NetIQ Access Manager 3.2 Readme

April 2012

This Readme describes the NetIQ Access Manager 3.2 release.

For more information about the new features and enhancements added in this release, see "What's New in Access Manager 3.2 "in the *NetIQ Access Manager 3.2 Installation Guide*.

1 What's New?

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

1.1 General Enhancements

Simplified Deployment: Access Manager 3.2 offers a simplified deployment model. The entire product can now be deployed as an appliance in a single-box form factor. This is in addition to the existing deployment modes that support deployments in physical environments and in virtualized environments for VMware and XEN. It reduces the maintenance complexity and lowers the cost with lesser hardware.

For more information, see "Differences Between Access Manager and Access Manager Appliance" in the *NetIQ Access Manager 3.2 Installation Guide*.

Supported Operating Systems: New platforms have been added to this release. You can now install Access Manager on the RHEL 6.2 platform. This new platform support is in addition to the currently supported SUSE Linux Enterprise Server (SLES) 11 SP1 or a higher version and Windows 2008 Server R2 platforms. The Access Manager 3.2 components are supported only on the 64-bit architecture.

For more information, see "Hardware Platform Requirements".

Compatibility with Smartphones: This release includes Apple iOS 5 support for browser based applications. New enhancements also provide accessibility from the smartphones to help the infrastructure software administrators in performing their basic administrative tasks.

Performance Enhancements: With Access Manager 3.2, customers can get up to 100% improvement (over the 3.1 version) on transactions per second (TPS) and up to five-fold improvement on the number of concurrent sessions per box. (Refer to the hardware specifications for details. Partners, system integrators, and implementers may refer to the performance benchmark results for sizing, capacity planning, and workload characterization for target implementations.)

1.2 Identity Server

- **Federation Support:** Access Manager identity federation enhancements includes the following:
  - **Active Directory Federation Services (AD FS) 2.0 support using SAML 2.0:** For more information, see "Configuring Active Directory Federation Services with SAML 2.0" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

    Access Manager 3.2 supports the SharePoint services through AD FS federation. For more information, see "Editing Claim Rules for the SharePoint 2010 Application" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **OIOSAML:** A new standard for exchanging security information expressed in SAML assertions.

    For more information, see "Defining Options for Liberty or SAML 2.0" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Enhancements to the Identity Service SDK:** SUpport to retrieve attributes from external sources, which makes the software well-suited for use by cloud providers in addition to the enterprise.

    For more information, see *NetIQ Access Manager 3.2 - API Doc (http://developer.novell.com/documentation/nacm32/nacm_enu/data/bookinfo.html)*and "Creating External Attribute Source Policies" in the *NetIQ Access Manager 3.2 Policy Guide*.
  - **Transient User Mapping:** You can map a temporary identifier (transient user) to a local user using attribute matching.

    For more information, see "Configuring the Attribute Matching Method for SAML 1.1" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Step Up Authentication:** You can configure a specific authentication contract that is required for a service provider.

    For more information, see "Defining Options for Liberty or SAML 2.0 Service Provider" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Authentication Contract to Type Mapping:** Authentication contracts in the Identity Servers have been enhanced to be configured with an Authentication Class Reference.

    For more information, see "Configuring Authentication Contracts" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **A Tool to Remove the Orphaned Federated Identity Objects:** For more information, see "Orphaned Identity Objects" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Certificate Revocation List (CRL) Check Periodicity:** This release supports periodic certificate revocation checks for the remote identity provider or service provider.

    For more information, see "Configuring Communication Security for a SAML 2.0 Identity Provider " in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Central Metadata Repositories:** Access Manager 3.2 allows you to configure several identity providers and service providers metadata entries by using a multi-entity metadata file available in a central repository.

    For more information, see "Metadata Repositories" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
  - **Manual Metadata Entry:** This release supports manual metadata entry for SAML 2.0 service provider.

