Access Manager 4.4 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 more information about this release and for the latest release notes, see the Documentation page. To download this product, see the Product (https://www.netiq.com/products/access-manager/) page.

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

- Section 1, “What’s New?,” on page 1
- Section 2, “Installing or Upgrading,” on page 11
- Section 3, “Verifying Version Number After Upgrading to 4.4,” on page 12
- Section 4, “Supported Upgrade Paths,” on page 12
- Section 5, “Known Issues,” on page 13
- Section 6, “Contact Information,” on page 19
- Section 7, “Legal Notice,” on page 19

1 What’s New?

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

- Section 1.1, “New Features and Enhancements,” on page 1
- Section 1.2, “Operating System Upgrade,” on page 8
- Section 1.3, “Updates for Dependent Components,” on page 9
- Section 1.4, “Browser Support,” on page 9
- Section 1.5, “Software Fixes,” on page 9

1.1 New Features and Enhancements

This release introduces the following new features and enhancements:

- Section 1.1.1, “Support for Business-to-Consumer Capabilities,” on page 2
- Section 1.1.2, “New Mobile SDK for iOS,” on page 3
1.1.1 Support for Business-to-Consumer Capabilities

Access Manager 4.4 re-looks at the Consumer Identity and Access Management needs of customers and offers a solution that addresses a broad set of Business-to-Customer (B2C) use cases. B2C solution enables you to securely identify and engage with your customers while providing a seamless experience on any device, app, or service they are using.

Access Manager, in combination with Self Service Password Reset (https://www.netiq.com/products/self-service-password-reset/) and Advanced Authentication (https://www.netiq.com/products/advanced-authentication/) products, delivers support for B2C use cases such as user on-boarding, account validation, customizable web logins, portal integration, device registration and management, preference, profile and privacy management. These are achieved through a broad set of APIs, customizable scripts (packaged as a convenient framework library) and built-in portal to support these use cases. Access Manager enables customers to set up end-consumer facing applications and portals, enabling better end-consumer interaction. Access Manager also provides tools to support privacy and security requirements outlined in regulations such as GDPR and PSD2.

Access Manager B2C features are delivered through a combined solution of Access Manager and Self Service Password Reset. Advanced Authentication is also required to support specific advanced authentication functions. The following is the list of Access Manager B2C features:

- **User-driven functionalities**: To enable users to perform self-registration and manage their devices and applications without administrative intervention.
- **Better user experience**: To enable seamless access to applications from anywhere and from any device.
- **Intelligent and secure authentication mechanism**: To provide a secure access to users by using methods such as risk-based authentication, identity proofing-email verification, device fingerprinting, and multi-factor authentication.
- **Social authentication**: To grant access based on users' social media identity to reduce their overhead of managing multiple accounts and for just-in-time provisioning.

- **APIs**: To enable better integration with your applications, Access Manager provides APIs that enable programmatic interfaces to access administration and user data.

- **Scalability**: To support a large number of identities and to provide always-available access.

- **Data privacy**: To ensure privacy of users’ data by asking their consent and enabling them to select the information they want to share.

- **End user data control**: To enable end users to view, manage, and delete their applications and devices. It also enables end users to manage their profile.

For more information, see Business to Consumer Access Management in the *NetIQ Access Manager 4.4 Administration Guide*.

### 1.1.2 New Mobile SDK for iOS

The Mobile SDK for iOS provides simple APIs that enable developers to allow their native mobile apps perform OAuth and OpenID Connect protocol flows with the providers and be integrated with Access Manager server achieving server-side SSO. It adheres to OAuth 2.0 best practices for native apps.

In addition, the SDK provides convenient methods to assist with common tasks in the flow, achieves native mobile app SSO, and basic device management.

You can download Mobile SDK 2.0 for iOS file from the Developer Documentation page.

### 1.1.3 Connector Studio

Connector Studio enables you to develop customizable federation and SaaS single sign-on (SSO) application connectors. Application connectors significantly reduces the configuration steps required to enable federated SSO to SaaS and other federation enabled services.

For more information, see Using Custom Connectors in the *Access Manager Applications Configuration Guide 4.4*.

### 1.1.4 Support for Role-Based Access Control to Office365

This release provides a connector for Microsoft Office 365 that allows you to create a federated connection between Access Manager and Microsoft Office 365 by using WS Federation and WS-Trust protocols. This connector allows role-based authorization to Office365 applications.

For more information, see Configuring the Applications for Office 365 Using WS Federation and WS-Trust in the *Access Manager Applications Configuration Guide 4.4*.

### 1.1.5 New Basic Single Sign-On Connectors

This release adds a number of new Basic SSO connectors in the Applications Catalog.

For the list of supported connectors, see Application Connector Catalog (https://catalog.netiq.com/ncarest/displayCatalog).

