Access Manager 4.3 Release Notes

October 2016

Access Manager 4.3 includes new features, 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 4.2 Service Pack 2 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.

1 What’s New?

Access Manager 4.3 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release introduces the following new features and enhancements:

1.1.1 Simplified Federations

Access Manager provides a simplified way to provide users secure, single sign-on (SSO) access to different web applications through the **Applications** page in Administration Console. The Applications page allows you to either create a federated connection between Access Manager and SAML 2.0 applications through connectors or use Basic Single Sign-on connectors to securely save users' credentials.

Connectors simplify the process of creating federated SAML 2.0 connections or to securely store users' credentials without having to create an HTML Form Fill policy. To see a list of all of the available connectors, see https://catalog.netiq.com.

The connectors also allow you easily control who has access to this application through role assignment. When you assign roles to the connectors, this provides access to the applications. When you assign roles to appmarks, this controls the visibility of the applications on the User Portal page. For more information, see Overview of Access Manager Applications in the Access Manager Applications Configuration Guide

1.1.1.1 Basic Single Sign-On

Basic Single Sign-on (SSO) allows users to securely store their credentials for existing accounts of on-line applications while providing a single sign-on experience for users. For example, a user Maria has an account for Evernote. Maria uses Evernote to take notes for her job in marketing. Instead of logging into Evernote with separate credentials each time she wants to use it, she would log into Evernote once and Basic SSO will save and replay her saved credential every time she accesses Evernote.

Basic SSO and Form Fill policies both automatically populate HTML forms. Form Fill policies scan each login page, accelerated through the Access Gateway, to see if the Form Fill policy can populate the credential information. For more information, see Form Fill Policies. Basic SSO does not go through the Access Gateway. Basic SSO provides connectors for the different applications. You configure the connector for the specific site. Basic SSO captures the users' credentials through a browser plugin or extension. It securely stores the users' credentials on Identity Server, never using the Access Gateway. For more information, see Understanding Basic Single Sign-On in the Access Manager Applications Configuration Guide.

1.1.1.2 SAML 2.0 Applications

SAML 2.0 applications allow you to create a federated connection between Access Manager and SAML 2.0 applications using connectors provided by Access Manager. Creating these applications in Administration Console replaces the steps for manually creating Service Providers that could SAML 2.0 applications in the past.

The new Applications page simplify the process of creating the federated connections and this provides your users with a secure single sign-on experience. For more information, see Understanding Federated Single Sign-On with SAML 2.0 in the Access Manager Applications Configuration Guide.

1.1.2 Analytics Dashboard

Access Manager 4.3 can integrate with Access Manager Analytics Server to display Analytics Dashboard that provides visual analytics for the access related data.

The Analytics Dashboard displays the data based on the events that are generated from Access Manager components. There are multiple graphs that display data in real-time and historic data mode. These graphs help in visualizing the access patterns, improving the policies, and getting insights about the usage of Access Manager. For more information about Analytics dashboard, see Analytics Dashboard (https://www.netiq.com/documentation/access-manager-43/admin/data/b1kyp92l.html) in the NetIQ Access Manager 4.3 Administration Guide.

1.1.3 Analytics Server

Access Manager 4.3 introduces a new component, Analytics Server. It is a standalone soft appliance which is easy to install and configure. It stores the data based on the events that generates from Identity Server and Access Gateway. It offers the following:

- The out-of-the-box reports based on the usage of Access Manager components.
- The data for Analytics Dashboard that provides visual analytics of user behavior, application access trends, health, performance and so on.

For more information about installing Analytics Server, see Installing Analytics Server in the NetIQ Access Manager 4.3 Installation and Upgrade Guide.

1.1.4 Device Fingerprinting

The device fingerprinting feature enables you to identify the type of device from which a user can log into the applications secured by Access Manager. The device can be a desktop, a laptop, or a mobile device. Each device has many characteristics such as operating system, hardware, browser characteristics. Access Manager uses device characteristics and user identity to create a unique fingerprint of the device. You can use the fingerprint to uniquely identify and associate a risk profile for the device.

