Access Manager Appliance 4.1 Service Pack 2 Release Notes

February 2016

Access Manager Appliance 4.1 Service Pack 2 (4.1.2) supersedes Access Manager Appliance 4.1 Service Pack 1 Hotfix 1 (4.1.1 HF1).

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.1 SP1 HF1 Release Notes..

1 What’s New?

This release includes the following platform updates and fixed issues:

- Section 1.1, “Operating System Upgrade,” on page 1
- Section 1.2, “Updates for Dependent Components,” on page 1
- Section 1.3, “Fixed Issues,” on page 2

1.1 Operating System Upgrade

In this release, the embedded SLES 11 SP3 is upgraded to SLES 11 SP4.

1.2 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.6
- Java 1.8.0_66
- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, CVE-2013-5704,and CVE-2015-3183)
- OpenSSL 1.0.1p
- Tomcat 8.0.24
- iManager 2.7.7.5

NOTE: Access Manager 4.1.2 by default supports Tomcat 8.0.24 and OpenSSL 1.0.1p, but the Administration Console uses Tomcat version 7.0.56 due to dependency on iManager.

1.3 Fixed Issues

This release includes software fixes for the following components:

- Section 1.3.1, “Identity Server,” on page 2
- Section 1.3.2, “Access Gateway,” on page 3

1.3.1 Identity Server

The following issues are fixed in the Identity Server:

- Section 1.3.1.1, “Authorization Policy Fails after Upgrading from 4.0.1 to 4.1.x,” on page 2
- Section 1.3.1.2, “SAML Tokens Are Line Wrapped,” on page 2
- Section 1.3.1.3, “The Post Authentication Method Configured for a SAML Identity Provider Does Not Work,” on page 2
- Section 1.3.1.4, “Re-authentication Is Required During a spsend Request When a Contract Contains the Equal or higher level Flag,” on page 2
- Section 1.3.1.5, “Issue in Message Digest Generation of Metadata,” on page 3
- Section 1.3.1.6, “The External Attribute Policy Does Not Return Multi-Valued Responses,” on page 3
- Section 1.3.1.7, “Authentication Fails When Multiple Methods Defined in a Contract and x509 Is First Contract,” on page 3

1.3.1.1 Authorization Policy Fails after Upgrading from 4.0.1 to 4.1.x

Issue: When acting as a service provider, Access Manager does not pass the role information received in the assertion from the external identity provider to the policy. The configured authorization policy searches for a specific attribute or value pair. If the value is unavailable, the policy fails. [`Bug 952298`]

1.3.1.2 SAML Tokens Are Line Wrapped

Issue: The SAML tokens that contain a signature and certificates are line wrapped. This issue happens due to old XML signature library.[`Bug 918552`]

Fix: The XML signature library has been upgraded. But, by default the SAML tokens are line wrapped. To disable line wrapping, set the following option in the `/opt/novell/nam/idp/conf/tomcat7.conf` file:

```
JAVA_OPTS="${JAVA_OPTS} -Dorg.apache.xml.security.ignoreLineBreaks= true
```

1.3.1.3 The Post Authentication Method Configured for a SAML Identity Provider Does Not Work

Issue: If a user is not federated and logs first time in to an external identity provider, the post authentication method is not executed. However, on subsequent attempts, the post authentication executes successfully. [`Bug 938287`]

1.3.1.4 Re-authentication Is Required During a spsend Request When a Contract Contains the Equal or higher level Flag

Issue: When a user is authenticated with same level contract and the **Equal or higher level** option is enabled in the spsend step up contract, the Identity Server prompts for re-authentication. [`Bug 937642`]

1.3.1.5 Issue in Message Digest Generation of Metadata

Issue: The message digest generation of metadata fails when `AuthnRequestsSigned` is set to true. This causes a signature validation failure and hence fails to import the provider. [`Bug 922019`]

1.3.1.6 The External Attribute Policy Does Not Return Multi-Valued Responses

Issue: The external attribute policy does not return multi-valued responses. [`Bug 924013`]

1.3.1.7 Authentication Fails When Multiple Methods Defined in a Contract and x509 Is First Contract

Issue: Authentication fails when multiple methods are defined in a contract with x509 being the first method. [`Bug 908949`]

1.3.2 Access Gateway

The following issues are fixed in the Access Gateway:

- Section 1.3.2.1, "Rewriter Automatically Rewrites the URL in the Location Header for the Query," on page 3
- Section 1.3.2.2, "CORS Enabled Web Servers Wrongly Recognizes the Request," on page 3
- Section 1.3.2.3, "Access Gateway Sets Wrong Values for the X-Forwarded-Host Header," on page 3
- Section 1.3.2.4, "Host HTTP Header Attack," on page 3
- Section 1.3.2.5, "No Option to Disable the X-Forwarded-Host Header," on page 3
- Section 1.3.2.6, "Issue in Rewriting Location Header," on page 4
- Section 1.3.2.7, "The Access Gateway Runs Out of Memory When the Extended Logging Is Enabled," on page 4

1.3.2.1 Rewriter Automatically Rewrites the URL in the Location Header for the Query

Issue: The Rewriter rewrites the location header with the URL in the query string automatically. There is no option to enable or disable rewriting the location header. [`Bug 945684`]

Fix: This issue is now resolved and the Rewriter rewrites the location header with the URL in the query string only when you enable the `RWOutboundHeaderQueryString` advance option. For more information about this option, see Advanced Access Gateway Options in the NetIQ Access Manager Appliance 4.1 Administration Guide.