### 1.1.6 REST APIs for Connectors

Creation and configuration of application connectors can now be done over a set of programmable REST APIs.
1.1.7 Support for Rebranding and Customizing MobileAccess App

This release provides the following enhancements for the MobileAccess App:

- You can change the background color and images for the login screen, app landing, preference, and self-service pages.
- Support for restricting accessing applications using jailbroken or rooted devices.

1.1.8 OAuth Enhancements

Extended Support for OAuth protocol with a number of new enhancements that offer better application interoperability, flexibility and improved security. The enhancements include:

- Section 1.1.8.1, "Tokens in JSON Web Token Format," on page 4
- Section 1.1.8.2, "Client Specific Token Time-out Configuration," on page 4
- Section 1.1.8.3, "Virtual Attributes in Scope," on page 4
- Section 1.1.8.4, "Single Sign-On to a Native Application Using Persistent Cookie," on page 5
- Section 1.1.8.5, "Proof Key for Code Exchange Support for Authorization Flow," on page 5
- Section 1.1.8.6, "Enhanced TokenInfo Endpoint," on page 5
- Section 1.1.8.7, "Token Revocation Using REST API," on page 5
- Section 1.1.8.8, "Exchange SAML 2 Assertion with OAuth Access Token," on page 5

1.1.8.1 Tokens in JSON Web Token Format

A JSON Web Token is an easy-to-use compact format for developers. It is used for transmitting user information as JSON objects between authorization server (Identity Server) and resource server in a secure manner. This allows resource server to validate the access token without the need to send the token back to Access Manager for validation. A resource server can validate only if Access Manager encrypts the access token by using the resource server’s key. The data inside a JWT token is encoded and signed. Based on the requirement, you can configure a resource server in Access Manager to encrypt or not encrypt the access token.

For more information about encrypting access token, see Encrypting Access Token in the NetIQ Access Manager 4.4 Administration Guide.

1.1.8.2 Client Specific Token Time-out Configuration

You can now specify token time-out configuration for each client application during the client registration. When you are registering a client application, you can configure the token time-out under Token Timeout Configuration - Optional. If you do not configure the time for token time-out, Access manager considers the time-out configured in the OAuth Global Settings page. For more information about token time-out configuration, see Registering OAuth Client Applications in the NetIQ Access Manager 4.4 Administration Guide.

1.1.8.3 Virtual Attributes in Scope

You can now use virtual attributes as scopes within access token. For information about using claims and virtual attributes in scope, see Configuring User Claims or Permission in Scope in the NetIQ Access Manager 4.4 Administration Guide.
1.1.8.4 Single Sign-On to a Native Application Using Persistent Cookie

When registering client applications, you can enable Use Persistent Cookie in Client Type. This allows single sign-on for a user who uses client applications on a desktop or a mobile. For more information about this option, see Registering OAuth Client Applications in the NetIQ Access Manager 4.4 Administration Guide.

1.1.8.5 Proof Key for Code Exchange Support for Authorization Flow

Access Manager supports Proof Key for Code Exchange by OAuth Public Clients (PKCE) specification defined by RFC 7636. If client initiates PKCE flow, Access Manager will support PKCE.

For more information about PKCE, see API documentation.

1.1.8.6 Enhanced TokenInfo Endpoint

TokenInfo Endpoint supports both GET and POST format. It provides additional details about the tokens that is defined in the token introspection RFC. For information about TokenInfo Endpoint, see Viewing Endpoint Details in the NetIQ Access Manager 4.4 Administration Guide.

1.1.8.7 Token Revocation Using REST API

An administrator can revoke the refresh token and its associated access token by sending the refresh token to Revocation Endpoint.

Access Manager follows RFC 7009 to revoke the refresh tokens by using REST APIs. For more information, see API documentation.

A new option, Always Issue New Refresh Token is introduced that can be selected during client registration. If this option is selected, Access Manager will issue new refresh tokens with the same time-out configuration whenever a refresh token is used for issuing an access token. This will help in changing the already issued binary refresh token to JWT refresh token. For information about this option, see Registering OAuth Client Applications in the NetIQ Access Manager 4.4 Administration Guide.

NOTE: You can revoke only JWT refresh tokens. For previously issued refresh tokens, you can use the Always Issue New Refresh Token option to exchange the previously issued binary tokens with new JWT refresh tokens.

1.1.8.8 Exchange SAML 2 Assertion with OAuth Access Token

Access Manager complies with RFC 7521 and RFC 7522 to support SAML 2 bearer profile with authorization grant flow. You can use a SAML 2 assertion to request an access token. Access Manager can validate the assertion and generate the access token, which can be used to access OAuth protected resources.

