	3.2 IR1	3.2 SP1	3.2 SP1 IR1a
All Access Manager Components	3.2.0.370	3.2.1.57	3.2.1-57 + IR1-201

2.1.2 Verifying Version Number After Upgrading to 3.2 SP2

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Verify that the Version field lists 3.2.2.77.

3 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

3.1 Issue with Attribute Mapping

Issue: You cannot edit or view an existing Attribute Mapping from the Administration Console. (Bug 789663)

Workaround: None.

3.2 Issue with Load Balancer

Issue: The load balancer continues to send browser requests even though the Identity Server is in a non-responsive state. (Bug 797770)

Workaround: None.

3.3 Issue with TCP Connect Options

Issue: When you set the value of TCP Connect Options to more than 1440 seconds, the configuration update for Access Gateway fails. (Bug 796078)

Workaround: None.

3.4 Issue with Extended Logging

Issue: In Microsoft Windows, the Access Gateway does not create extended logs for reverse proxy requests configured for extended logging. (Bug 797559)

Workaround: None.

3.5 Issue with the SSL VPN Client Installation

Issue: If the Java JRE 1.7.0_21 plugin is enabled in the browser, the SSL VPN client installation (both traditional and ESP enabled) fails. (Bug 822759)

Workaround: Install the SSL VPN client by using a browser with JRE plugin older than version 1.7.0_21.

3.6 Kerberos Constrained Delegation Fails

Issue: Kerberos Constrained Delegation fails single sign-on authentication to the ADFS server. (Bug 819139)

Workaround: None

3.7 Users Cannot Get Redirected to the Password Management Servlet after applying Access Manager 3.1 SP4 IR1

Issue: When users authenticate to the Identity Server and get the password expired message, they are not redirected to the Password Management Servlet defined for that contract. (Bug 814057)

Workaround: None.

3.8 You are not Prompted to Re-authenticate even if forceAuth is Enabled

Issue: The Name Password Form contract does not prompt users to be re-authenticated when forceAuth is enabled. (Bug 814785)

Workaround: None.

3.9 Configuring an Additional Replica Does Not Work When Secret Store is Enabled

Issue: When you enable the eDirectory user store to use secret store, the port listed is 389 and you cannot click *Use secure LDAP connections* and the communication with the newly added replica fails. (Bug 811887)

Workaround: Remove the SecretStore entry, add the replicas with secure LDAP and add the SecretStore entry again.

3.10 Issue with the Identity Injection Policy

Issue: The Identity Injection policy configured to inject the query string parameter causes looping if a query string parameter already exists in the URL. (Bug 813132)

Workaround: None.

3.11 Access Gateway Does Not Accept New Client Connections

Issue: The Access Gateway stops accepting new client connections. (Bug 813132)

Workaround: To fix this issue, see TID 7010977.

3.12 Authentication Occurs for Revoked Certificates

Issue: When you select the revoked certificate and continue with the authentication process, the browser should display an error message that the certificate has been revoked. (Bug 805216)

Workaround: After revoking the certificate, restart the Identity Server.

3.13 Webtrends Does Not Read Log Files with Extended Logging

Issue: Webtrends perform data analysis based on the Access Gateway HTTP logs. When you upgrade to 3.2.1 IR1a, webtrends cannot read log files with extended logging enabled. (Bug 822598)

Workaround: None.

3.14 Removing eDirectory Replica from 3.1 SP4 Secondary Administration Console Fails While Migrating to 3.2

Issue: After migrating to the primary Administration Console, removal of the eDirectory replica from 3.1 SP4 secondary Administration Console fails. (Bug 822206)

Workaround: Wait for 20 to 30 minutes until eDirectory replica status changes to `Up` (`ndsstat -s` command). Once status is up, the eDirectory replica can be removed.

4 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate Web site (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of Qmunity (http://community.netiq.com/), our community Web site that offers product forums, product notifications, blogs, and product user groups.

5 Legal Notice

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.

If this product claims FIPS compliance, it is compliant by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

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