NetIQ Access Manager Appliance 3.2 Service Pack 2 IR2

January, 2014

NetIQ Access Manager Appliance 3.2 Service Pack 2 IR2 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 that our products meet all your needs. You can post feedback in the Access Manager forum on Qmunity, our online community that also includes product information, blogs, and links to helpful resources.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 3.2 SP2 Readme and Access Manager Appliance 3.2 Service Pack 2 IR1 Readme.

The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at the Access Manager NetIQ Documentation page. To download this product, see the NetIQ Access Manager 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 Software Fixes for the Identity Server

NetIQ Access Manager Appliance 3.2 Service Pack 2 IR2 includes software fixes that resolve several previous issues.

1.1.1 Cannot Create Additional Replicas if Secret Store is Enabled

Issue: You cannot check the "Use Secure LDAP" box while creating a replica in eDirectory to store secrets and the port communication with the newly added replica fails. (Bug 811887)

Fix: Configuring an eDirectory user store to use secretstore is now possible as the **Use secure LDAP connections** option will be selected and the default port is set to 636 on the new server replica userstore screen.

1.1.2 Single Sign-on Does Not Work With Different Contracts on SAML Requests

Issue: The Identity Server prompts you to re-authenticate on SAML requests even though the Identity Server has already authenticated at a higher level contract. (Bug 832443)

Fix: If authentication request has any context comparison parameter, check is performed on contract levels with already authenticated contracts at the Identity Server. If request is to check exact level or context comparison is not set, already authenticated contract level check will not be performed.

1.1.3 NetIdentity Users are Prompted Twice for Credentials

Issue: When NetIdentity client is enabled and Kerbeos authentication is configured, users were prompted for credentials twice even though correct credentials were used the first time. (Bug 833978)

Fix: If Netidentity flag is enabled and the Netidentity header exists with the request, Kerberos will not be executed. Hence, you will not be asked for credentials the second time.

1.1.4 Unable to Modify Customization Profile After Authenticating to Remote Identity Server

Issue: You can modify an LDAP attribute defined under the customisation profile when you have authenticated to the Identity Server locally, but you will get an error message that you cannot modify when you are logged in from a remote Identity Server. (Bug 836097)

Fix: `nidp.jar` file has been updated and you can view and modify the customization profile.

1.1.5 Identity Server Session Failover Does Not Work With External Authentications

Issue: Identity Server failover does not work as the Identity Server does not send the temporary user information to the failover server to recreate the session. (Bug 838608)

Fix: Identity server session failover works now, when other servers in the cluster are not working.

1.1.6 Radius Authentication With Token Fails

Issue: On a Radius server authentication fails when the login page is displayed the second time. (Bug 838625)

Fix: JSP changes have been made where the submitted parameter value now accepts the user entered value.

1.1.7 X.509 Authentication Lists the Entire List of Certificates

Issue: X.509 authentication lists the entire list of certificates imported to the browser. (Bug 841757)

Fix: In the `/nidp vhosts` apache configuration file (`/etc/opt/novell/apache2/conf/vhosts.d/NAM-Service.conf`), the SSLCACertificateFile has been removed and SSLCACertificatePath `/opt/novell/apache2/cacerts/`custom line has been added. To restrict the list to only certain certificates, see Troubleshooting Identity Server and Authentication. By default `Location/nidp/nidpsecure` tag in the below file `/etc/opt/novell/apache2/conf/vhosts.d/NAM-Service.conf` is updated as

```
<Location /nidp/nidpsecure>
    SSLOptions +ExportCertData
    SSLVerifyClient optional_no_ca
    SSLCACertificatePath /opt/novell/apache2/cacerts/custom
  </Location>
```

1.1.8 Federation Fails if SAML 2.0 Post Response Is Signed

Issue: Federation fails if the SAML 2.0 post response contains signature and assertion does not. (Bug 842788)

Fix: Added nidp config property SAML2_AVOID_SIGN_AND_VALIDATE_ASSERTION_TRUSTEDPROVIDERS in the service provider. If response is signed and assertion is not, federation is successful. For more information, see Configuring SAML 2.0 to Sign Messages.

1.2 Software Fixes for the Access Gateway

NetIQ access manager appliance 3.2 Service Pack 2 IR2 includes software fixes that resolve several previous issues.

1.2.1 GZip Compression Issues with Small Payloads Accelerating Sentinel or Liferay

Issue: When GZip is enabled and you access Sentinel/Liferay portal through Access Manager, a blank page is displayed. (Bug 772808)

Fix: The Access Gateway will decompress the GZip data even if data is less than 10 bytes.

1.2.2 Access Gateway Does Not Work When the <form> Tag Includes an Empty Method Element

Issue: Access Gateway does not work when the `<form>` tag includes an empty method element while processing a Form Fill policy. (Bug 823555)

Fix: Null check has been introduced and the Access Gateway works without any issue.

1.2.3 Cannot Log Cache Status Extended Log Field

Issue: The cache status field is not logged though you have enabled the extended HTTP logging for a proxy service. (Bug 829714)

Fix: Added *CACHE_STATUS* field in the logging configuration.

1.2.4 Username Is Logged as a Public in Common/Extended Logging When Accessing Protected Resource with Non-Redirected Login

Issue: When you access a protected resource with a valid basic authentication header (which will not redirect them for login to the NIDP server) will get access as expected but the common / extended logging entry stores them as "public" user. (Bug 836066)

Fix: A valid user name will be logged instead of storing the user name as "public".

1.2.5 IP Mismatch Errors Display "Access forbidden" or "NULL"

Issue: When you access a protected resource from the Access Gateway and change the IP address of the client, Access Forbidden or NULL message is displayed. (Bug 838228)

Fix: A valid error message is now displayed.

