Access Manager Appliance 4.5 Release Notes

April 2019

Access Manager Appliance 4.5 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.

For information about the previous release, see Access Manager Appliance 4.4.4 Release Notes (https://www.netiq.com/documentation/access-manager-44-appliance/accessmanager444-release-notes/data/accessmanager444-release-notes.html).

For more information about this release and for the latest release notes, see the Documentation (https://www.netiq.com/documentation/access-manager-45-appliance/) page. To download this product, see the Product (https://www.netiq.com/products/access-manager/) page.

If you have suggestions for documentation improvements, click **comment on this topic** at the top or bottom of the specific page in the HTML version of the documentation posted at the Documentation (https://www.netiq.com/documentation/access-manager/) page.

For information about Access Manager support lifecycle, see the Product Support Lifecycle page.

What's New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

New Features and Enhancements

This release introduces the following new features and enhancements:

OAuth Enhancements

Access Manager provides the following enhancements to the OAuth support for better application interoperability, flexibility, and improved security. The enhancements include:

Support for Introspection of an Access Token or a Refresh Token

An authorized resource server can introspect an access token or a refresh token to check the status of the token.

When a client application sends a token to a resource server for authorization, the resource server must know whether the token is valid. To check the status of the token, the resource server can send an API request to the authorization server (Identity Server) introspection endpoint. This endpoint responds with a JSON document that includes the token status (`active`: true or false) and the meta information of the token. For more information about token introspection, see RFC 7662 (https://tools.ietf.org/html/rfc7662).

The Token Introspect Endpoint is listed in the **Endpoint summary** page of **OAuth & OpenID Connect**. For information about the request and response for introspecting a token, see "Token Introspect Endpoint" in *Access Manager 4.5 OAuth Application Developer Guide*.

HTTP Basic Authentication Support to Authenticate Client Applications

Access Manager now supports the requests containing client credentials within the basic authorization header. The client application can use any of the following ways to request for a token:

- Use `client_id` and `client_secret` in the request body parameters.
- Send the client credentials in the basic authorization header. For more information, see RFC 6749 (https://tools.ietf.org/html/rfc6749?#section-2.3.1).

The request containing client credentials within the basic authorization header is supported for the following endpoints:

- Token Introspect Endpoint
- Token Endpoint
- Revocation Endpoint

The ID Token Signing Algorithm for the Response Is Now Mandatory During the Client Registration

ID Token Signed Response Algorithm is now a mandatory field if you have selected **Token Types:** as **ID Token** during the client registration. For more information, see "Registering OAuth Client Applications".

Support for Adding User Attributes to an ID Token and Adding Claims to both Access and ID Tokens

You can now add the required user attributes and user claims/ permissions to ID token. Also, you can add claims/permissions to access token. For more information about configuring the scope for ID and Access tokens and see "Configuring User Claims or Permission in Scope".

Support for Multiple Response Type Encoding

You can specify the response mode as query, fragment, or form_post in the request to the authorization endpoint. Also, you can specify the none response type when sending the request to the authorization endpoint. For more information about the request parameters, see "Authorization Endpoint".

For information about response types and response modes, see OAuth 2.0 Multiple Response Type Encoding Practices (https://openid.net/specs/oauth-v2-multiple-response-types-1_0.html).

Enhanced Metadata Endpoint

In addition to the existing details, the metadata endpoint now provides the following details:

- Revocation Endpoint
- Introspection Endpoint
- Supported response type
- Supported response mode
- Token endpoint authentication method
- Supported revocation endpoint authentication methods
- Supported introspection endpoint authentication methods

For more information about metadata endpoint, see "Metadata Endpoint".

The TokenInfo Endpoint Is Deprecated

The TokenInfo Endpoint is deprecated. Therefore, it will not be enhanced any longer. You can use Token introspection to know the status of the token. For information about the endpoints, see "Viewing Endpoint Details".

Support for Using Tokens in the Binary Format

The default format for tokens is JWT. To continue using tokens in the binary format, you can configure the **OAUTH TOKENS IN BINARY FORMAT** setting in the Identity Server global options. It is recommended to use the default JWT format. However, if the legacy client application cannot manage JWT tokens, then use this setting until you update the client application to use JWT tokens.

If this setting is selected, the new features, such as token encryption using resource server keys and token revocation, will not be available. For more information about this setting, see "Configuring Identity Server Global Options" in the NetIQ Access Manager Appliance 4.5 Administration Guide.