    For more information, see "Creating a Trusted Provider for Liberty or SAML 2.0 " in the *NetIQ Access Manager 3.2 Identity Server Guide*.

- **Compressible SAML 2.0 Assertions:** The Identity Server can be configured to compress the SAML 2.0 assertions.

  For more information, see "Configuring a SAML 2.0 Authentication Request" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

- **Support for Cloud Service Providers:** Access Manager 3.2 has been designed to address the configuration and support needs for hosts and cloud service providers in addition to the enterprises. This release offers:
  - Flexibility to configure authentication parameters.
  - Enhanced flexibility in configuring authentication parameters.
  - Enhanced authentication for the identity provider.
  - Support for a central metadata repository, which is a key driver for cloud providers and for enterprises with private clouds.
  - Service Provider (SP) Broker feature. This feature allows you to configure policies that control Intersite Transfers. Thus, it helps you to control the authentication flow between multiple identity providers and service providers in a federation circle.

    For more information about the SP Broker feature, see "SP Brokering " in the *NetIQ Access Manager 3.2 Identity Server Guide*.

- The Client Integrity Check in the Identity Server. For more information, see "Configuring Client Integrity Check" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

- User lookup based on the LDAP attribute for the Radius authentication. For more information, see "Configuring for RADIUS Authentication" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

1.3 Administration Console

Improved Certificate Management: Access Manager 3.2 adds popular trusted roots by default, thus reducing the overhead in certificate management.

For more information, see "Security and Certificate Management" in the *NetIQ Access Manager 3.2 Administration Console Guide*.

URL Query Strings: The URL query strings usages in regular expression matches of the Access Gateway Authorization policies. For more information, see "URL Condition " in the *NetIQ Access Manager 3.2 Policy Guide*.

User Interface for touch files: In Access Manager 3.2, you can manage the touch files in the Advanced Options section of the Access Gateway from the Administration Console. it removes the complexity of creating touch files for each device manually. For more information, see "Configuring Advanced Options for a Domain-Based Proxy Service" in the *NetIQ Access Manager 3.2 Access Gateway Guide*.

1.4 Access Gateway Enhancements

Some other important enhancements include the support for the following:

Cookie Mangling: Manipulates cookies so that when a browser retains application cookies from the Web servers after a user logs out, these cookies become invalid. For more information, see "Enabling Cookie Mangling" in the *NetIQ Access Manager 3.2 Access Gateway Guide*.

URL Attribute Filter: URL Attribute Filter : Filtering can be added to each proxy service that will filter out specific URLs from auditing under the *URL Accessed* audit event. For more information, see "URL Attribute Filter" in the *NetIQ Access Manager 3.2 Access Gateway Guide*.

2 Upgrading or Migrating to Access Manager 3.2

After you have obtained the Access Manager license, log in to the Novell Customer Center (http://www.novell.com/center), then follow the link that allows you to download the software.

The following files are available:

Filename	Description
`AM_32_AccessManagerService_Linux64.tar.gz`	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server.
`AM_32_AccessManagerService_Win64.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008.
`AM_32_AccessGatewayAppliance_Linux_SLES11_64.iso`	Contains the upgrade RPMs for SLES 11 version of the Access Gateway Appliance and the Traditional SSL VPN server.
`AM_32_AccessGatewayAppliance_Linux_SLES11_64.tar.gz`	Contains the upgrade for the Access Gateway Appliance from evaluation version to full.
`AM_32_AccessManagerAppliance_Linux_SLES11_64.iso`	Contains the Access Manager Appliance.
`AM_32_AccessManagerAppliance_Linux_SLES11_64.tar.gz`	Contains the upgrade for the Access Manager Appliance from evaluation version to full.
`AM_32_AccessGatewayService_Win64.exe`	Contains the Access Gateway Service for Windows Server 2008.
`AM_32_AccessGatewayService_Linux_64.tar.gz`	Contains the Access Gateway Service for SLES 11 and RHEL 6.2.
`AM_32_ApplicationServerAgents_AIX.bin`	Contains the Agents service for AIX platform.
`AM_32_ApplicationServerAgents_Linux.bin`	Contains the Agents service for Linux platform.
`AM_32_ApplicationServerAgents_Solaris.bin`	Contains the Agents service for Solaris platform.
`AM_32_ApplicationServerAgents_Windows.exe`	Contains the Agents service for Windows platform.

