Access Manager Appliance 3.2 Service Pack 2 IR1 Readme

September 2013

Access Manager Appliance 3.2 Service Pack 2 IR1 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 the previous release, see Access Manager Appliance 3.2 SP2 Readme.

For more information about this release and for the latest release notes, see the Access Manager Documentation (http://www.netiq.com/documentation) 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 Configuration Options in SAML 2.0 Identity and Service Provider

Access Manager Appliance acting as SAML 2.0 service provider, will now make a onbehalfof authentication request using SAML extensions. For more information, see Enabling or Disabling SAML Tags.

1.2 SAML2_SEND_ACS_INDEX Property

The AssertionConsumerServiceIndex value is now available to generate an AuthnRequest to the remote Identity server. For more information, see Enabling or Disabling SAML Tags.

1.3 Software Fixes for the Administration Console

Access Manager Appliance 3.2 SP2 IR1 includes software fixes that resolve several previous issues.

1.3.1 Administration Console Does Not Allow You to Disable HTTP Redirect for Single Logout

Issue: You cannot disable HTTP Redirect for single logout when you go to **SAML 2.0** > **Profiles** from the Administration Console. (Bug 828579)

Fix: The **Enable** or **Disable** options in the Administration Console for SAML 2.0 profiles work now.

1.4 Software Fixes for the Identity Server

Access Manager Appliance 3.2 SP2 IR1 includes software fixes that resolve several previous issues.

1.4.1 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)

Fix: Requests with similar headers as in the Identity Injection headers do not inject duplicate headers.

1.4.2 The Identity Server Does Not Prompt You to Re-authenticate when forceAuth is Enabled

Issue: The Name/Password form contract does not prompt you to re-authenticate when forceAuth is enabled. (Bug 814785)

Fix: A condition is now added to a java file and the Name/Password form contract will prompt you to authenticate.

1.4.3 Option to Specify File Location or Path for Custom or Extended Logging is not Available

Issue: You cannot set a file location or path for either custom or extended logging for proxy services. (Bug 818257)

Fix: You can now add custom log file location.

1.4.4 Cannot Generate an AuthnRequest to Remote Identity Server

Issue: You cannot generate an AuthnRequest to the remote Identity server without including the AssertionConsumerServiceIndex value. For more information, see Enabling or Disabling SAML Tags and TID 7012438 (http://www.novell.com/support/kb/doc.php?id=7012438). (Bug 819996)

Fix: Set the SAML2_SEND_ACS_INDEX property in the `nidpconfig.properties` file.

1.4.5 The Identity Server Policy Evaluation Fails

Issue: If the data entry value of an LDAP attribute in a Role based policy includes an & or any special characters in the field, the condition fails. (Bug 824629)

Fix: The policy evaluation, now uses the correct value with special characters and encoding and decoding of values is now correctly handled.

1.4.6 Issue Connecting to a Service Provider

Issue: An error occurred while connecting to a Service provider with the Identity server through SAML 2.0. Access Manager is not supporting the used name identifier format. (Bug 830082)

Fix: The used name identifier format is now supported.

1.4.7 Redirection to Password Management Servlet Fails

Issue: When you authenticate to the Identity server, you will not be redirected to the password management servlet when the user password has expired. (Bug 820652)

Fix: You will now be redirected to the password management servlet.

1.5 Software Fixes for the Access Gateway

Access Manager Appliance 3.2 SP2 IR1 includes software fixes that resolve several previous issues.

1.5.1 400 Error Occurs when a Protected Resource is Redirected to an ESP when SSL Terminator Flags are Enabled

Issue: Accessing a protected resource which redirects to an ESP for authentication, uses HTTPs and default port number 80 when the SSL terminator is on. (Bug 802210)

Fix: The standard HTTP port number 80 is removed and HTTP is replaced with HTTPs.

1.5.2 AGLogout Does Not Work on pbmh Service

Issue: When you access a html page through a pbmh service, an error occurs on logging out of the session through the AGLogout URL. (Bug 818139)

Fix: The Rewriter of Location header and page content URLs are now corrected and AGLogout on pbmh service occurs.

1.5.3 The Access Gateway Appliance Stops

Issue: The Access Gateway stops while trying to Form Fill a page that includes a select statement without a name. (Bug 821549)

Fix: Null check is introduced for select tag which now stores elements other than name, for example, id.

1.5.4 Issue With Path Based Proxy

Issue: An advanced option is available to make the path-based multi-homing path URL case-insensitive. For more information, see TID 7013265 (http://www.novell.com/support/kb/doc.php?id=7013265). (Bug 814354)

Fix: An advanced option is available to make the path-based multi-homing path URL case-insensitive. For more information, see Configuring the Global Advanced Options (https://www.netiq.com/documentation/netiqaccessmanager32/accessgatewayhelp/data/agsglobaladv.html).

1.5.5 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)

Fix: The HTTP extended logging provided by Access Manager now works well when logs are provided to external log analyzer tool such as Webtrends. Headers in extended log file are now added based on logging configuration.