For more information about this enhancement, see Exchanging SAML 2 Assertions with Access Token in the NetIQ Access Manager 4.4 Administration Guide.

1.1.9 SAML Enhancements

Access Manager provides the following SAML enhancements:

- Section 1.1.9.1, “Ability to Include Multiple Configurations in Identity Server Cluster for the Same Service Provider,” on page 6
- Section 1.1.9.2, “Minimize Service Interruption for a SAML 2 Service Provider,” on page 6
1.1.9.1 Ability to Include Multiple Configurations in Identity Server Cluster for the Same Service Provider

Access Manager now supports multiple instances of the same service provider on a single Identity Server cluster. Previously, an Identity Server cluster was able to support only a single instance of a given service provider. Now, Access Manager introduces a unique ID that you can use to differentiate between instances of the same service provider.

For more information about the unique ID, see Creating Different Instances of a SAML 2.0 Service Provider in an Identity Server Cluster in the NetIQ Access Manager 4.4 Administration Guide.

1.1.9.2 Minimize Service Interruption for a SAML 2 Service Provider

Access Manager minimizes service interruption by introducing the following:

**Additional signing certificate:** Access Manager now allows you to add a second signing certificate to a trusted service provider. The second certificate will have a longer expiry time and will have some overlapping validity interval. The secondary certificate functions as a fall-back option when the default signing certificate expires, minimizing the chances of a service interruption.

For more information, see Minimizing Service Interruption of SAML 2.0 Service Providers in the NetIQ Access Manager 4.4 Administration Guide.

**Update the SAML 2 trusted provider configuration:** After changing the settings of a SAML 2 service provider in Identity Server, you can now update the Identity Server with the SAML2 changes alone. Previously, you were forced to update the entire configuration, which sometimes caused the service provider to be temporarily unavailable.

For more information, see Minimizing Service Interruption of SAML 2.0 Service Providers in the NetIQ Access Manager 4.4 Administration Guide.

1.1.9.3 Add Step Up Authentication After Identity Provider Authentication

You can now force users to provide additional authentication to get authenticated to the SAML 2 services. This is used when a secure data is getting exchanged. The step up authentication provides additional security to the services. Identity Server acts as a service provider and can prompt for additional authentication when a request is sent for accessing SAML 2 services.

For more information about using step up authentication, see Selecting a User Identification Method for Liberty or SAML 2.0 in the NetIQ Access Manager 4.4 Administration Guide.

1.1.9.4 Global Option for the SAML 2.0 Attribute Consuming Index Value

You can now define the SAML2 ATTRIBUTE CONSUMING INDEX value globally. If this value is not set in SAML 2 > Options, the value specified in the global option is considered. You can specify the default index value globally.

For more information about this option, see Configuring Identity Server Global Options in the NetIQ Access Manager 4.4 Administration Guide.
1.1.10 OAuth Claims-Based Mechanism for Advanced Authentication Integration

In addition to the existing classes, this release provides a new OAuth claims-based Advanced Authentication Generic Class for integrating Access Manager with Advanced Authentication. This mechanism provides more secure and trusted communication.

For more information, see NetIQ Advanced Authentication in the NetIQ Access Manager 4.4 Administration Guide.

1.1.11 WebSocket Support

Access Manager 4.4 supports WebSocket. The WebSocket protocol is an extension to the HTTP 1.1 protocol to enable two-way communication between a client and a server. Access Manager automatically enables a WebSocket connection when it detects an application that supports WebSocket. Access Manager 4.4 upgrades Apache 2.2 to 2.4 to support WebSocket.

For more information, see WebSocket Support in the NetIQ Access Manager 4.4 Administration Guide.

1.1.12 Enhancement in Capability to Select Identity Providers for Authentication

Users can now authenticate by using an identity provider contract from a list of identity providers and save the selection.

For more information, see Configuring IDP Select Class in the NetIQ Access Manager 4.4 Administration Guide.

1.1.13 Risk-Based Authentication Enhancements

This release includes the following risk-based authentication enhancements:

- **Geo-Velocity Tracker Rule**: Using this rule, you can check user's current time and location compared to the time and location of the last login. The last login details are taken from the history database. If the time between the last successful login and the current login attempt is less than the shortest possible travel time, you can configure the following actions:
  - Prompt for an additional authentication
  - Deny access

  This helps in preventing man-in-the-middle, brute force, and DDoS attacks. For more information, see Risk-based Authentication in the NetIQ Access Manager 4.4 Administration Guide.

- **Ability to Select Multiple Methods and Classes for Additional Authentication**: In a risk policy, now you can select multiple classes and methods to configure additional authentication.
  For more information, see Configuring Risk Levels in the NetIQ Access Manager 4.4 Administration Guide.

