

Novell Access Manager Appliance 3.2 Beta Readme

December 2011

Novell®

The Novell Access Manager Appliance simplifies Access Manager deployment. It helps you quickly set up the Access Manager system. While installing the appliance, default configuration for all components are created and an association is made between Identity Provider and Access Gateway. The product is ready for use after it is installed.

- ♦ [Section 1, “Features Included in Beta Release,” on page 1](#)
- ♦ [Section 2, “Known Issues in Access Manager Appliance 3.2 Beta,” on page 2](#)
- ♦ [Section 3, “Documentation,” on page 3](#)
- ♦ [Section 4, “Legal Notices,” on page 4](#)

1 Features Included in Beta Release

- ♦ **Novell Access Manager Appliance Default Reverse Proxy:** The Novell Access Manager Appliance has a default SSL-enabled reverse proxy (NAM-RP). This reverse proxy can be used to accelerate the Web servers. The reverse proxy is associated with a self-signed certificate, which is created during installation of the primary Novell Access Manager Appliance, with the subject name as the host name provided during the Novell Access Manager Appliance ISO installation. For more information, see [“Managing Reverse Proxies and Authentication”](#) in *Novell Access Manager Appliance 3.2 BETA Access Gateway Guide*.
- ♦ **Sample Application:** The Sample Application is enabled by default during the Novell Access Manager Appliance installation. This application is a single place for launching the Administration Console and the Novell Access Manager Appliance help. You can use the application to learn and experiment the Access Manager Appliance quickly as long as it is not in production. For more information, see [“Sample Application”](#) in *Novell Access Manager Appliance 3.2 Beta Installation Guide*.
- ♦ **SAML Enhancements:** SAML 2.0 includes support for OIOSAML. OIOSAML is a standard for exchanging security information expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The OIOSAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions. It contains several features including Single Sign-On, attribute queries to an attribute service collocated with Identity Provider, single logout, and discovery of an Identity Provider. For more information, see [“Configuring Authentication Methods”](#) and [“Configuring the Attribute Matching Method for SAML 1.1”](#) in *Novell Access Manager Appliance 3.2 BETA Identity Server Guide*.
- ♦ **Simplified Certificate Management:** The Administration user interface for managing certificates in the Novell Access Manager Appliance has been simplified.
 - ♦ The Novell Access Manager Appliance uses one server certificate for performing the following tasks:
 - ♦ Securing communication between a browser and the Access Gateway reverse proxies, Identity Provider, embedded Service Provider and the SSL VPN.

- ♦ Signing and encrypting SAML assertions for Identity Provider and embedded Service Provider.
- ♦ Consuming and providing identity introductions.
- ♦ Encrypting the tunnel between the SSL VPN client and the SSL VPN server.
- ♦ **Trusted Roots:** Well-known trusted roots are provided with the Novell Access Manager Appliance. Identity Provider can inter-operate with other Identity Providers or it can provide X 509 authentication for the client certificates signed by well-known trusted roots.
- ♦ **Simplified User Interface for Administration:** Now administrators can configure certificates and trusted certificate authorities to the Novell Access Manager Appliance without worrying about the details of various trust stores and keystores that are internally maintained by the Access Manager Appliance. For the Identity Provider, Access Gateways, and SSL VPN components, the security configuration screens, where the certificate keystores and trust stores are configured, do not appear in the user interface.

For more information, see “[Security and Certificate Management](#)” in *Novell Access Manager Appliance 3.2 Beta Administration Console Guide*.

- ♦ **SSL VPN:** This release supports SSL VPN, which provides secure access to non-HTTP applications, such as e-mail servers, FTP services, or Telnet services. SSL VPN is a Linux-based service that is actually accelerated by (and shares session information with) the Access Gateway.

- ♦ **Clustering:** For additional capacity and for failover, you can cluster a group of Novell Access Manager appliances. Clustering enables the following features:

Configuration Synchronization: You configure the cluster, and the configuration is synchronized to all members of the cluster.

Session Sharing: Each cluster member can handle sessions held by another server in the cluster. After a session is established, the same member usually handles all requests for that session. However, if that cluster member is not available to handle a request, another member steps in and processes the request.

- ♦ **Nsure Audit Server:** Access Manager supports the Novell Nsure Audit server for audit logging and file logging at the component level. Access Manager is configured to send auditing events to the Novell Nsure Audit server to provide compliance assurance logging and to maintain the audit log entries.

The Nsure Audit server runs as a 32-bit application using 32-bit compatibility libraries.

For help on installing the appliance, see *Novell Access Manager Appliance 3.2 Beta Installation Guide*.

For a detailed list of all the new feature in Access Manager Appliance, see “[What’s New in the Novell Access Manager Appliance](#)” in *Novell Access Manager Appliance 3.2 Beta Installation Guide*.

2 Known Issues in Access Manager Appliance 3.2 Beta

The following table lists the known issues associated with bugs in Access Manager Appliance 3.2 Beta:

Table 1 *Issues*

Issue	Workaround
When configuration change is applied to the Access Gateway Cluster, intermittently there may be a connection loss to Administration Console.	Refresh the page.
Appliance installation fails if hard disk drive size is 40 GB and RAM size is 8GB.	Perform any one of the following actions: <ul style="list-style-type: none">♦ Delete the /var partition during installation.♦ Increase the hard disk drive size or RAM size.
SAML 1.1 Identity Provider is not configured without specifying PORT in the Login URL field.	<p>Workaround 1:</p> <ol style="list-style-type: none">1. While adding Identity Provide, do not specify the login URL and clear the show card option.2. While accessing the service provider, use the login URL: <code>https://idp.sitea.novell.com/nidp/saml/idpsend?PID=https://idp.siteb.novell.com/nidp/saml/metadata&TARGET=https://idp.siteb.novell.com/nidp/app</code> <p>Workaround 2:</p> <ol style="list-style-type: none">1. In Identity Provider, while adding the service provider, configure the ID at the Intersite Transfer Service page.2. Configure the login URL with port no: 2443 and specify the ID in place of the PID URL: <code>https://idp.sitea.novell.com:2443/nidp/saml/idpsend?id=<idname>&TARGET=https://idp.siteb.novell.com:2443/nidp/app</code>3. Clear the Show Card Option.

3 Documentation

The following sources provide information about Novell Access Manager Appliance:

- ♦ [Documentation Web Site \(http://www.novell.com/documentation/beta/novellaccessmanager32/\)](http://www.novell.com/documentation/beta/novellaccessmanager32/).
- ♦ [Access Manager Support \(http://www.novell.com/support/microsites/microsite.do\)](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 \(http://www.novell.com/products/accessmanager/\)](http://www.novell.com/products/accessmanager/).

4 Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

For Novell trademarks, see the Novell Trademark and [Service Mark list \(http://www.novell.com/\)](http://www.novell.com/).

All third-party trademarks are the property of their respective owners.