Access Manager Appliance 4.3 Service Pack 1 Release Notes

February 2017

Access Manager Appliance 4.3 Service Pack 1 (4.3.1) includes enhancements, improves usability, and resolves several previous issues.

Many of these improvements are 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 our community website that also includes product notifications, blogs, and product user groups.

For information about the previous release, see Access Manager Appliance 4.3 Release Notes.

For more information about this release and for the latest release notes, see the Documentation page. To download this product, see the Product Upgrade page.

The general support for Access Manager 4.3 ends on 31st May 2018. For more information, see the Product Support Lifecycle page.

- Section 1, “What’s New?,” on page 1
- Section 2, “Installing or Upgrading,” on page 5
- Section 3, “Supported Upgrade Paths,” on page 6
- Section 4, “Verifying Version Number After Upgrading to 4.3.1,” on page 6
- Section 5, “Known Issues,” on page 6
- Section 6, “Contact Information,” on page 7
- Section 7, “Legal Notice,” on page 8

1 What’s New?

Access Manager Appliance 4.3.1 provides the following enhancement and fixes in this release:

- Section 1.1, “Updates for Dependent Components,” on page 1
- Section 1.2, “Browser Support,” on page 2
- Section 1.3, “Enhanced Analytics Dashboard,” on page 2
- Section 1.4, “Fixed Issues,” on page 2

1.1 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.9
- Java 1.8.0_121
- OpenSSL 1.0.2k
- Tomcat 8.0.39
- iManager 2.7.7.8

NOTE: Access Manager 4.3.1 by default supports Tomcat 8.0.39 and OpenSSL 1.0.2k. However, Administration Console uses Tomcat version 7.0.68 due to dependency on iManager.

1.2 Browser Support

For accessing Access Gateway and Identity Server: This release adds support for the latest versions of the following browsers:

- Internet Explorer
- Chrome
- Firefox
- Safari

For accessing user portal and Administration Console: This release adds support for the following versions of the browsers:

- Chrome 56.0.2924.87
- Firefox 51.0.1
- Internet Explorer 11.576.14393.0 Update Versions 11.0.38 (KB32033621)
- Edge 38.14393.0.0/ EdgeHTML 14.14393 (only for user portal)

1.3 Enhanced Analytics Dashboard

This release introduces the following graphs in addition to the existing graphs:

- Most Accessed Users
- Client IP Addresses
- Most Used Contracts
- Failed Authentications

For information about enabling the required audit events, see Enabling Events for Each Graph.

1.4 Fixed Issues

This release includes software fixes for the following components:

- Section 1.4.1, “Administration Console,” on page 2
- Section 1.4.2, “Identity Server,” on page 3
- Section 1.4.3, “Access Gateway,” on page 4

1.4.1 Administration Console

The following issue is fixed in Administration Console:

1.4.1.1 The Administration Console Configuration Is Not Restored When You Change the Hostname

Issue: While restoring the Administration Console configuration by using amrestore, the restore fails if youspecify a different hostname. This happens because the hostname in the Certificate Authority (CA) also gets changed and does not match with the one that was originally specified. Hence, amrestore fails and you cannot restore Administration Console. [`Bug 1009556`]

Fix: This issue is fixed. The hostname in CA remains unchanged even when you change the hostname.

1.4.2 Identity Server

The following issues are fixed in Identity Server:

- Section 1.4.2.1, “Issue with the Kerberos Fall Back Contract When Used with Name/ Password Authentication,” on page 3
- Section 1.4.2.2, “WS Federation Fails for .Net Applications,” on page 3
- Section 1.4.2.3, “The Mobile device registration contract Field Allows Only the Username and Password Contract,” on page 3
- Section 1.4.2.4, “The Kerberos Fall Back Login Page Does Not Display the New Portal with Customized Branding,” on page 3
- Section 1.4.2.5, “The AuthnContextCLassRef Statement Does Not Match with that of the Service Provider,” on page 4
- Section 1.4.2.6, “Risk-based Authentication Step Up Never Shows Executed Method within its Own Context,” on page 4

1.4.2.1 Issue with the Kerberos Fall Back Contract When Used with Name/ Password Authentication

Issue: When you configure the Kerberos fall back by using name and password authentication class, Access Manager allows authentication by using the default contract, but does not redirect the request to resource server.

Hence, users cannot access a resource server even when they are authenticated by using the default contract. [`Bug 899646`]

Fix: This issue is resolved. The users can access the resource server when Kerberos fall back contract is configured.

