NetIQ Access Manager Appliance 3.2 Service Pack 2 IR3

April, 2014

NetIQ Access Manager Appliance 3.2 Service Pack 2 IR3 resolves several previous issues.

Many of these improvements were 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 that our products meet all your needs. You can post feedback in the Access Manager forum on Qmunity, our online community that also includes product information, blogs, and links to helpful resources.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 3.2 Service Pack 2 Readme and Access Manager Appliance 3.2 Service Pack 2 IR1 Readme and Access Manager Appliance 3.2 Service Pack 2 IR2 Readme

The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Access Manager NetIQ Documentation page. To download this product, see the NetIQ Access Manager Products Web site.

1 What’s New?

The following sections outline the issues resolved in this release:

1.1 Software Fixes for the Identity Server

The following are the fixes introduced in this release for the Identity Server:

1.1.1 Active Directory Users with an Expired Password Gets Redirected to Password Management URI

Issue: When an Active Directory user with an expired password logs in to an authentication contract with a Password Expiration servlet configured, the user is redirected to the password management URI. If the Password Management portal is protected by Access Manager, the user is prompted again for authentication and is not permitted to login as the user password has expired. (`Bug 847898`)

Fix: It is now possible for an user with an expired password to access the protected Password Management Portal.

Execute the following steps:

1. Add the following property for the method used by contract with Password Expiration servlet:

   `ExpiredCheck=true`

2. Add the following property for the method used by contract that protects the Password Management portal:

   `ExpiredCheck=true`

   `ExpireCheck=true`

3. On the Identity Server, locate the `/opt/novell/nam/idp/webapps/nidp/WEB-INF/classes/nidpconfig.properties` file.

   Add `AUTHENTICATE_WITH_EXPIRED_PASSWORD` property to the file.

   For example:

   `AUTHENTICATE_WITH_EXPIRED_PASSWORD=ad/name/password/uri`

4. Repeat Step 3 for all the Identity Server cluster members.
5. Restart the Identity Server for the changes to take effect.

1.1.2 The User Is not Redirected to the TARGET URL After Authentication Against Intersite URL Contract

Issue: After authenticating on the Identity Server, if the user attempts authentication with the contract specified in the Intersite URL, the user is not redirected to the idpsend TARGET. (`Bug 863343`)

Fix: After authenticating to the Intersite URL contract, the user is redirected to the idpsend TARGET.

1.1.3 Validation Check Fails for Audience Restriction Condition When Two SAML 2.0 Service Providers Are Configured With the Same Access Manager Host

Issue: If you have configured two SAML 2.0 service providers with the same Access Manager host, validation check fails for the Audience Restriction condition. (`Bug 864219`)

Fix: Under SAML 2.0 Service Provider properties, a new property is added to exclude audience information from a SAML 2.0 assertion.

Property Name: SAML2_AVOID_AUDIENCE_RESTRICTION

Value: True / False

If this property value is set to True, the audience information is excluded from the SAML 2.0 assertion.

1.1.4 Single Sign-on to SAML 2.0 Service Provider Fails When SAML 2.0 Assertion Includes LDAP Attributes With Binary Syntax

Issue: If the SAML 2.0 assertion includes LDAP attributes with binary syntax (stream) in eDirectory, single sign-on to SAML 2.0 service provider fails. (`Bug 864219`)

Fix: With this fix, binary values /XML incompatible values can be sent with a SAML 2.0 assertion with datatype as `xs:base64Binary`.

1.2 Software Fixes for the Access Gateway Appliance

The following are the fixes introduced in this release for the Access Gateway Service and the Access Gateway Appliance:

1.2.1 Login Fails if the Identity Injection Policy Contains Special Characters in Attributes

Issue: If the Identity Injection policy contains attributes that includes special characters, logging to an application fails. (`Bug 865649`)

Fix: Logging is successful even if the Identity Injection policy has attributes with special characters.

1.2.2 Form Fill Adds an Extra String if the InPlaceSilentPolicyDoesSubmit Advanced Option Is Enabled

Issue: When the `InPlaceSilentPolicyDoesSubmit` global option is enabled on the Access Gateway, an extra string is added and this leads to credential check failure and an unending loop. (`Bug 861631`)

Fix: Fixed the issue where an extra string is added when the `InPlaceSilentPolicyDoesSubmit` advanced option is enabled.

1.2.3 Extra Back Slash Added to Web Server Requests Leads to a 404 Error

Issue: The Access Gateway appends Web Server requests with an extra backslash (\) character when the requests have query strings. (`Bug 860236`)

Fix: Fixed the issue where the Access Gateway adds an extra backslash (\) character when the requests have query strings.

1.2.4 TCP Listener Binding Fails if More Than a Hundred IP Addresses Are Added to the Reverse Proxy List

Issue: If you attempt to add more than a hundred IP addresses to the **Adapter List** in network settings and then restart Apache after updating Access Gateway Service, it fails with an error. (`Bug 860233`)

Fix: There is no limitation on the number of IP addresses that can be added to the **Reverse Proxy** list.

1.2.5 The Access Gateway Service Evaluates Authorization Policy Before Redirecting to HTTPS

Issue: On an SSL-enabled resource, the Access Gateway Service evaluates authorization policy before redirecting to HTTPS. (`Bug 843622`)

Fix: The Access Gateway now redirects the URL from HTTP to HTTPS before evaluating any policies.

