Access Manager 4.0 Readme

November 2013

Access Manager 4.0 includes new features, improves usability, and 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 our products meet all your needs. You can post feedback in the Access Manager forum on Qmunity (http://community.netiq.com/forums/30.aspx), our community Web site that also includes product notifications, blogs, and product user groups.

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

For more information about this release and for the latest release notes, see the Documentation Web site. To download this product, see the Product Upgrade (http://www.netiq.com/products) Web site.

1 What’s New?

Access Manager 4.0 provides the following key features and functions as well as issues resolved in this release:

NOTE

- Support for CardSpace and J2EE Agents have been removed from Access Manager 4.0 onwards.
- Starting from Access Manager 4.0 release, there will be no enhancements or platform updates for the SSL VPN component. The component is however available and fully supported in Access Manager 4.0. The Administrative Console Dashboard labels the component as "Deprecated" to

convey this information. Deprecated means that SSL VPN will be removed from the subsequent version of Access Manager and you may consider other alternative solutions similar to SSL VPN.

1.1 Operating System Support

This version adds support to the following platforms, in addition to the platforms introduced in the 3.2 SP2 release:

- RHEL 6.4 64-bit
- SLES 11 SP3 64-bit

1.2 Updates for Dependent Components

This release provides the following updated components:

- iManager 2.7.7
- Java 1.7.0_25
- Tomcat 7-7.0.42
- eDirectory 8.8.8

1.3 Support for Authorization Policies Based on IPv6 Addresses

Access Manager supports the forwarding of client IPv6 addresses in the X-Forwarded-For HTTP header. This support is provided by taking advantage of the IPv4-IPv6 dual stack support in the L4 switch. The option to bind IPv6 addresses to the Access Manager components is not available. For more information about IPv6 support, see "Setting up L4 Switch for IPv6 Support" in the *NetIQ Access Manager 4.0 Setup Guide* and "X-Forwarded-For IP Condition " in the *NetIQ Access Manager 4.0 Policy Guide*.

1.4 Wizard Based Configuration for Office 365, Google Applications, and Salesforce.com

This release introduces an easy way to configure cloud service providers such as Office 365, Google Applications, and Salesforce.com. You can access this wizard in SAML 2.0 Service Provider configuration. Integration of these providers is simpler because most of the settings are pre-configured. For more information about creating trusted service providers for Google Applications, Office 365, and Salesforce.com see "Creating a Trusted Service Provider for SAML 2.0 ", and for more information on pre-configured metadata, see "Sample Configurations" in the *NetIQ Access Manager 4.0 Identity Server Guide*.

1.5 Supports WS-Trust Secure Token Service

Access Manager addresses the need for securing Web services in SOAP world. This release provides security tokens to Web services using standard WS-Trust 1.3 and WS-Trust 1.4 protocols. You can now write smart clients that can communicate securely with WS-Trust enabled Web services. You can also validate the SAML based tokens, delegate or impersonate users at trusted Web service providers using SOAP based WS-Trust protocol. For more information about WS-Trust STS, see "WS-Trust Security Token Service" in the *NetIQ Access Manager 4.0 Identity Server Guide*.

1.6 Monitoring Access Manager using Simple Network Management Protocol

This release introduces support for Simple Network Management Protocol(SNMP). Using this protocol in combination with any Network Monitoring System (NMS) helps gather statistics from Administration Console for the purpose of monitoring. For more information about this feature, see "Monitoring Access Manager By Using Simple Network Management Protocol" in the *NetIQ Access Manager 4.0 Administration Console Guide*.

1.7 NetIQ Advanced Authentication Framework Support

Access Manager now supports advanced/multi-factor authentication add-on. Following are the supported authentication methods for Access Manager AA plugin:

- OATH OTP authentication
- Flash drive authentication
- Universal Card authentication

For more information about this authentication framework, see NetIQ Advanced Authentication Framework documentation.

1.8 Google Authenticator

Access Manager supports two factor authentication using Google Authenticator One Time Password (OTP). Google Authenticator is an open source implementation of HMAC Based One-time Password (HOTP) and the Time-based One Time Password (TOTP). Access Manager supports shared secret store as the only option for storing Google authentication secret seed value. For more information about integrating Google Authenticator, see "Configuring Google Authenticator for Two-Factor Authentication" in the *NetIQ Access Manager 4.0 Identity Server Guide*.

For more information about limitations of 4.0 features listed above, see the respective Access Manager guides mentioned against each feature in "What's New?" on page 1.

2 Installing or Upgrading

After you purchased Access Manager 4.0, log in to the Novell Downloads page and follow the link that allows you to download the software. The following files are available:

Table 1 *Files Available for Access Manager 4.0.*

Filename	Description
AM_40_AccessManagerService_Linux64.tar.gz	Contains the Identity Server, the Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server for Linux.
AM_40_AccessManagerService_Win64.exe	Contains the Identity Server and the Administration Console for Windows Server 2008 R2.
AM_40_AccessGatewayAppliance_Linux_SLES11_64.iso	Contains the Access Gateway Appliance and the traditional SSL VPN server iso.

Filename	Description
AM_40_AccessGatewayAppliance_Linux_SLES11_64.tar.gz	Contains the Access Gateway Appliance tar file.
AM_40_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008 R2.
AM_40_AccessGatewayService_Linux64.tar.gz	Contains the Access Gateway Service tar file.

To install Access Manager 4.0, see the *NetIQ Access Manager 4.0 Installation Guide*.

For the supported upgrade/migration paths for 4.0, see the following table. For more information on upgrading/migrating Access Manager 4.0, see *NetIQ Access Manager 4.0 Migration and Upgrade Guide*.