1.4.2.2 WS Federation Fails for .Net Applications

Issue: When a .NET WS-Federation service provider federates with an Access Manager STS/ WS-Federation identity provider, an error occurs and federation fails. This happens when you import the metadata to the .Net service provider. [`Bug 918163`]

Fix: This issue is resolved. The WS-Federation metadata can be obtained by using Samlv2Meta as described in the WS-Federation 1.1 and 1.2 specification. Also, to obtain the metadata, use the `<base-url>/nidp/wsfed/metadata?type=Samlv2Meta` URL format.

1.4.2.3 The Mobile device registration contract Field Allows Only the Username and Password Contract

Issue: In the **Mobile device registration contract** field, the only contract available is the username and password contract. [`Bug 998693`]

Fix: This issue is resolved. You can choose any required contract under Mobile device registration contract field.

1.4.2.4 The Kerberos Fall Back Login Page Does Not Display the New Portal with Customized Branding

Issue: When Kerberos fails, the fall back authentication login page does not show the custom branding.[`Bug 1003919`]

Fix: This issue is resolved. The fall back login page displays the custom branding.

1.4.2.5 The AuthnContextCLassRef Statement Does Not Match with that of the Service Provider

Issue: When Access Manager is a service provider, it cannot set custom authentication class references in AuthnRequest's **AuthnContextClassRef** element during spsend. This happens because the SAML 2.0 identity provider authentication card allows to configure only fixed set of authentication types when **Requested By** is set to **Use Types**. [`Bug 1001488`]

Fix: This issue is resolved with the introduction of the **SAML 2 CUSTOM AUTHNCONTEXT CLASS REF LIST** advance option. In Identity Server configuration, click **SAML 2.0 > *IDP name* > Configuration > options > New**, set **SAML2 CUSTOM AUTHNCONTEXT CLASS REF LIST** to specify one or more custom authentication class references. You can use the delimiter, **&**,to specify more than one references.

1.4.2.6 Risk-based Authentication Step Up Never Shows Executed Method within its Own Context

Issue: When you configure the step up authentication using the risk contract, the step up method is displayed inside the primary method's context. [`Bug 1005305`]

Fix: This issue is resolved. The step up method is shown in its own context, not inside the primary method's context.

1.4.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.4.3.1, "The Access Gateway Logout Page Does Not Display the Customized Branding," on page 4
- Section 1.4.3.2, "A Mangled Cookie Includes Multiple Values," on page 5
- Section 1.4.3.3, "Access to a Secure Web Server Fails with Unknown CA After Upgrading to Access Manager 4.3," on page 5
- Section 1.4.3.4, "Cannot Disable the HTTP Strict Transport Security Protocol on Access Gateway After Upgrading to Access Manager 4.3," on page 5
- Section 1.4.3.5, "Additional Characters Are Introduced When Adding the Post Data for Parking," on page 5
- Section 1.4.3.6, "Cannot Inject LDAPCredentials to Back-End Servers When the PreAuthRiskBasedAuthenticationClass Contract is Executed," on page 5

1.4.3.1 The Access Gateway Logout Page Does Not Display the Customized Branding

Issue: When the branding of the User Portal page is changed, the Access Gateway logout page does not display those changes. [`Bug 1019019`]

Fix: The `/AGLogout` and `/nesp/app/logout` pages now display the branding as it is configured on the User Portal. For this fix to work, ensure that you update the Access Gateway configuration after changing the branding.

To update Access Gateway configuration, you can perform any one of the following:

- Click **Troubleshooting > Current Access Gateway Configurations > Re-push Current Configuration**
- Make some negligible changes to Access Gateway cluster to activate the update status, then click **Update**
- Restart Access Gateway

1.4.3.2 A Mangled Cookie Includes Multiple Values

Issue: When accessing protected resources in the same domain, multiple values get assigned to a mangled cookie. [Bug 1009962]

Fix: This issue is resolved. A mangled cookie includes only the latest cookie value.

1.4.3.3 Access to a Secure Web Server Fails with Unknown CA After Upgrading to Access Manager 4.3

Issue: When users access the secure web servers, the browser displays the 502 error instead of launching the application. This happens because there was an issue with calculating the certificate hash. [Bug 1010876]

Fix: This issue is resolved. After upgrading to Access manager 4.3.1, the certificate hash is calculated properly.

1.4.3.4 Cannot Disable the HTTP Strict Transport Security Protocol on Access Gateway After Upgrading to Access Manager 4.3

Issue: After upgrading Access Manager to 4.3, you cannot disable the HTTP Strict Transport Security (HSTS) on Access Gateway. [Bug 1011260]

Fix: The issue is resolved. A new global advanced option, **SetStrictTransportSecurity**, is introduced to disable and enable HSTS now as the Access Gateway injects the modified attributes.