- **Enhancements in the Device Fingerprint Rule**: The device fingerprint now supports the following two new capabilities:
  - Ask user consent before registering the device.
  - Send email notification when a user tries to access from an unknown device.

  For more information, see Device Fingerprinting in the NetIQ Access Manager 4.4 Administration Guide.
1.1.14 Email Notifications For an Unrecognized Login Attempt

In a risk-based authentication, now you can configure to send emails to users’ registered email IDs when a user logs in from an unknown device for the first time. You can use this feature through the Device Fingerprint rule.

For information about how to configure the email server, see Email Server Configuration in the NetIQ Access Manager 4.4 Administration Guide. For information about the Device Fingerprint rule, see Device Fingerprinting in the NetIQ Access Manager 4.4 Administration Guide.

1.1.15 Support for Restricting the X.509 Authentication to a Specific Certificate Authority

Access Manager now enables you to configure mutual authentication to succeed only when a user submits an X.509 user certificate issued by the specified CA. This restriction does not restrict the certificates available on the client side. This restriction is applicable only during processing or validating certificates.

For more information, see Restricting the X.509 Authentication to a Specific Certificate Authority in the NetIQ Access Manager 4.4 Administration Guide.

1.1.16 Support for Deleting Exported Code Promotion Configuration

Access Manager now supports deleting an exported configuration in the Code Promotion page by using Delete.

1.1.17 User Attributes Retrieval from REST Web Servers

You can now retrieve an attribute from a REST Web service.

For creating data source, attribute source, and virtual attribute for REST Web Server, see User Attribute Retrieval and Transformation in the NetIQ Access Manager 4.4 Administration Guide.

1.1.18 Support for Adding LDAP Replicas in the LDAP Data Source for Virtual Attribute

When you add a datasource for LDAP, you can now specify multiple search context and LDAP replicas. The Administration Console interface is enhanced to support this functionality.

For more information about the data source for LDAP, see Creating a Data Source in the NetIQ Access Manager 4.4 Administration Guide.

1.2 Operating System Upgrade

In addition to the existing supported platforms, this release supports installation of Access Manager components on RHEL 7.4.

NOTE: For more information about system requirements, see System Requirements in the NetIQ Access Manager 4.4 Installation and Upgrade Guide.
1.3 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 9.0.3.1
- Java 1.8.0_141
- Apache 2.4.27
- OpenSSL 1.0.2k
- Tomcat 8.0.45
- iManager 3.0.3.2

1.4 Browser Support

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

- Edge
- Internet Explorer
- Chrome
- Firefox
- Safari

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

- Chrome 60.0.3112.101
- Firefox 54.0.1
- Internet Explorer 11.0.9600.18738 Update Versions 11.0.44 (KB4025252)
- Edge 38.14393.0.0/ EdgeHTML 14.14393

1.5 Software Fixes

Access Manager 4.4 includes software fixes for the following components:

- Section 1.5.1, “Administration Console,” on page 9
- Section 1.5.2, “Identity Server,” on page 10
- Section 1.5.3, “Access Gateway,” on page 11

1.5.1 Administration Console

The following issues are fixed in Administration Console:

- Section 1.5.1.1, “Administration Console Randomly Deletes Certificate Trust Store Objects,” on page 9
- Section 1.5.1.2, “Cannot Perform Any Action on the Conditions Specified for an Authorization Policy,” on page 10

1.5.1.1 Administration Console Randomly Deletes Certificate Trust Store Objects

The Identity Server cluster is not displayed in Administration Console because the certificates get deleted from the trust store. Hence, you must re-configure the Identity Server cluster. (Bug 1051781)
1.5.2 Identity Server

The following issues are fixed in Identity Server:

- Section 1.5.2.1, “Login Page Does Not Render Properly After a Kerberos Authentication Method Failure,” on page 10
- Section 1.5.2.2, “User Provisioning Fails with Multiple Replicas of the User Store,” on page 10
- Section 1.5.2.3, “Opening a Word File Through Internet Explorer Displays the HTTP 401 Unauthorized Error Message,” on page 10
- Section 1.5.2.4, “Cannot Use Virtual Attributes in OAuth Attribute Set,” on page 10
- Section 1.5.2.5, “Cannot Configure HTTP Redirect URIs for OAuth Clients,” on page 10

1.5.2.1 Login Page Does Not Render Properly After a Kerberos Authentication Method Failure

**Issue:** The fallback login page is not rendered properly after a Kerberos method authentication failure. (Bug 1003919)

**Fix:** The fallback login page now renders properly and retains customization as well. You no longer need to follow the configuration steps mentioned in TID (https://www.netiq.com/support/kb/doc.php?id=7015049).