A new Device Fingerprint Rule has been introduced in risk-based authentication. Using this rule, you can achieve the following activities as part of risk-based authentication:

- Uniquely identify users' devices used in login attempts
- Evaluate risks associated with a login attempt by using device identification details and decide the action based on the risk

For more information, see Device Fingerprinting in the NetIQ Access Manager 4.3 Administration Guide

1.1.5 Advanced Session Assurance

This release introduces Advanced Session Assurance to prevent session replay attacks by adding an additional layer of security to your sessions. When a session is established, Access Manager creates a unique fingerprint of the device from which the session is established. During the session, at a configurable time interval, Access Manager validates the session to ensure that the fingerprint matches with that of the device it originated from. Access Manager also generates a new ID for the session at a specified time interval. If the fingerprint or the session ID does not match, Access Manager logs the user out and invalidates the session. For more information, see Setting Up Advanced Session Assurance in the NetIQ Access Manager 4.3 Administration Guide.

1.1.6 Advanced Authentication

With this release, Advanced Authentication Access Manager plug-in comes bundled with Access Manager. Using Advanced Authentication methods, you can configure multi-factor authentication. Some of the supported Advanced Authentication classes include - FIDO U2F class, Password (PIN) class, and Smartphone class. For more information, see NetIQ Advanced Authentication in the NetIQ Access Manager 4.3 Administration Guide.

1.1.7 Impersonation

This release introduces Impersonation. Impersonation enables a help desk user to perform certain actions on behalf of users without knowing their credentials. The help desk user gains access to the user's existing configuration and performs the necessary actions required for troubleshooting. For more information, see Impersonation in the NetIQ Access Manager 4.3 Administration Guide

1.1.8 reCAPTCHA

reCAPCTHA feature enables you to protect your user login page against any spam, malicious registrations, and other forms of attack where bots or malicious software pretend as humans to access your computer. reCAPTCHA can help you secure Access Manager against attacks such as denial-of-service (DoS) and brute-force, which can impact the system performance to a large extent. For more information, see Enabling reCAPTCHA in the NetIQ Access Manager 4.3 Administration Guide.

1.1.9 Support for Swedish

Access Manager User Portal now supports Swedish in addition to German, French, Spanish, Italian, Japanese, Portuguese, Dutch, Chinese (Simplified), and Chinese (Traditional).

1.2 Operating System Support

In addition to the existing platforms, this release adds support to RHEL 6.8.

1.3 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.8
- Java 1.8.0_92
- Apache 2.2.27 (This release includes fixes for CVE-2014-0231, CVE-2014-0226, CVE-2013-5704,and CVE-2015-3183)
- OpenSSL 1.0.2j
- Tomcat 8.0.35
- iManager 2.7.7.7 (20160708_1400)

NOTE: On Windows, Administration Console and Identity Server use Tomcat version 7.0.68. The Tomcat version is not upgraded to version 8.0.35 due to dependency on iManager.

Access Manager 4.3 by default supports Tomcat 8.0.35 and OpenSSL 1.0.2j but Administration Console uses Tomcat version 7.0.68 due to dependency on iManager.

1.4 Browser Support

This release adds support for latest versions of the following browsers:

- **For accessing Access Gateway and Identity Server** (latest versions)
  - Internet Explorer
  - Chrome
  - Firefox
  - Safari
- **For accessing user portal and Administration Console**
  - Firefox (41 and later)
  - Chrome (45 and later)
  - Edge (23.10565 with EdgeHTML 13.10565 and later)
  - IE11 (11.0.9600 and later)

1.5 Enhancements

This release introduces the following enhancements:

- Section 1.5.1, “OAuth Enhancements,” on page 5
- Section 1.5.2, “New Default View,” on page 5
- Section 1.5.3, “Enhanced Access Manager Security,” on page 5

1.5.1 OAuth Enhancements

This release introduces the following OAuth enhancements:

- Access Gateway injects the Access token on behalf of web applications
- Access Manager authenticated user’s roles can be configured as OAuth scope attributes

1.5.2 New Default View

This release comes with a new default view. This view allows you to quickly access other tasks that you commonly need to access.

1.5.3 Enhanced Access Manager Security

To ensure higher security, Access Manager 4.3 configuration uses stronger TLS protocols, ciphers, and other security settings. For more information, see NetIQ Access Manager 4.3 Security Guide

1.6 Fixed Issues

This release includes software fixes for the following components:

- Section 1.6.1, “Administration Console,” on page 6
- Section 1.6.2, “Identity Server,” on page 6
- Section 1.6.3, “Access Gateway,” on page 7

1.6.1 Administration Console

The following issues are fixed in Administration Console:

- Section 1.6.1.1, “MobileAccess Only Supports Username And Password Contracts,” on page 6
- Section 1.6.1.2, “Various Ports Allow SSL/TLS Connections Over TLSv1.0,” on page 6

- On ports 9000 and 9001, there is a reverse shell connection to Administration Console. This leads to security vulnerabilities. (TID 7018159)
- The attributes with a shared settings defined Attribute Set are not editable. (TID 7018109)

1.6.1.1 MobileAccess Only Supports Username And Password Contracts

Issue: When you would enable MobileAccess, the only available options were **Secure Name/Password - Form** and **Name/Password - Form**. Access Manager 4.2 only supported the username and password contracts for MobileAccess. [Bug 989957]

Fix: Access Manager 4.3 or later allows you to select any available contracts. However, not all contracts work with mobile devices. You must select a contract that works with mobile devices. In general, any basic authentication contracts or certificate contracts do not work on mobile devices.