1.5.6 Form Fill Policy Does Not Work

Issue: The Form Fill policy fails to auto submit data when the login page is larger than 200 KB in size. (Bug 826406)

Fix: The HTML page size for the Access Gateway Service Form Fill is increased to 500 KB.

1.5.7 Referer Header is Rewritten When Rewrite Inbound Headers are Enabled

Issue: After upgrading from 3.2 SP1 IR1a to 3.2 SP2, inbound headers are rewritten even though the option is not enabled for the default rewriter profile. (Bug 829503)

Fix: An advanced option `NAGDisableHdrRewriteToWebServer on` will disable the rewriting the inbound headers. For more information, see Configuring the Global Advanced Options (https://www.netiq.com/documentation/netiqaccessmanager32/accessgatewayhelp/data/agsglobaladv.html).

1.5.8 An Error Occurs When the URL Path Contains % Encoding Character

Issue: An error occurs when a protected resource with an URL path containing % encoding character is assigned to a proxy service. (Bug 831132)

Fix: The Access Gateway serves the request and accepts the encoded characters in the URL.

1.5.9 SSO Fails Due to Change in Behavior of Protected Resource Path Matching

Issue: If you configure a protected resource with `/path/portal/*` it will not match requested URL with `/path/portal`. (Bug 833107)

Fix: The requested URL `/path/portal` now matches the protected resource URL `/path/portal/*`.

2 Installing or Upgrading Access Manager

To upgrade Access Manager Appliance 3.2 Service Pack 2 IR1, download the AM_32_SP2_IR1.zip, which contains the Access Manager Appliance Patch Tool and the patch file from Novell Downloads (http://download.novell.com/index.jsp). To upgrade to this version, you must be using 3.2 Service Pack 2.

To install Access Manager Appliance 3.2 Service Pack 2, see the NetIQ Access Manager Appliance 3.2 SP2 IR1 Installation Guide (https://www.netiq.com/documentation/netiqaccessmanager32_appliance/sb_installation/data/bookinfo.html).

You can upgrade from 3.2 Service Pack 2 to 3.2 Service Pack 2 IR1. For more information on upgrading to Access Manager Appliance 3.2 Service Pack 2 IR1, see "Upgrading Access Manager Appliance" in the *NetIQ Access Manager Appliance 3.2 SP2 IR1 Installation Guide.*

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 Service Pack 2 IR1. 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 IR1

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 IR1. The version field should list 3.2.2-77.

2.1.2 Verifying Version Number After Upgrading to 3.2 SP2 IR1

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

2 Verify that the **Version** field lists 3.2.2-77 + IR1-107.

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 Identity Injection Policy Continuously Appends the Injected Query Line

Issue: The Identity Injection policy enabled on a protected resource duplicates the credential information sent to the Web server. For more information, see TID 7013274 (http://www.novell.com/support/kb/doc.php?id=7013274). (Bug 835916)

Workaround: None.

3.2 Internet Explorer and Firefox Fail to Install the x-nmasweb Plugin

Issue: When the customer tries to access an application protected by the Access Gateway using smart card contract for smart card authentication, both Internet Explorer and Firefox fail to install the x-nmasweb plugin. (Bug 832436)

Workaround: None.

3.3 The Access Gateway Does Not Rewrite URLs

Issue: The Access Gateway does not rewrite URLs if an IP address is used for Web Server Host Name. (Bug 830743)

Workaround: Configure the DNS Name of the back end server in **Web Server Host Name** field.

3.4 Issue with Extended Logging

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

Workaround: None.

3.5 Form Fill Issues in the Access Gateway

Issue: When you give the value of form number as 0, the Access Gateway Form Fill policy does not support submitting all the forms on a HTML page. (Bug 828203)

Workaround: None.

3.6 Issue with SSO to Back End Application

Issue: The back end application does not accept NTLM protocol when you access it through the Access Gateway and you will not be able to view the HTML page unless you submit your credentials continuously. (Bug 827639)

Workaround: None.

3.7 Issue in Deleting URL Paths with Tilde Sign

Issue: You cannot delete an URL path below a protected resource with tilde sign after applying the changes. (Bug 822808)

Workaround: None.

3.8 Using Kerberos as the Identity Server Default Contact Fails to Render Complete Fallback Login Page

Issue: On fallback, only the content of the `login.jsp` file is rendered without the banner or footer. (Bug 820580)

Workaround: Follow the procedure below:

1. Create a copy of `login.jsp` and name it as `login1.jsp`.
2. Modify the `login1.jsp` and add the following script below the body tag.

```
<script>
        if(top.location.href == window.location.href)
        {
            window.location.href="/nidp/jsp/main.jsp";
        }
    </script>
```

3.9 Subject NameID Value Sent with Assertion Does Not Change Despite Change on Back End User Store

Issue: The changes made in the back end user store are not reflected when the subject name identifier value is sent with assertion. (Bug 820472)

Workaround: Stop the user sessions on the Identity Server, by using the `KillUserSession` utility. When you login again, the changes are reflected.

3.10　Installation Fails Due to Incorrect Disk Space Detection

Issue: The installation fails when the disk space partitioning below /opt is sufficient but /opt is not. (Bug 819810)

Workaround: None.

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

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.