1.5.2.2 User Provisioning Fails with Multiple Replicas of the User Store

When Access Manager acts as a service provider, user provisioning fails to update user attributes if you have specified the user store that has multiple replicas. (Bug 1011790)

1.5.2.3 Opening a Word File Through Internet Explorer Displays the HTTP 401 Unauthorized Error Message

When you set the global setting NAGGlobalOptions AllowMSWebDavMiniRedir=on for accessing MS Office documents, Internet Explorer does not launch the document post authentication. Users can edit the document after authentication, but Access Manager will not open the document in read mode within a browser. (Bug 907592)

1.5.2.4 Cannot Use Virtual Attributes in OAuth Attribute Set

When specifying user attributes for the OAuth scope, you cannot add virtual attributes in the attribute set. (Bug 1010987)

1.5.2.5 Cannot Configure HTTP Redirect URIs for OAuth Clients

**Issue:** When you register a client application by selecting Client Type as Web Based, Access Manager does not allow HTTP URI in Redirect URIs. (Bug 1035206)

**Fix:** With this release, Access Manager allows registering web-based client applications with either HTTP or HTTPS redirect URIs. It is recommended to use HTTPS for the redirect URI.
1.5.3 Access Gateway

The following issues are fixed in Access Gateway:

- Section 1.5.3.1, “Unable to Set the Advanced Option noURLNormalize=on at Proxy Level,” on page 11
- Section 1.5.3.2, “Clustered Access Gateway Does Not Restore Postparked Data for Web Server After Authentication,” on page 11

1.5.3.1 Unable to Set the Advanced Option noURLNormalize=on at Proxy Level

**Issue:** You can set `noURLNormalize=on` at global level only when you set `NAGGlobalOptions noURLNormalize=on`. This disables URL normalization for all proxy services. (Bug 897709)

**Fix:** A new option is added at the proxy level, `NAGHostOptions noURLNormalize=on/off`. The priority level is as follows:

1. Path
2. Proxy
3. Global

For more information, see Configuring Advanced Options for a Domain-Based and Path-Based Multi-Homing Proxy Service in the NetIQ Access Manager 4.4 Administration Guide.

1.5.3.2 Clustered Access Gateway Does Not Restore Postparked Data for Web Server After Authentication

In an Access Gateway cluster, if the data is parked in one of the Access Gateways and ESP requests are sent on another Access Gateway, then after authentication data is not restored. (Bug 1036669)

2 Installing or Upgrading

After purchasing Access Manager 4.4, log in to the NetIQ Downloads (http://dl.netiq.com/) page and follow the link that allows you to download the software.

**IMPORTANT:** Windows packages KB2919442 and KB2919355 must be installed before installing or upgrading Access Gateway Service on Windows Server 2012. These packages must be installed in the same sequence. You can verify whether these packages are installed by using the following commands:

- `dism /online /get-packages | findstr KB2919442`
- `dism /online /get-packages | findstr KB2919355`

If these packages are installed, you will get a confirmation message. If the packages are not installed, you will not receive any response.

**NOTE:** In this release of Access manager there were no changes made to Analytics Server. Access Manager and Access Manager Appliance can be used with Analytics Server 4.3.2. Hence, you can find the Analytics Server 4.3.2 binaries with other Access Manager 4.4 components.

The following files are available:
Table 1  Files Available for Access Manager 4.4

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM_44_AccessManagerService_Linux64.tar.gz</td>
<td>Contains Identity Server and Administration Console .tar file for Linux.</td>
</tr>
<tr>
<td>AM_44_AccessManagerService_Win64.exe</td>
<td>Contains Identity Server and Administration Console .exe file for Windows Server.</td>
</tr>
<tr>
<td>AM_44_AccessGatewayService_Win64.exe</td>
<td>Contains Access Gateway Service .exe file for Windows Server.</td>
</tr>
<tr>
<td>AM_44_AccessGatewayService_Linux64.tar.gz</td>
<td>Contains Access Gateway Service .tar file for Linux.</td>
</tr>
<tr>
<td>AM_43_SP2_AnalyticsServerAppliance.iso</td>
<td>Contains Analytics Server Appliance .iso file.</td>
</tr>
<tr>
<td>AM_43_SP2_AnalyticsServerAppliance.tar.gz</td>
<td>Contains Analytics Server Appliance .tar file.</td>
</tr>
</tbody>
</table>

The b2cFramework-1.0.zip file contains the B2C Framework login pages. You can download this file from the Developer Documentation page.

For information about the upgrade paths, see Section 4, “Supported Upgrade Paths,” on page 12. For more information about installing and upgrading, see the NetIQ Access Manager 4.4 Installation and Upgrade Guide.