1.6.1.2 Various Ports Allow SSL/TLS Connections Over TLSv1.0

Issue: On various Access Manager components, ports 8444, 1443, 1444, and 4984 allow SSL/TLS connections over TLSv1.0 with a weak Diffie-Hellman (DH) Moduli. This is as per the Nessus scan report. [`Bug 999221 and 999870`]

Fix: The issue is resolved now as the SSL/TLS connection is restricted only to TLSv1.1 and TLSv1.2. Also, the ephemeral DH key size is restricted to 2048 bits.

1.6.2 Identity Server

The following issues are fixed in Identity Server:

- Section 1.6.2.1, “Issues in Using Multiple External Signing Certificates,” on page 6
- Section 1.6.2.2, “SAML Encrypted Assertion And Encrypted NameIdentifier Are Corrupted,” on page 7
- Section 1.6.2.3, “HTTP 400 Error After Upgrading Access Manager 4.2 to 4.2 SP1,” on page 7
- Section 1.6.2.4, “Extended Log Option Deletes Unrelated Log Files,” on page 7
- Section 1.6.2.5, “Kerberos Fallback Login Method Does not Report Expired Password,” on page 7
- Section 1.6.2.6, “Identity Server Returns a 500 Internal Server Error During an Authorization Code Request,” on page 7

- If the AuthnRequest contains a DOCTYPE element, Access Manager Identity Server does not process the request and returns an error. (TID 7018160)

1.6.2.1 Issues in Using Multiple External Signing Certificates

Fix: Identity Server can now use multiple external certificates for signing SAML 2.0 service providers. The external certificates can be from a single or multiple external keystores or HSMs. However, the certificates must be exportable as Identity Server does not send payloads to be signed to an external device. [`Bug 936014`]

1.6.2.2 SAML Encrypted Assertion And Encrypted NameIdentifier Are Corrupted

Issue: The SAML Encrypted Assertion and Encrypted NameIdentifier are corrupted due to a third party component. This issue is seen in Access Manager 4.2.1 and 4.2.2. [`Bug 992045`]

Fix: The issue is resolved.

1.6.2.3 HTTP 400 Error After Upgrading Access Manager 4.2 to 4.2 SP1

Issue: After upgrading Access Manager 4.2 to 4.2 SP1, few web applications return a HTTP 400 error. This is because the Server Name Indication (SNI) request expects only the host name and not the port name. [`Bug 983924`]

Fix: This issue is resolved now as only the host name of the backend server is sent.

1.6.2.4 Extended Log Option Deletes Unrelated Log Files

Issue: When you configure a proxy service with **Extended log** option and specify a value in the **Limit Number of Files to** field, it deletes all log files including the unrelated log files. [`Bug 973321`]

Fix: The issue is resolved now as each proxy service maintains only the log files specified in the **Limit Number of Files to** option and does not delete the unrelated log files.

1.6.2.5 Kerberos Fallback Login Method Does not Report Expired Password

Issue: When you try to log in with an expired password, the Kerberos Fallback Login method does not display the following error message: `Your password has expired`. This happens during Kerberos authentication when you configure `FALLBACK_AUTHCLASS com.novell.nidp.authentication.local.PasswordClass`. [`Bug 958478`]

Fix: The error message is displayed when the user logs in with an expired password.

1.6.2.6 Identity Server Returns a 500 Internal Server Error During an Authorization Code Request

Issue: For an OAuth scope, when you disable **Require user permission**, and in the **OAuth Global Settings**, you do not configure **Authorization Grant LDAP Attribute**, while authorization code request, the Identity Server returns a 500 internal server error. `Bug [981385]`

Fix: This issue is resolved as the authorization code request returns the authorization code instead of the 500 internal server error.