1.3.2.2 CORS Enabled Web Servers Wrongly Recognizes the Request

Issue: The CORS enabled web servers wrongly recognizes the request as cross-origin request. This is due to the Access Gateway failing to rewrite the origin header. [`Bug 941674`]

1.3.2.3 Access Gateway Sets Wrong Values for the X-Forwarded-Host Header

Issue: The Access Gateway sets wrong values for the X-Forwarded-Host header when sending the request to a web server. [`Bug 945683`]

1.3.2.4 Host HTTP Header Attack

Issue: A Host HTTP Header attack exists in the Access Gateway. An additional HTTP header is added with the original header. This header redirects you to a malicious URL. [`Bug 926063`]

1.3.2.5 No Option to Disable the X-Forwarded-Host Header

Issue: The Access Gateway does not support disabling the X-Forwarded-Host header. [`Bug 949368`]

Fix: This issue is fixed now. An advanced option `NAGAddProxyHeader` is introduced to disable the X-Forwarded-Host header. For more information about this option, see Advanced Access Gateway Options in the NetIQ Access Manager Appliance 4.1 Administration Guide.

1.3.2.6 Issue in Rewriting Location Header

Issue: When multiple path-based proxy services are configured and the **Remove Path on Fill** option is enabled, the Rewriter either does not rewrite or rewrites to a wrong path-based proxy service when setting 302 Location Header for a path-based proxy service. [`Bug 931748`]

1.3.2.7 The Access Gateway Runs Out of Memory When the Extended Logging Is Enabled

Issue: This happens because of a memory leak in the `/opt/novell/apache2/sbin/rotatelogs` process. [`Bug 941796`]

2 Supported Upgrade Paths

To upgrade to Access Manager 4.1.2, you must be on any one of the following Access Manager versions:

- 4.0 Service Pack 2
- 4.0 Service Pack 2 HF1
- 4.1
- 4.1 Service Pack 1
- 4.1 Service Pack 1 HF1

3 Installing or Upgrading Access Manager

After purchasing Access Manager Appliance 4.1.2, 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 Access Manager Appliance 4.1.2*

Filename	Description
`AM_41_SP2_AccessManagerAppliance.iso`	Contains the Access Manager Appliance iso.
`AM_41_SP2_AccessManagerAppliance.tar.gz`	Contains the Access Manager Appliance tar file.

For information about supported upgrade paths, see Section 2, “Supported Upgrade Paths,” on page 4. For more information about installing and upgrading, see the NetIQ Access Manager Appliance 4.1 Installation and Upgrade Guide.

4 Verifying Version Numbers After Upgrading to 4.1.2

After upgrading to Access Manager 4.1.2, verify that the version number of the component is indicated as **4.1.2.0-23**. To verify the version number, perform the following steps:

1. In the Administration Console, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.1.2.0-23**.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issue is currently being researched. If you need further assistance with any issue, please contact Technical Support.

5.1 The Rewriter Does Not Exclude DNS Names Specified in the Exclude DNS Name List

Issue: The URL references containing excluded DNS names are rewritten even when the DNS names are specified in the **Exclude DNS Name List** option. [`Bug 927855`]

Workaround: Not available.

5.2 Upgrading Access Manager from 4.1.2 to 4.2 Terminates Abruptly

Issue: If you attempt to upgrade from 4.1.2 to 4.2, the upgrade process terminates abruptly. [`Bug 967757`]

Workaround: If you are planning an upgrade from 4.1.2 to 4.2, perform the following steps:

1. Extract the 4.1 installer files and locate `upgrade_utility_functions.sh` file.
2. Locate the section that includes the following line:
   ```
   supportedVersions="|3.2.3\|4.0.0\|4.0.2\|4.1.0.0\|4.1.1.0\|4.1.1.1\|4.2.0.0"
   ```
3. Modify the **supportedVersion** section by adding 4.1.2 as the supported upgrade platform in the following manner:
   ```
   supportedVersions="|3.2.3\|4.0.0\|4.0.2\|4.1.0.0\|4.1.1.0\|4.1.1.1\|4.2.0.0\|4.1.2.0"
   ```
4. Upgrade the components using the information in Upgrading Access Manager Appliance.

5.3 The Facebook Social Auth Class Displays an Error

Issue: When you setup a new app in Facebook on 2.5 API and configure the social auth class, the following error message is displayed: `Invalid Scopes: read_stream`.

Workaround: To workaround this issue, upgrade the social auth library to the latest version (4.10). For more information, see TID.

6 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 website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice

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/.