3  Verifying Version Number After Upgrading to 4.4

After upgrading to Access Manager 4.4, verify that the version number of the component is indicated as 4.4.0.0-337. To verify the version number, perform the following steps:

1  In Administration Console Dashboard, click Troubleshooting > Version.
2  Verify that the Version field lists 4.4.0.0-337.

4  Supported Upgrade Paths

To upgrade to Access Manager 4.4, you need to be on one of the following versions of Access Manager:

- 4.2 Service Pack 2
- 4.2 Service Pack 3 or 4.2 Service Pack 3 Hotfix 1
- 4.2 Service Pack 4
- 4.3 Service Pack 1 or 4.3 Service Pack 1 Hotfix 1
- 4.3 Service Pack 2
**IMPORTANT:** If you are using SQL database and you are upgrading to Access Manager 4.4, you must run a utility to re-factor the database. This is to ensure that Access Manager and its associated products use the same naming convention. For more information about this utility and how to run it, see Refactoring SQL Database in the NetIQ Access Manager 4.4 Installation and Upgrade Guide.

For more information about upgrading Access Manager, see “Upgrading Access Manager” in the NetIQ Access Manager 4.4 Installation and Upgrade Guide.

## 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 (http://www.netiq.com/support).

- Section 5.1, “(Windows) The Import Application from File Option in the Applications Page Does Not Work,” on page 14
- Section 5.2, “(RHEL 6.9) Identity Server Is Restarted When a User Tries to Log In to User Portal Through an iOS Device,” on page 14
- Section 5.3, “Applications Page: Remote Namespace in Attribute Mappings Is Not Included in the Download,” on page 14
- Section 5.5, “Identity Server Install Log File Includes False Entries for Error Messages,” on page 15
- Section 5.6, “Accessing a Policy that is Created Using REST API May Return Null Pointer Exception,” on page 15
- Section 5.7, “Issue in Connecting to Self-Signed Certificates from iOS 10.3.1,” on page 15
- Section 5.8, “False Errors Are Recorded When a Delegated Administrator Accesses Administration Console Dashboard,” on page 16
- Section 5.9, “(RHEL) Apache Fails to Start After Upgrading or a Fresh Install of Access Manager 4.4,” on page 16
- Section 5.11, “iOS 10.3 or later Does Not Trust Access Manager CA Root Certificate,” on page 17
- Section 5.12, “Canceling a Social Authentication User Registration Process Results in Error,” on page 17
- Section 5.13, “Modifications Made in a Basic SSO Application’s Description Using Internet Explorer Are Not Shown in the Application UI,” on page 17
- Section 5.14, “Issue in Creating and Editing a Basic SSO Application in the Application UI on Internet Explorer,” on page 17
- Section 5.15, “Saving a New SAML Application With Two Signing Certificates Adds Only One Certificate to the Trust Store,” on page 18
- Section 5.16, “SAML Application Does Not Get Saved If a String Type Setting Has Multi-Part Query String Data,” on page 18
- Section 5.17, “Checks for Duplicate Values for Entity ID and Unique ID in the Applications Page Does Not Consider Case,” on page 18
5.1 (Windows) The Import Application from File Option in the Applications Page Does Not Work

**Issue:** This issue may occur when you run Administration Console on Windows 7 and Windows 10, 64-bit. Trying to import a connector from the downloaded ZIP file using the latest Chrome browser may not work. *(Bug 1053094)*

**Workaround:** Use any other browser instead of Chrome.

5.2 (RHEL 6.9) Identity Server Is Restarted When a User Tries to Log In to User Portal Through an iOS Device

**Issue:** This issue occurs when Identity Server is installed on RHEL 6.9 on ESXi 6.5 with Virtual Machine version 13. If MobileAccess is enabled and an end user tries to log in to User Portal through an iOS device, the RHEL 6.9 server restarts. *(Bug 1049504)*

**Workaround:** Upgrade the Virtual Machine version 13 to the latest patches.

5.3 Applications Page: Remote Namespace in Attribute Mappings Is Not Included in the Download

**Issues:** This issue occurs when you create a SAML application using the Applications page and modify it to use a local attribute set. The local attribute set contains an attribute mapping that has a remote namespace configured. If you download the application to a connector, the downloaded connector file does not contain the namespace configuration. *(Bug 1052323)*

**Workaround:** When importing the connector using the downloaded file, restore Remote Namespace settings by using the Shared Settings page. *(Devices > Identity Server > Shared Settings)*

5.4 Single Sign-On to Advanced Authentication Enrollment Page Does Not Work

**Issue:** If you log in using Social authentication, X.509 digital certificates or Kerberos methods, single sign-on to Advanced Authentication enrollment page will not work because the identity injection policy needs password for injection and password is not available with these authentication methods. *(Bug 1051498)*