1.6.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.6.3.1, "Web Server Request URL Does Not Retain Encoded Characters," on page 8
- Section 1.6.3.2, "Access Gateway Does Not Rewrite the Response Page for Path-Based Proxy Service," on page 8
- Section 1.6.3.3, "Access Gateway Session Cookie Susceptible to Hijacking," on page 8
- Section 1.6.3.4, "Unable to Specify Contracts in the OAuth Resource Owner Credential Flow," on page 8
- Section 1.6.3.5, "Modifying Attribute Set Used by OAuth Scope Does Not Prompt for Identity Server Update," on page 8

- Section 1.6.3.6, “Cannot Inject LDAP Operational Attributes as OAuth Claims,” on page 8
- Section 1.6.3.7, “OAuth UserInfo Service Does Not Send Roles,” on page 9
- The Apache Gateway health is in yellow after you reboot the server. This happens because Activemq and Apache services start at the same time as they are in the same execution run-level. (TID 7018108)
- The Web application firewall (WAF) blocks initial redirects to ESP from Access Gateway protected resource. (TID 7018110)

1.6.3.1 Web Server Request URL Does Not Retain Encoded Characters

Issue: When the Web server requests for a URL, the URL does not retain the encoded characters before sending it to the back end Web server. [`Bug 934320`]

Fix: To fix this issue, a new advance option `NoCanonicalization on` is introduced. This option is added to the proxy service level which adds the nocanon keyword to the ProxyPass directives. You also need to enable `NAGGlobalOptions noURLNormalize=on` and `AllowEncodedSlashes on` advance options at the proxy service level.

1.6.3.2 Access Gateway Does Not Rewrite the Response Page for Path-Based Proxy Service

Issue: The selection of path-based application based on the URL of a request is case-sensitive. Due to this, when users access the URL with a different case then the one configured, the parent proxy gets selected. This leads to error in rewriting of the backend URL. [`Bug 925213`]

Fix: This issue is resolved now as the selection of path-based proxy service is no longer case-sensitive.

1.6.3.3 Access Gateway Session Cookie Susceptible to Hijacking

This issue is resolved as part of the new Access Manager 4.3 feature - Advanced Session Assurance. For more information, see Setting Up Advanced Session Assurance. [`Bug 345531`]

1.6.3.4 Unable to Specify Contracts in the OAuth Resource Owner Credential Flow

This issue is resolved now. A new option **Contracts for Resource Owner Credentials Authentication** is added in the OAuth Global Settings interface. This option enables you to specify authentication contracts in the OAuth Resource Owner flow. For more information, see Defining Global Settings. [`Bug 979605`]

1.6.3.5 Modifying Attribute Set Used by OAuth Scope Does Not Prompt for Identity Server Update

Issue: When you modify an existing OAuth attribute set, the system does not prompt for an Identity Server update. Due to this, Access Gateway does not inject the OAuth scope’s modified attributes. [`Bug 966282`]

Fix: The issue is resolved now as the Access Gateway injects the modified attributes.

1.6.3.6 Cannot Inject LDAP Operational Attributes as OAuth Claims

Issue: Access Gateway cannot inject LDAP operational attributes defined as OAuth claims. [`Bug 966249`]

Fix: The issue is resolved now as Access Gateway can inject operational attributes like `entryDN` as OAuth claims.

1.6.3.7 OAuth UserInfo Service Does Not Send Roles

Issue: Access Manager authenticated user's roles cannot be configured as OAuth scope attributes, due to this, the UserInfo service does not return roles. [`Bug 947310`]

Fix: The issue is resolved now as the OAuth UserInfo returns the roles.

2 Installing or Upgrading

After purchasing Access Manager 4.3, log in to the NetIQ Downloads page and follow the link that allows you to download the software. The following files are available:

IMPORTANT: After upgrading to Access Manager 4.3, you must clear the browser cache to view the upgraded Administration Console. For more information, see TID 7018166.

Table 1 *Files Available for Access Manager 4.3*

Filename	Description
`AM_43_AccessManagerService_Linux64.tar.gz`	Contains Identity Server and Administration Console .tar file for Linux.
`AM_43_AccessManagerService_Win64.exe`	Contains Identity Server and Administration Console .exe file for Windows Server.
`AM_43_AccessGatewayAppliance.iso`	Contains Access Gateway Appliance .iso file.
`AM_43_AccessGatewayAppliance.tar.gz`	Contains Access Gateway Appliance .tar file.
`AM_43_AccessGatewayService_Win64.exe`	Contains Access Gateway Service .exe file for Windows Server.
`AM_43_AccessGatewayService_Linux64.tar.gz`	Contains Access Gateway Service .tar file for Linux.
`AM_43_AnalyticsServerAppliance.iso`	Contains Analytics Server Appliance .iso file.