Table 2 *Supported Upgrade Paths for 4.0*

Source	Destination
3.2 SP1	4.0
3.2 SP1 IR1a	4.0
3.2 SP2	4.0
3.2 SP2 IR1	4.0

Table 3 *Supported Migrate Paths for 4.0*

Source	Destination
3.1 SP4	4.0
3.1 SP4 IR1	4.0
3.1 SP5	4.0

2.1 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrading or migrating to Access Manager 4.0, verify the existing Access Manager version.

2.1.1 Verifying Version Number Before Migrating to 4.0

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Verify that the Version field displays a version that is eligible for upgrading to 4.0.

Components	3.1 SP4	3.1 SP4 IR1	3.1 SP5
All Access Manager Components	3.1.4.27	3.1.4.57	3.1.5.42

2.1.2 Verifying Version Number Before Upgrading to 4.0

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Verify that the Version field displays a version that is eligible for upgrading to 4.0.

Components	3.2 SP1	3.2 SP1 IR1a	3.2 SP2	3.2 SP2 IR1
All Access Manager Components	3.2.1-57	3.2.1-57 + IR1-201	3.2.2-77	3.2.2-77 + IR1-107

2.1.3 Verifying Version Number After Upgrading to 4.0

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Verify that the Version field lists 4.0.0.110.

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 The Access Gateway Alerts are Sent to all Configured Monitoring Profiles

Issue: Whenever an alert gets generated, an email notification is sent to all recipients configured in profiles irrespective of which email is designated to receive those specific alerts. (Bug 833336)

Workaround: None.

3.2 WS-Trust RST Does Not Work Without the <wsp:AppliesTo> Element

Issue: After configuring WS-Trust, when a requester sends a Request Security Token (RST) without the <wsp:AppliesTo> element to Secure Token Service (STS), the request fails. (Bug 838323)

Workaround: None.

3.3 Empty Values are Displayed for Access Gateway Service Statistics After Migration

Issue: When you migrate the Administration Console from 3.1 SP4 to 4.0, the Access Gateway Service displays empty values in the Administration Console statistics page. (Bug 838393)

Workaround: Upgrade the Access Gateway Service to 4.0. If the versions for the Administration Console and the Access Gateway are on 4.0, correct statistics are displayed.

3.4 Issue with HTTP Logging Old File Options

Issue: When you restart the Access Gateway Service, Apache does not consider the existing log files during next rollover of logs. This causes a mismatch between the number of existing log files on the Access Gateway device and the **Limit Number of Files to** or **Delete Files Older Than** options set in the Access Gateway logging through the Administration Console. (Bug 840534)

Workaround: Manually delete the files. Default location is `/var/log/novell/reverse/<reverse_proxy>` in the Access Gateway system.

3.5 The Access Gateway is Unable to Uncompress Data

Issue: The Access Gateway is unable to uncompress the data that is sent by the back end server. This occurs when the back end server sends the validation bytes in multiple packets and the Access Gateway does not wait until it gets all the validation bytes. (Bug 841743)

Workaround: None

3.6 Access Gateway Returns Bad Request Error

Issue: Accessing a protected resource with a URL containing `%09` returns an error. (Bug 842481)

Workaround: None.

3.7 Syslog Level Logging Issue in the Access Gateway

Issue: The Access Gateway Service shuts down, if you have not enabled the syslog level logging on the Access Gateway server. (Bug 842805)

Workaround: Enable syslog level logging on the Access Gateway proxy server. For more information about enabling syslog level logging, see TID 7011611.

3.8 WS-Trust Secure Token Service Fails

Issue: An error occurs when an RST request is sent by using SOAP 1.2. (Bug 843094)

Workaround: Modify the end point `/opt/novell/nam/idp/webapps/nidp/WEB-INF/sun-jaxws.xml`. Restart the Identity Server using `/etc/init.d/novell-idp restart` command in Linux. For details, see (http://jax-ws.java.net/2.1.5/docs/soap12.html).

3.9 SSL Connection to the Back-End Web Server Fails with Self-signed Certificate on Windows

Issue: Accessing a protected resource fails when SSL connection is set up between a proxy service and a Web server by using a self-signed Web server certificate and the user selects the option to verify the certificate authority of the Web server certificate. If the certificate is signed by standard CA, then this works fine. `(Bug 843143)`

Workaround: There is no work around. This will work if you choose to disable verification of the certificate authority of the Web server certificate by selecting **Do Not Verify for the Web Server Trusted Root** option.

3.10 Apache Generates Core Dump

Issue: Apache generates a core dump when you create a character profile without adding any value inside the profile and then request a protected resource where this profile is created. `(Bug 845764)`

Workaround: None.

3.11 403 Error Occurs When URLs Contain %0A

Issue: A 403 permission denied error occurs when URLs query string contains `%0A` character. `(Bug 847364)`

Workaround: None.

3.12 SNMP Logs Are Not Generated During Upgrade on Windows

Issue: SNMP related information is not logged in the `platfom.log` file. `(Bug 847454)`

Workaround: For the workaround, see Viewing the Logs.

3.13 Administration Console Upgrade Sometimes Fails

Issue: The Administration Console fails when the `nds.conf` file in the eDirectory contains duplicate lines. `(Bug 847988)`

Workaround: Before upgrading, follow the procedure given in "Upgrading from Access Manager 3.2, 3.2 SP1, 3.2 SP1 IR1a, 3.2 SP2 to 4.0"in the *NetIQ Access Manager 4.0 Migration and Upgrade Guide*.

3.14 Google Authenticator Does Not Support Firefox

Issue: Google Authenticator does not work on Firefox. `(Bug 850838)`

Workaround: Use Internet Explorer version 9 and 10 or Chrome browser.

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 Qmunity (http://community.netiq.com/), our community Web site that offers product forums, product notifications, blogs, and product user groups.

5 Legal Notice

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)