1.2.6 Error While Uploading a File Which Contains NULL Bytes

Issue: When you upload an attachment that contains NULL bytes, the upload is truncated. The Web server displays an error as the end of the HTTP transaction is missing. (Bug 838690)

Fix: You can now attach a file which contains NULL bytes.

1.2.7 Multiple Authentication Requests While Opening Microsoft Excel Files

Issue: You are requested for multiple authentications when you open Microsoft Excel files through the Access Gateway. (Bug 839878)

Fix: Changes have been made for handling the WebDAV options request, and you can now open the Microsoft Excel files without entering the credentials multiple times.

1.2.8 Identity Injection Fails to Inject Basic Authentication Information

Issue: After accessing a protected resource, if you access a public resource of an Access Gateway with identity injection policy enabled, the credentials with which you logged in the first time is not injected into the header. (Bug 841228)

Fix: The parameters configured in the Identity Injection policy are now injected while accessing a public resource.

1.2.9 Rewriter Issue with /nesp/app/plogout URLs

Issue: An incorrect DNS name is rewritten in the Location header. (Bug 841237)

Fix: The rewriter will not rewrite now if the back end URL contains the published name and the URL is `/nesp/app/plogout`.

1.2.10 Rewriter Fails to Rewrite Meta HTML Headers

Issue: The Access Gateway does not rewrite the name from the back end server to a published name if you configure the Web server IP address as DNS name instead of the IP address. (Bug 848877)

Fix: If the Web server host name is configured as dns name then the Access Gateway rewrites the URL if the back end DNS name exists as part of the URL.

1.2.11 Proxy Service Requests Go to the Same Web Server Though Round Robin is Configured

Issue: Proxy service requests go to the same Web server, though the Session Stickiness and Persistence Connection have been disabled and round robin is enabled. (Bug 851138)

Fix: If Persistence Connection to Web server is disabled and Session Stickiness is enabled, the ZNPCQ003 cookie setting is not removed now.

2 Installing or Upgrading Access Manager

To upgrade access manager appliance 3.2 Service Pack 2 IR2, download the AM_32_SP2_IR2.zip, which contains the access manager appliance Patch Tool and the patch file from Novell Downloads. To upgrade to this version, you must be using 3.2 Service Pack 2 or 3.2 Service Pack 2 IR1.

To install access manager appliance 3.2 Service Pack 2, see the NetIQ Access Manager Appliance 3.2 SP2 IR1 Installation Guide.

You can upgrade from 3.2 Service Pack 2 or 3.2 Service Pack 2 IR1 to 3.2 Service Pack 2 IR2. for more information on upgrading to Access Manager Appliance 3.2 Service Pack 2 IR2, see Upgrading Access Manager Appliance 3.2 SP2 Using the Patch Process (https://www.netiq.com/documentation/netiqaccessmanager32/installation/data/bzevr1p.html#b13pyszn).

2.1 Verifying Version Numbers

It is important to verify the version number of existing Access Manager components before you upgrade to 3.2 Service Pack 2 IR2. This ensures that you have the correct version of files on your system.

2.1.1 Verifying Version Numbers Before Upgrading to 3.2 SP2 IR2

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 Service Pack 2 IR2. The version field should list 3.2.2-77 for 3.2 SP2 or 3.2.2-77 + IR1-107 for 3.2 Service Pack 2 IR1.

2.1.2 Verifying Version Numbers After Upgrading to 3.2 SP2 IR2

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field lists 3.2.2-77 + IR2-117 when you upgrade from 3.2 SP2 and 3.2.2-77 + IR1-107, IR2-117 when you upgrade from 3.2 SP2 IR1.

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 During SSL Renegotiation When X.509 Authentication is Configured

Issue: An error occurs during SSL renegotiation after you select a client certificate while accessing a resource. (Bug 842019)

Workaround: Copy the CA certificates manually to `/etc/opt/novell/apache2/conf/cacerts/custom` folder and restart apache.

3.2 Web Server Load Balancing Does Not Work

Issue: Load balancing does not occur equally among the web servers in a proxy service setup. (Bug 842496)

Workaround: Forcefully restart the Access Gateway when you update the server instead of a graceful restart. Edit the `agm.properties` file, search for `linux.apache.command.gracefulrestart` and replace it with `linux.apache.command.restart`. Restart the Access Gateway using the `/etc/init.d/novell-mag restart` command. For more information and to fix this issue, see TID 7014203.

3.3 The Access Gateway Sometimes Does Not Work When Syslog Level Logging to error_log Is Not Enabled

Issue: The Access Gateway has performance and stability issues when the proxy is enabled in verbose mode and errors are reported regularly in the error_log file. (Bug 842805)

Workaround: Enable syslog level logging on the Access Gateway Proxy server if the Access Gateway service is running on SLES or RedHat. For more information, see TID 7011611.

3.4 Authentication Assertion Fails When Encrypt Assertions is Selected

Issue: If you have imported metadata initially using URL or text and edited manually, then no authentication assertions are returned in response when **Encrypt assertions** and **Want assertion to be signed** options are selected. (Bug 846558)

Workaround: Reimport the metadata through URL or text and follow the documentation steps available at (https://www.netiq.com/documentation/netiqaccessmanager32/identityserverhelp/data/bjk7fd1.html#bpzkjib) to enable message signing and use `nidpconfig.properties` for configuring it.

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 our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

[Return to Top]

5 Legal Notice

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.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/ (http://www.netiq.com/company/legal/).

[Return to Top]