For information on the upgrade paths, see Section 3, "Supported Upgrade Paths," on page 10. For more information about installing and upgrading, see the NetIQ Access Manager 4.3 Installation and Upgrade Guide.

3 Supported Upgrade Paths

To upgrade to Access Manager 4.3, you need to be on one of the following versions of Access Manager:

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

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

4 Verifying Version Number After Upgrading to 4.3

After upgrading to Access Manager 4.3, verify that the version number of the component is indicated as **4.3.0.0-392**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.3.0.0-392**.

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, “Services Fail to Start After You Stop Tomcat,” on page 10
- Section 5.2, “User Logs Out After Cookies Renewal Interval,” on page 11
- Section 5.3, “500 Internal Error on Mixed Node Cluster,” on page 11
- Section 5.4, “Issue with reCAPTCHA Threshold Value,” on page 11
- Section 5.5, “Random Signature Verification Messages in Identity Server Catalina.out,” on page 11
- Section 5.6, “Error in Office 365 Active Applications After Upgrading to Access Manager 4.3,” on page 11
- Section 5.7, “Mobile Device Registration Contracts Only Work in Certain Circumstances,” on page 12

5.1 Services Fail to Start After You Stop Tomcat

Issue: When you stop Tomcat abruptly using the `kill` command, all services fail to start on the Access Manager respective components. This occurs on SLES 12 SP1 and RHEL 7.2. `[Bug 1002957]`

Workaround: To workaround this issue, you need to restart the respective services using the following command:

- `/etc/init.d/novell-ac restart`

- /etc/init.d/novell-idp restart
- /etc/init.d/novell-mag restart

5.2 User Logs Out After Cookies Renewal Interval

Issue: When you enable session assurance on Access Gateway cluster, and enable **SSL with Embedded Service Provider** but disable **Enable SSL between Browser and Access Gateway**, and **Redirect Requests from Non-Secure Port to Secure Port**, user logs out after cookie renewal interval. This is due to the AGIDC cookie mismatch. [Bug 999828]

Workaround: To workaround this issue, you need to either select all of the three options, or deselect all of them.

5.3 500 Internal Error on Mixed Node Cluster

Issue: When a user portal is running on a mixed node cluster environment, and the request moves from Access Manager 4.3 to a node in same session that is running on Access Manager version other than 4.3, a 500 internal error occurs. [Bug 1002174]

Workaround: To workaround this issue, you need to modify the web.xml file of the Access Manager version other than 4.3. In the web.xml file, replace /ospui/osp/* with /ospui/* in ClusterRequestFilter and restart Identity Server.

5.4 Issue with reCAPTCHA Threshold Value

Issue: If you set the threshold value to more than zero, reCAPCTHA may be skipped by refreshing the browser. [Bug 1000312]

Workaround: To workaround this issue, it is recommend to set the threshold value to zero.

5.5 Random Signature Verification Messages in Identity Server Catalina.out

Issue: In Identity Server, Signature verification messages are printed randomly (Example: INFO: Verification successful for URI "#ideihgNhCjwBxlxy6n74D9yiwUWqk) in catalina.out. This happens even when no log level is selected in the **Component File Logger Levels** field. [Bug 1000067]

Workaround: Currently, there is no workaround for this issue.

5.6 Error in Office 365 Active Applications After Upgrading to Access Manager 4.3

Issue: After you upgrade Access Manager 4.2.2 to 4.3, the Office 365 active applications like Skype for Business may fail and display the following error message: There was a problem acquiring a personal certificate required to sign in. [Bug 999476]

This issue occurs when Skype for Business does not initiate a SSL connection in TLSv1.1 or TLSv1.2. Since the connection is initiated only in TLSv1, you need to enable it in Identity Server.

Workaround: To workaround this issue, you need to add the following in the `NIDP_Name=connector` element of the `server.xml`:

- TLSv1 to `sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2"`
- `TLS_RSA_WITH_AES_128_CBC_SHA`, or `TLS_RSA_WITH_AES_256_CBC_SHA` to the ciphers list

5.7 Mobile Device Registration Contracts Only Work in Certain Circumstances

Issue: The mobile device registration contracts only work if the method and the contract have the same name. If they have different names, the methods satisfied by mobile contracts do not work. [`Bug 1004362`]

Workaround: To workaround this issue, ensure that the mobile authentication contract and the method have the same name.

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/.

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