1.4.3.5 Additional Characters Are Introduced When Adding the Post Data for Parking

Issue: Access Gateway adds extra bytes when parking the post data that results in invalid content-length to post the data. [Bug 1014817]

Fix: This issue is resolved. The extra bytes are not added when parking the post data and content-length is correct to post the data.

For more information about this issue and its resolution, see TID 7018493.

1.4.3.6 Cannot Inject LDAPCredentials to Back-End Servers When the PreAuthRiskBasedAuthenticationClass Contract is Executed

Issue: When a contract contains PreAuthRiskBasedAuthenticationClass, you cannot inject LDAPCredentials to the back-end web servers. [Bug 1022068]

Fix: The issue is resolved. LDAPCredentials are cached and can be injected into backend servers even for PreAuthRiskBasedAuthenticationClass contract.

2 Installing or Upgrading

After purchasing Access Manager Appliance 4.3.1, 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 4.3*

Filename	Description
AM_43_SP1_AccessManagerAppliance.iso	Contains Access Manager Appliance .iso file.
AM_43_SP1_AccessManagerAppliance.tar.gz	Contains Access Manager Appliance .tar file.

Filename	Description
`AM_43_SP1_AnalyticsServerAppliance.iso`	Contains Analytics Server Appliance .iso file.
`AM_43_SP1_AnalyticsServerAppliance.tar.gz`	Contains Analytics Server Appliance tar file.

For information about the upgrade paths, see Section 3, “Supported Upgrade Paths,” on page 6. For more information about installing and upgrading, see the *NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide*.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.3.1, you need to be on one of the following versions of Access Manager:

- 4.1.x
  - 4.1 Service Pack 2 Hotfix 1
- 4.2.x
  - 4.2 Service Pack 2
  - 4.2 Service Pack 3
- 4.3

For more information about upgrading Access Manager Appliance, see “Upgrading Access Manager Appliance” in the *NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide*.

4 Verifying Version Number After Upgrading to 4.3.1

After upgrading to Access Manager 4.3.1, verify that the version number of the component is indicated as **4.3.1.0-53**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.3.1.0-53**.

5 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.

- Section 5.1, “ESP Global Option Configuration Does Not Work at the First Attempt,” on page 7
- Section 5.2, “Invalid Value Error When Adding a New Rule for OAuth in an Identity Injection Policy,” on page 7
- Section 5.3, “The Modifications Done in the Legacy SAML2 Page Does Not Synchronize with the Value in the Applications Interface,” on page 7
- Section 5.4, “Identity Server Returns Insecure Additional HTTP Cookies,” on page 7

5.1 ESP Global Option Configuration Does Not Work at the First Attempt

Issue: When you configure an ESP global option, it does not get applied to all Access Gateway ESPs at the first attempt. This is an intermittent issue. Also, if you disable a specific option by adding pound symbol (#), it may get deleted from the list. `[Bug 1002542]`

Workaround: Re-configure the ESP global options. If you require to add a pound symbol to any option for later use, copy and save the option from the list to a file and use it when required.

5.2 Invalid Value Error When Adding a New Rule for OAuth in an Identity Injection Policy

Issue: When you add a new rule for OAuth in the identity injection policy, the older values display the `Invalid value` message. This is an intermittent issue. `[Bug 1003262]`

Workaround: Cancel the modification and reopen the policy for editing.

5.3 The Modifications Done in the Legacy SAML2 Page Does Not Synchronize with the Value in the Applications Interface

Issue: After a SAML 2.0 application is created by using **Applications** under **Administration Tasks**, the applications task may not reflect the values of settings that are modified by using the legacy page, which is, under the SAML 2.0 tab of the identity provider cluster. `[Bug 1022909]`

Workaround: There is no workaround, but if the metadata is modified using the legacy SAML 2.0 page, avoid further changes to the **Application Connector Setup** section in the **Applications** task to avoid overwriting the metadata that was manually configured in the legacy page.

5.4 Identity Server Returns Insecure Additional HTTP Cookies

Issue: Identity Server returns insecure additional HTTP cookies. This happens because Tomcat sets additional cookies that are not enabled with secure flag. [`Bug 999087`]

Workaround: Add the following in the `web.xml` file of Identity Server at `/opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml`:

```
<session-config>
 <cookie-config>
  <secure>true</secure>
 </cookie-config>
</session-config>
```

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 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.

7 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

© 2017 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.