For migration, upgrade, and installation information:

2.1 Migration and Upgrade Instructions

For instructions on upgrading or migrating from 3.1 SP4 to 3.2, see "Upgrading Access Manager" in the *NetIQ Access Manager 3.2 Migration and Upgrade Guide*.

You should first upgrade any Access Manager version prior to 3.1 SP4 to 3.1 SP4. For more information on upgrading to 3.1 SP4, see the Novell Access Manager 3.1 SP4 Installation Guide (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

For information on differences between the 3.1 SP4 Access Gateway Appliance and the 3.2 Access Gateway Appliance, see "Feature Comparison of Different Types of Access Gateways" in the *NetIQ Access Manager 3.2 Installation Guide*.

2.2 Installation Instructions

For installation instructions of the Access Manager Administration Console, the Identity Server, the Access Gateway Appliance, the Access Gateway Service, and the SSL VPN server, see the *NetIQ Access Manager 3.2 Installation Guide*.

2.3 Verifying Version Numbers before Upgrading or Migrating

Before upgrading or migrating to Access Manager 3.2 from any previous version, ensure that you have upgraded all components to Access Manager 3.1 SP4.

To determine the existing version:

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.
2. Examine the value in the *Version* field. The following table indicates the versions that can be upgraded to 3.2.

Component	3.1 SP4
Administration Console	3.1.4.27
Identity Server	3.1.4.27
Linux Access Gateway	3.1.4.27
Access Gateway Services	3.1.4.27
SSL VPN	3.1.4.27

2.4 Verifying Version Numbers after Upgrading

After upgrading all the Access Manager components, verify their version as follows:

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version.*
2. Examine the value in the *Version* field to verify that the component has been upgraded to 3.2.

Component	Version
Administration Console	3.2.0.327
Identity Server	3.2.0.327
Access Gateway Appliance	3.2.0.327
Access Gateway Services	3.2.0.327
SSL VPN	3.2.0.327

3 Known Issues in Access Manager 3.2

The following table lists the known issues and appropriate workaround in Access Manager 3.2:

Issue	Workaround
The Identity Server delegated administrators do not have view or modify rights after migrating from the 3.1 SP4 Identity Server to the 3.2 Identity Server.	1. Remove the Identity Server delegated administrators before migration. 2. Add the delegated administrators back after migration.
Downloading `stdout.logs` through the Administration Console on Windows Server fails.	1. Log into the Access Gateway on Windows. 2. Navigate to `C:\Program Files\Novell\Tomcat\logs\stdout.log` and access the logs.
If the data posted to the Access Gateway before authentication exceeds 50 KB, the data will be lost.	None
The Alert feature with Access Gateway Appliance works only for configuration changes and when the proxy goes up/down.	None
Under the Identity Server logging section in the Administration Console, if the *Log File Path* is left blank, the Identity Server XML log file gets created in `/opt/novell/nam/idp/webapps/nidp/WEB-INF/logs/`. It results in having less space in the `/opt` partition than the `/var` partition.	Specify the *Log File Path* to `/var`.
Changing the IP address of the Access Gateway Management interface fails.	1. Remove the Access Gateway appliance from the cluster. 2. Change the IP address of the Access Gateway Appliance from YaST. 3. Import the Access Gateway Appliance with the current configuration.
Apache does not cache a file if the file size is more than 1 MB.	None