Enhanced Application Connector Catalog

The **Application Connector Catalog** has been updated with new SAML and SSO Assistant connectors. In addition, the catalog now provides the following tabs to categorize connectors based on the type and to improve the search:

- **All**: Includes all types of connectors. See Application Connector Catalog > All (https://catalog.netiq.com/ncarest/displayCatalog?type=all).
- **SAML**: Includes all SAML connectors that have the capability of providing SSO for existing user accounts. These connectors do not perform user accounts provisioning to the SaaS providers. See Application Connector Catalog > SAML (https://catalog.netiq.com/ncarest/displayCatalog?type=saml).
- **Account Management**: Includes SAML connectors that can be configured either for SAML only (to provide SSO for existing user accounts) or for SAML with Account Management to get the added benefit of user provisioning. See Application Connector Catalog > Account Management (https://catalog.netiq.com/ncarest/displayCatalog?type=accmgmt).
- **WS Federation**: Includes the WS Federation connector. See Application Connector Catalog > WS Federation (https://catalog.netiq.com/ncarest/displayCatalog?type=wsfed).
- **SSO Assistant**: Includes all SSO Assistant connectors. See Application Connector Catalog > SSO Assistant (https://catalog.netiq.com/ncarest/displayCatalog?type=basicsso).

Support for Provisioning User Accounts Using SaaS Account Management

SaaS Account Management (SAM) in Access Manager enables you to provision user accounts to your SaaS providers automatically. SAM performs the following actions based on changes made to the user store and user groups that are configured at the SAML Application Configuration page in Access Manager:

- Automatically provision user accounts to supported SAML applications.
- Synchronize any changes you make in your user store.
- Automatically deprovision accounts for connected applications based on changes made in your user store.

The provisioning and deprovisioning can also happen if you make changes in the Account Management tab of the connector where it is imported.

To provision SAML accounts by using SAM, you must first purchase and deploy the SAM appliance and configure the appropriate SAM connector for the SAML application. For more information about deploying the SAM appliance and SAM connectors, see the NetIQ SaaS Account Management Installation Guide (https://www.netiq.com/documentation/saas-account-management-10/sam-install/data/bookinfo.html) and SaaS Account Management Connectors Guide (https://www.netiq.com/documentation/saas-account-management-10/sam-connectors/data/bookinfo.html).

Access Manager provides a number of SAML connectors that support account provisioning when SAM is deployed. To see the list of all account management connectors that Access Manager provides, see Application Connector Catalog > Account Management (http://catalog.netiq.com/ncarest/displayCatalog?type=accmgmt).

Secure API Manager Integration

You can integrate Access Manager with Secure API Manager to extend Access Manager's capability of securing micro-services, REST-based web services, IoT devices, and legacy API systems.

Secure API Manager uses the OAuth feature of Access Manager to allow token-based authorization for the API requests.

For information about Secure API Manager, see Secure API Manager Documentation (https://www.netiq.com/documentation/secure-api-manager-10/).

Access Manager and Advanced Authentication Integration Guide

This release introduces Access Manager and Advanced Authentication Integration Guide in the documentation library. This guide provides the step-by-step information to integrate Advanced Authentication with Access Manager to use multi-factor authentication.

For more information, see *Multi-Factor Authentication Using Advanced Authentication*.

Updates for Dependent Components

This release adds support for the following dependent components:

- Apache 2.4.37
- eDirectory 9.1.1.1
- iManager 3.1.2
- OpenSSL 1.0.2r
- ZuluOpenJDK 1.8.0_192

OpenID Certification

Access Manager is now OpenID Connect certified for the following OpenID Provider conformance profiles:

- Basic
- Implicit
- Hybrid
- Config

For more information, see the OpenID Certification (https://openid.net/certification/#OPs) page.

Software Fixes

Access Manager 4.5 includes software fixes for the following components:

Administration Console

The following issue is fixed in Administration Console:

The Silent Installation of Configuration Store Fails In Access Manager Appliance

Issue: When Access Manager Appliance is installed with two IP addresses, configured as private and public. If the Configuration Store host file is configured with one IP address (public) and Access Manager Appliance is configured to listen to the private IP address then the Configuration Store installation fails. (Bug 1064721)

Fix: From this release, Access Manager Appliance adds the private IP address to the host file with the existing public IP address. Configuration Store creates the certificate for the IP addresses mentioned in the host file.