1.3 Software Fixes for the Administration Console

The following are the fixes introduced in this release for the Administration Console:

1.3.1 Access Gateway Updates Remain in Pending State After Audit Configuration is Removed

Issue: When audit configuration is changed through the Administration Console, the updates remain in pending state. (`Bug 863762`)

Fix: The configuration changes are saved without any errors.

1.3.2 Random Exception Messages While Accessing the Access Gateway or the Policy Tab

Issue: A random, connecting to the datastore message error is displayed while accessing the Access Gateway or the Policy tab. (`Bug 855844`)

Fix: No errors are displayed while accessing the Access Gateway or the Policy tab.

1.3.3 CPU Utilization Graph Shows a Zero Value for Multi-Core CPU Access Gateway Devices

Issue: The CPU utilization graph in the Administration Console shows a zero value for multi-core CPU Access Gateway devices. (`Bug 862772`)

Fix: The CPU utilization graph displays correct CPU utilization statistics

2 Installing or Upgrading Access Manager

NOTE: Ensure that you are currently on one of these following version before upgrading to Access Manager 3.2 Service Pack 2 IR3:

- ❒ Access Manager 3.2 Service Pack 2
- ❒ Access Manager 3.2 Service Pack 2 Hotfix 1
- ❒ Access Manager 3.2 Service Pack 2 Hotfix 2

For installation details, see the NetIQ Access Manager Appliance 3.2 Service Pack 2 IR2 Installation Guide.

To upgrade Access Manager Appliance 3.2 Service Pack 2 IR2, download the `AM_32_SP2_IR3.zip`, that contains the Access manager appliance Patch Tool and the patch file using the following steps:

1. Go to NetIQ Downloads page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_32_SP2_IR3.zip` in the search box and download the Hotfix file.
4. Upgrade using the procedure described in Upgrading Access Manager Appliance 3.2 SP2 Using the Patch Process.

2.1 Verifying Version Numbers Before Upgrading

It is important to verify the version number of existing Access Manager components before you upgrade to 3.2 Service Pack 2 IR3. This ensures that you have the correct version of files on your system.

Refer the following table to determine if you have the correct version installed:

Access Manager Version	Value in the Version field (Access Manager > Auditing > Troubleshooting> Version)
Access Manager 3.2 Service Pack 2	3.2.2-77
Access Manager 3.2 Service Pack 2 IR1	3.2.2-77 + IR1-107
Access Manager 3.2 Service Pack 2 IR2	3.2.2-77 + IR2-117

2.2 Verifying Version Numbers After Upgrading

It is important to verify the version number of existing Access Manager components after upgrading to 3.2 Service Pack 2 IR3. This ensures that you have the correct version of files on your system.

Refer the following table to determine if you have the correct version installed:

Access Manager Version	Value in the Version field (Access Manager > Auditing > Troubleshooting> Version)
Access Manager 3.2 Service Pack 2 and then upgrade to IR3	3.2.2-77 + IR3+122
Access Manager 3.2 Service Pack 2 IR1and then upgrade to IR3	3.2.2-77 + IR1-107, IR3-122
Access Manager 3.2 Service Pack 2 IR2 and then upgrade to IR3	3.2.2-77 + IR1-107, IR2-117, IR3-122

3 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)

3.1 Kerberos Single Sign-On Fails On Usernames With Extended Character Set

Issue: Logging into Access Manager using Kerberos authentication with a username that has extended characters, (For example: Irish Fada or Umlauts) throws an error. (`Bug 859487`)

3.2 Additional DNS Name List Does Not Accept a Host Name in the Rewriter Profile

Issue: Adding a host name to the Access Gateway Rewriter Profile leads to an `IP Address or DNS is invalid` error. (`Bug 868388`)

3.3 Access Gateway Statistics Report High Number of Requests to Origin Server During Load Testing

Issue: The Access Gateway statistics page indicate a large count for the `Current connections are to origin server` field during high load.(`Bug 873699`)

3.4 Form Fill Not Matching Page When Autosubmit is Enabled

Issue: If you have configured a form fill policy to autosubmit a form that was developed using Dojo code, autosubmit does not work.(`Bug 874965`)

3.5 Cannot Proxy SAML 2.0 AuthnRequest With an External Contract to a Remote SAML 2.0 Identity Server

Issue: Differences in the `AuthnContextDeclRef` statement of the service provider `AuthnRequest`, leads to failure in processing the assertion request by the Identity Provider. (`Bug 869990`)

3.6 Access Gateway Corrupts or Concatenates SAP Application Server Cookies Sent by Browser Client

Issue: When Access Gateway protects a SAP application server, and a POST request is issued it corrupts the application cookie resulting in a HTTP 500 error.(`Bug 872117`)

3.7 Rapid Redirections Between the ESP and an Application in Active Directory Domain

Issue: If the user has logged into an Active Directory domain and is attempting to access an application using Internet Explorer 10, there are rapid redirections between the ESP and the application. (`Bug 874568`)

Workaround: To workaround this issue, you an either add the domain to Internet Explorer Trusted Site list Or, use a Mozilla Firefox or Chrome browser to access the application.

3.8 Authentication Issues if the Access Gateway is Configured With the Behind Third-Party SSL Terminator Option Enabled

Issue: When Access Gateway is configured with the **Behind Third-Party SSL Terminator** option enabled, users are not authenticated due to configuration errors in NAGCookieBroker. (`Bug 857620`)

4 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 our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

[Return to Top]

5 Legal Notice

documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/ (http://www.netiq.com/company/legal/).

[Return to Top]