Issue	Workaround
If *Force Secure Cookie* is enabled, authentication goes into a loop when redirecting from HTTP to HTTPS.	Disable the *Force Secure Cookie* option.
The access log is enabled by default in the Windows Administration Console and Identity Server.	By default, the access log is enabled in the Windows Administration Console and Identity Server. Comment out the line `Valve className="org.apache.catalina.valves.AccessLogValve` in the `\ProgramFiles(x86)\Novell\Tomcat\conf\server.xml` file.
Advanced option `NAGHostOptions mangleCookies=on` can cause looping issues.	In version 3.2, for mangling cookies, add the following two options to the Advanced options: ◆ `NAGHostOptions mangleCookies=on` ◆ `NAGWSMangleCookiePrefix AGMANGLE`
The SSL VPN client works in Enterprise mode, but shuts down Windows Explorer using ActiveX. If you restore/downgrade the Windows XP client to Windows XP SP3, the SSL VPN client works in Kiosk mode.	Use Firefox with Java.
If the IP address and DNS servers are configured statically on MAC Leopard and the SSL VPN connection is established, the DNS resolution fails to use the DNS server's IP address pushed from the SSL VPN server.	None
When you install the Administration Console and the Identity Server on a Windows Server 2008 server, you cannot completely uninstall the components. The uninstall program hangs before it cleans all the files and the registry entries.	To uninstall all Access Manager files and registry entries: 1. Run the uninstall program. The program removes most of the files. 2. When the program hangs, exit the program. 3. Delete the following directories: ◆ C:\Novell ◆ C:\Program Files (x86)\Novell ◆ C:\Program Files\Novell\Nsure Audit 4. Run regedit and remove the following entries: ◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\AccessManager ◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\NDS ◆ \HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\nici_x64 5. Restart the machine.
When the DNS server is not reachable and ESP debug logging is enabled, each authentication request will be delayed by 20 to 30 seconds.	Add an `/etc/hosts` entry for authentication domain in Access Gateway appliance.

Issue	Workaround
The extended logging format has changed between the Linux Access Gateway and the Access Gateway Appliance.	None
The Identity Server installation displays the `/novell-access-manager/scripts/nam_utility_functions.sh: line 424: export: <special characters>: not a valid identifier` error message, when the Administration Console password contains special characters, for example, @,$, and (.	Ignore the message.
There may be issues with Identity Injection Policies when the resources are protected by Access Gateway with Non-Redirected Login contract.	Enable the *Redirect to Identity Server When No Authentication Header is Provided* option.
An error `XML document structures must start and end within the same entity` occurs when the values are different in `/opt/novell/nam/mag/conf/server.xml` and `/etc/opt/novell/apache2/conf/httpd.conf` files.	Add the `packetSize` and `maxPostSize` parameters with value 65536 in the `/opt/novell/nam/mag/conf/server.xml` file to the "Connector" element with protocol AJP. For example `<Connector port="9009" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0" connectionTimeout="20000" packetSize="65536" maxPostSize="65536"/>` Also, add the value 65336 to the parameter `ProxyIOBufferSize` in the `/etc/opt/novell/apache2/conf/httpd.conf` file. **NOTE:** The size values in both the conf files must be the same.
When the *Remove Path on Fill* option is enabled in the Path-Based Multi-Homing page, you may have some issues for example, with the help links, *Cancel* button and so on.	None
Browsing help links in the Sharepoint portal using the Access Gateway Appliance fails if the Sharepoint Web portal is configured as a path based multihomed service with remove path on fill enabled.	None

4 Documentation

The following sources provide information about Access Manager:

- Documentation Web Site (http://www.novell.com/documentation/novellaccessmanager32/index.html).
- Access Manager Support (http://www.novell.com/support/microsites/microsite.do). For TIDs and Cool Solutions articles, select *Access Manager* for the *Product* and *Articles / Tips* in the *Advanced Search* options.
- Novell Access Manager Product Site (http://www.novell.com/products/accessmanager/).

5 Legal Notices

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and 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.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.