Identity Server

The following issues are fixed in Identity Server:

Enabling Session Assurance Causes Issues

Issue 1: When Session Assurance is enabled, customization of `top.jsp` is removed. This issue occurs because the parameters posted to the `/nidp/app/login` location are deleted. This issue occurs in Access Manager 4.3. (Bug 1074840)

Issue 2: When Session Assurance is enabled, the external authentication to Identity Server fails to redirect to Access Gateway. (Bug 1079654)

Fix: From this release, Session Assurance starts working when a request that requires user login is received from the user's browser. The regular Session Assurance checks are enabled after the user authenticates successfully.

Customization of the TOTP Form Is Lost When Used After Kerberos Method

Issue: When a contract contains Kerberos as the first method and TOTP as the second method, customization of the top section of the page is lost during the TOTP authentication. This issue occurs only when the Kerberos method is executed successfully without a fallback to another method. This issue occurs only when the Kerberos method is executed successfully without a fallback to another method. (Bug 1111268)

Fix: A check is introduced to ensure that the TOTP form is not missing the customization. If the TOTP form is missing the customization, the TOTP form is reloaded with customization.

OAuth Endpoints Do Not Accept Unencrypted Tokens

TokenInfo, UserInfo, and Token Introspect fail to accept the signed token in the authorization header because the token is not encrypted. Also, the signed token is not introspected by the Token Introspect endpoint. (Bug 1102336)

Identity Server Is Not Updated When the LDAP Server Replica Is Not Reachable

Issue: When the user store replicas are not reachable, the Identity Server update moves to the pending state and takes a longer time to update. Also, the heartbeat URL takes a longer time to display the Identity Server health. If the heartbeat URL is configured at the load balancer, the load balancer will stop Identity Servers. (Bug 1121936)

Fix: From this release, the LDAP `Operation timeout` and the `Idle Connection timeout` configured in Administration Console are now considered by Identity Servers while making LDAP connection to the user stores.

Access Manager Does Not Support the Multi-Value antiClickjacking XSS Controls

Issue: In a multi-domain environment, Identity Server authentication fails while using the single value of the `anticlickjacking X-FRAME-OPTIONS` header. (Bug 1079346)

Fix: Access Manager allows configuring custom response headers for every Identity Servers. You can also create the Content Security Policy header that can be used for securing the communication between the client browser and Identity Server.

For more information, see "Configuring the Custom Response Header for an Identity Server Cluster" in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Access Manager Does Not Add A New OpenID Connect Application

Issue: When an OpenID Connect application is created, Administration Console stores the application attributes in eDirectory. eDirectory can store the string type attributes up to a limit. If you create a new application after the limit is reached, the `Unexpected error` message is displayed. (Bug 1104160)

Fix: From this release, the `nidsOAuth2CFGXML` attribute type is changed from string to stream to fix this issue.

Access Gateway

The following issues are fixed in Access Gateway:

- "The Favicon.ico Requests Cause Browser Connection Limitations" on page 7
- "Access Gateway Considers Valid URLs As XSS Attack" on page 8

The Favicon.ico Requests Cause Browser Connection Limitations

Issue: Access Gateway considers the client's request for the favicon.ico as public and each request creates a new TCP connection or uses an existing one. When a limit is specified for the number of connections per user session, the favicon.ico requests can block new client requests. (Bug 1110753)

Fix: The following two options are introduced to block the favicon.ico requests. It prevents the favicon.ico requests to create new TCP connections.

`NAGGlobalOptions DisableFavicon`

`NAGHostOptions DisableFavicon`

For more information about these options, see "Configuring Global Advanced Options" and "Configuring Advanced Options for a Domain-Based and Path-Based Multi-Homing Proxy Service" in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Access Gateway Considers Valid URLs As XSS Attack

Issue: The reference header of every browser request is checked for possible XSS attacks. An administrator can not specify exceptions to skip this check. (`Bug 1083726`)

Fix: The following fixes are introduced to fix this issue:

- The following global options are introduced:
  - `NAGGlobalOptions DisableDetectXSS=on`
  - `NoXSSURLs`
  - `NoXSSRefererURLs`

  For more information about these options, see "Configuring Global Advanced Options" in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.
- The `NAGHostOptions DisableDetectXSS=on` proxy level advanced option is introduced.