**Workaround:** If the user store is eDirectory, you can configure passwordfetch class to fetch the password. When the password is fetched, it can be used in the identity injection policy.
5.5 Identity Server Install Log File Includes False Entries for Error Messages

**Issue:** During Identity Server installation, all installer messages indicate everything is fine. Identity Server gets installed successfully. However, the log file might include entries for false issues. (Bug 1041712)

**Example of false issues:**

Loader Failed:for ebassl_cli, error ebassl_cli: cannot open shared object file: No such file or directory, errno 2
Loader Failed:for spmclnt, error spmclnt: cannot open shared object file: No such file or directory, errno 2
Tree=null, IPAddress=X.X.X.X, Port=0, ServerDN=null, User=cn=namadmin,o=novell
Error: -5984
at com.novell.security.japi.pki.NPKIAPI createContext (NPKIAPI.java:1769)
at com.novell.security.japi.pki.NPKIAPI.initialize(NPKIAPI.java:6004)

You can ignore these entries.

5.6 Accessing a Policy that is Created Using REST API May Return Null Pointer Exception

**Issue:** This issue might occur when you create a policy using the addPolicy() (POST) REST API while keeping Administration Console open. Clicking this policy in the Administration Console Dashboard may return a blank page showing Null Pointer Exception. (Bug 1043265)

**Workaround:** Ensure the following:

- While creating a policy using REST API, you are not logged in to Administration Console.
- If you need to be logged in to Administration Console while using REST API, use the incognito mode of the browser.
- If you were logged in to Administration Console while using REST API, then log out, clear your browser’s cache, and re-login to access the policy.

5.7 Issue in Connecting to Self-Signed Certificates from iOS 10.3.1

**Issues:** A certificate validation issue exists in iOS 10.3. This issue may cause difficulty connecting to self-signed certificates in Access Manager. (Bug 1051589)

**Workaround:** Perform the following actions:

1. Upgrade iOS to version 10.3.2.
2. Import self-signed certificate.
3. Open Settings.
4. Navigate to General > About.
5. Select Certificate Trust Settings.

Each root that has been installed through a profile is listed under Enable Full Trust For Root Certificates. You can disable or enable the roots as required.
5.8 False Errors Are Recorded When a Delegated Administrator Accesses Administration Console Dashboard

**Issue:** Whenever a delegated administrator tries to access Dashboard or any menu on Dashboard, false exceptions and SEVERE level errors are recorded into Administration Console catalina.out. (Bug 1049712)

Ignore these errors. The following is a snippet of `catalina.out` containing an example of such errors:

```text
INFO: Delegated users denied
Jul 20, 2017 8:24:07 AM com.microfocus.amapi.v1.resources.IDPClustersAPI
getIDPClusters
INFO: Forbidden access
com.microfocus.amsvc.v1.sdk.client.ApiException:
{"response":{"code":"FORBIDDEN","detail":"Delegated users denied"}}
SEVERE: Forbidden access
com.microfocus.amsvc.v1.sdk.client.ApiException:
{"response":{"code":"FORBIDDEN","detail":"Delegated users denied"}}
```

5.9 (RHEL) Apache Fails to Start After Upgrading or a Fresh Install of Access Manager 4.4

**Issue:** This issue occurs when more than 60 proxy services are configured. RHEL has 128 semaphore arrays by default, which is inadequate for more than 60 proxy services. Apache 2.4 requires a semaphore array for each proxy service. (Bug 1054426)

**Workaround:** To resolve this issue, you must increase the number of semaphore arrays depending on the number of proxy services you are going to use. Perform the following steps to increase the number of semaphore arrays to the recommended value:

1. Open the `/etc/sysctl.conf` file.
2. Add `kernel.sem = 250 256000 100 1024`  
   This creates the following:
   - Maximum number of arrays = 1024 (number of proxy services x 2)
   - Maximum semaphores per array = 250
   - Maximum semaphores system wide = 256000 (Maximum number of arrays x Maximum semaphores per array)
   - Maximum ops per semop call = 100
3. Use the `sysctl -p` command to update the changes.
4. Start Apache.

5.10 Authorization Server Fails to Issue the Access Token and Displays Invalid Code Error Even When the Authorization Code Is Valid

**Issue:** This issue occurs in the Identity server (authorization server) cluster environment. When an authorization code is issued from one node and that goes down, requesting access token using this code from a different node of the cluster results in failure of the request. This happens because the authorization code is stored in the Identity Server’s system memory and it is not shared with other nodes in the cluster. (Bug 1054355)
Workaround: To resolve this issue, you must ensure that all the nodes of Identity Server cluster are functional.

5.11 iOS 10.3 or later Does Not Trust Access Manager CA Root Certificate

Issue: iOS 10.3 or later does not trust the default CA created in Access Manager. Therefore, default certificates for SSL cannot be trusted in Apps such as MobileAccess or the SDK. (Bug 1055333)

Workaround: Replace the SSL certificates with a certificate signed by another CA that can be trusted or from an already trusted CA.