  For more information about this option, see "Configuring Advanced Options for a Domain-Based and Path-Based Multi-Homing Proxy Service" in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

Installing or Upgrading

After purchasing Access Manager Appliance 4.5, log in to the NetIQ Downloads (http://dl.netiq.com/) 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 4.5*

Filename	Description
`AM_45_AccessManagerAppliance.iso`	Contains Access Manager Appliance .iso file.
`AM_45_AccessManagerAppliance.tar.gz`	Contains Access Manager Appliance .tar file.

NOTE: This release does not provide files for installing or upgrading Analytics Server. For a fresh installation of Analytics Server, use `AM_442_AnalyticsServerAppliance.iso` file, and then upgrade Analytics Server to 4.4 Service Pack 3 by using `AM_443_AnalyticsServerAppliance.tar.gz` file. If you are already using a previous version of Analytics Server, then upgrade to Analytics Server 4.4 Service Pack 3.

For information about the upgrade paths, see "Supported Upgrade Paths" on page 9. For more information about installing and upgrading, see the NetIQ Access Manager Appliance 4.5 Installation and Upgrade Guide.

Verifying Version Number After Upgrading to 4.5

After upgrading to Access Manager Appliance 4.5, verify that the version number of the component is indicated as **4.5.0.0-191**. To verify the version number, perform the following steps:

1. In Administration Console Dashboard, click **Troubleshooting > Version**.
2. Verify that the **Version** field lists **4.5.0.0-191**.

Supported Upgrade Paths

To upgrade to Access Manager Appliance 4.5, you must be on one of the following versions of Access Manager:

- 4.4 Service Pack 4
- 4.4 Service Pack 3
- 4.4 Service Pack 2

For more information about upgrading Access Manager Appliance, see "Upgrading Access Manager Appliance" in the *NetIQ Access Manager Appliance 4.5 Installation and Upgrade Guide*.

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).

Creating the EC Certificate Displays the PKI -1217 Error Message

Issue: Fresh installation of Access Manager 4.5 does not create the ECDSA Root CA certificate and displays the `PKI -1217` error message. (Bug `1126123`)

Workaround: No workaround is available.

Issue in Using an EC Certificate as the OAuth Signing Certificate

Issue: The JSON Web Key Set endpoint stops working when you assign an EC certificate as the OAuth signing certificate. This issue occurs because the SAML metadata does not accept the EC certificate for signing and encryption. (Bug `1124189`) and (Bug `1128131`)

Workaround: Use the REST certificate as OAuth signing certificate.

iManager Displays Certificate Revocation List Endpionts

Issue: When Access Manager is upgraded to the 4.5 version, all new certificates created by iManager include a list of Certificate Revocation List (CRL) endpoints. The endpoints refer to the configuration store IP address. CRL endpoints are disabled for the fresh installation of Access Manager 4.5. (Bug 1126434)

Workaround: See TID 7023739 (https://support.microfocus.com/kb/doc.php?id=7023739).

Promoting a Secondary Administration Console to Primary Does Not Work Properly

Issue: When a secondary Administration Console is promoted to primary Administration Console then it does not allow installation of new Identity Servers. (Bug 1122742)

Workaround: See TID 7023786 (https://support.microfocus.com/kb/doc.php?id=7023786).

The iManager Certificate Server CRL List on the Certificate Authority Object Is Empty

Issue: The CRL tab of iManager Certificate Server Plugin does not display the CRL Endpoints. This issue occurs because the `ndspkiCRLContainerDN` attribute is missing from the Certificate Authority object. (Bug 1126281)

Workaround: No workaround is available.

Single Sign-On to Skype for Business Does Not Work

Issue: You cannot log in to Skype for Business 2016 using the Identity Server login page. This issue occurs because Access Manager uses the JQuery version that is higher than the version used in the earlier release of Access Manager. The higher version is used for preventing any security vulnerability and this version of jQuery is not compatible with the Skype for Business 2016 application. (Bug 1126708)

Workaround: To continue using an old version of jQuery, which is less secure, you can replace the new jQuery files with the old file. For more information about how to replace these files, see Single Sign-on Fails in Skype for Business 2016 (https://www.netiq.com/documentation/access-manager-45/admin/data/b65ogn0.html#skype-2016-not-working) in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

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 (http://www.netiq.com/support/process.asp#phone).

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

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/.