5.12 Canceling a Social Authentication User Registration Process Results in Error

Issue: In the social registration process, the Cancel button redirects the user to an error page. In this case, a user needs to go to the login page manually for re-registration. (Bug 1049174)

Workaround: None.

5.13 Modifications Made in a Basic SSO Application’s Description Using Internet Explorer Are Not Shown in the Application UI

Issue: This issue occurs if you create a new Basic SSO application on the Applications UI using the Chrome or Firefox browser (not Internet Explorer). Access the Applications UI on Internet Explorer and edit the description of the previously created Basic SSO application, and save the changes. After saving, the changes are not reflected. (Bug 1055559)

Workaround: Perform the following steps:

1. Open Internet Explorer.
2. Go to Internet Options > General > Browsing history > Settings.
3. Under the Check for newer versions of stored pages option, select Every time I visit the webpage.

5.14 Issue in Creating and Editing a Basic SSO Application in the Application UI on Internet Explorer

Issue: This issue occurs when you use Internet Explorer to access Administration Console. If you create a new Basic SSO application using Internet Explorer, the details are not saved properly. Editing a Basic SSO also does not work. (Bug 1055570)

Workaround: Perform the following steps:

1. Open Internet Explorer.
2. Go to Internet Options > General > Browsing history > Settings.
3. Under the Check for newer versions of stored pages option, select Every time I visit the webpage.
5.15 Saving a New SAML Application With Two Signing Certificates Adds Only One Certificate to the Trust Store

**Issue:** In the Applications page, when saving a new SAML application with two signing certificates, only one certificate is added to the Trusted Roots store. (Bug 1055774)

**Workaround:** Import the second certificate from the Administration Console dashboard by clicking Certificates > Trusted Roots > Import.

5.16 SAML Application Does Not Get Saved If a String Type Setting Has Multi-Part Query String Data

**Issue:** In the Applications page, configuring a String type setting of a SAML 2.0 application with a URL that includes a multi-part query string (for example: https://1.2.3.com?a=b&c=d) fails and endless spinner is displayed. (Bug 1054778)

**Workaround:** Use Connector Studio to change the setting type from String to URL.

5.17 Checks for Duplicate Values for Entity ID and Unique ID in the Applications Page Does Not Consider Case

**Issue:** The checks made for duplicate Entity ID and Unique ID is case-insensitive in the Applications page. Whereas the it is case-sensitive in the SAML 2.0 configuration page. (Bug 1053914)

**Workaround:** Specify values for Unique ID and Entity ID that are unique in characters and case.

5.18 Importing a Connector Does Not Process Attributes With a Remote Namespace

**Issue:** In the Applications page, when importing or exporting a SAML connector, the Remote Namespace and Remote Format for attribute mappings are not preserved. (Bug 1052312)

**Workaround:** After importing a connector, edit the attribute set using the Shared Settings page to restore Remote Namespace and Remote Format configuration.

5.19 Downloading or Importing a SAML Application Does Not Preserve Unique ID Setting of Service Provider

**Issue:** In the Applications page, downloading or importing a SAML application does not preserve the Unique ID setting. (Bug 1044750)

**Workaround:** When importing the connector, specify a Unique ID if an existing service provider with the same provider ID already exists on the Identity Server cluster.

5.20 Administration Console Upgrade Fails

**Issue:** Administration Console upgrade fails if the system host entry in Linux is incorrect. You get the following error message:

```
Upgrading the Novell Access Manager Configuration Store:
sed: can't read /tmp/nids_inst_bind_rest.ldif: No such file or directory
```

sed: can't read /tmp/nids_inst_bind_rest.ldif: No such file or directory
**Workaround**: To workaround this issue, perform the steps mentioned in Administration Console Upgrade Fails in the NetIQ Access Manager 4.4 Installation and Upgrade Guide or TID 7021289 (https://www.netiq.com/support/kb/doc.php?id=7021289).

### 5.21 Issue with the reCAPTCHA Threshold Value

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

**Workaround**: To workaround this issue, set the threshold value to zero.

### 5.22 Some Operating System Commands May Fail After Upgrading Administration Console on the SLES 12 Platform

After upgrading Administration Console on a SLES 12 platform, the curl and the zypper commands fail with the DEFAULT_SUSE error. For more information about this issue and how to resolve it, see TID 7021958 (https://www.novell.com/support/kb/doc.php?id=7021958) and TID 7022106 (https://www.novell.com/support/kb/doc.php?id=7022106).

### 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. 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.

### 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/.

Copyright © 2017 NetIQ Corporation. All Rights Reserved.