



Novell® Access Manager™ 3.1

To compete successfully, your business must provide secure access to all types of users, including employees, customers and partners, regardless of location or time of day. Novell® Access Manager™ solves this challenge, helping you maximize users' access—without limiting security or control.

Novell Access Manager 3.1 simplifies and safeguards online asset-sharing, helping customers control access to Web-based and traditional business applications. Trusted users gain secure authentication and access to portals, Web-based content and enterprise applications, while IT administrators gain centralized policy-based management of authentication and access privileges. What's more, Novell Access Manager supports a broad range of platforms and directory services, and it's flexible enough to work in even the most complex multi-vendor computing environments.

Accessibility Without Vulnerability

Give your IT personnel the tools they need to easily establish secure, hassle-free access to Web-based and corporate server-based applications. Access is granted based on users' roles within the organization or their relationship to it.

Standards-based Web Single Sign-on

Passwords can be a problem, not because of what they are but where they are—

stuck all over monitors, keyboards or other all-too-obvious places in the office. In fact, passwords are sometimes a major security liability, usually when people need to keep track of several just to do their jobs. Fortunately, Novell Access Manager enables Web single sign-on, which means your employees and partners only have to remember one login for authorized access to all corporate Web-based applications.

Simplified Identity Federation

Using Novell Access Manager, you can enable your applications for federation without modifying content or installing additional software on the Web server. Through federation, you can provide users with secure Web access to resources on trusted partners' sites, and vice versa.

Simplified, Centralized Administration

Novell Access Manager makes administration easy. You can use it to centralize access control for all digital resources, and it eliminates the need for multiple software tools at various locations. One access solution

- **Solutions:**
Identity and Access Management
- **Products:**
Novell Access Manager 3.1



“Novell Access Manager is a full-featured Web access management offering that benefits from full administration features as well as built-in SSL VPN, SSL concentration and federation capabilities. Novell has emerged as a leader in the identity and access management market.”

Gartner



Novell Access Manager makes administration easy. You can use it to seamlessly centralize access control and eliminate the need for multiple software tools at various locations. It's an access solution that works for all your users, including employees, customers and partners.

fits all applications and information assets. In addition, Novell Access Manager includes support for major federation standards including Security Assertions Markup Language (SAML), WS-Federation and Liberty Alliance.



Figure 1. Novell Access Manager administration console

Support for Regulatory Compliance

Novell Access Manager delivers visibility into network events and generates detailed reports based on user behavior—such as who authenticated to a particular resource and when the resource was accessed. Whether for an internal assessment or an external audit, the data generated by Access Manager can support your efforts to comply with Sarbanes-Oxley, HIPAA, European Union privacy laws and other government regulations.

Access Manager Components

Novell Access Manager comprises several tightly integrated components, each with an important role to play in controlling access to network content, applications and services. These components are fully compliant with SAML (both 1.x and 2.0), WS-Federation and Liberty Alliance. They include:

Identity Server

This component provides user authentication services for all Novell Access Manager components, according to Access Manager policy declarations. It communicates

out-of-the-box with popular identity stores, including Novell eDirectory™, Sun ONE* Directory Server and Microsoft* Active Directory*, and it generates user roles to facilitate authorization decisions.

Identity Server also enables federated provisioning, which automatically creates user accounts on a federation request. This is an especially useful feature for enabling access to legacy systems, which may require that identity information be placed in a specific directory in a certain format. In such cases, Access Manager automatically provisions these accounts without requiring the user or administrator to manually add them to the legacy system's directory.

Policy Engine

The policy engine guides and controls all Novell Access Manager components. From a central location, it distributes role-based policies to all product services. The roles generated by the policy engine can be used by all components to make effective policy decisions and strengthen enforcement.

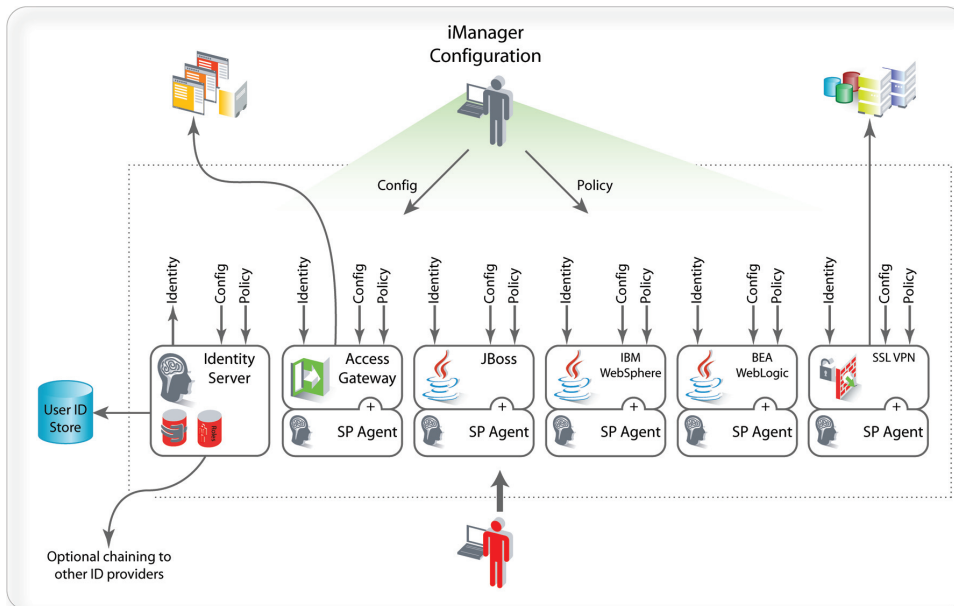


Figure 2. Component overview

Access Gateway

A key component of Novell Access Manager, the Access Gateway provides authorization, single sign-on and personalization without requiring any modifications to the Web server, supported platforms or the the operating system. Furthermore, with the Access Gateway, Access Manager enables many existing Web applications to support new identity standards without change.

Secure Sockets Layer Virtual Private Network (SSL VPN)

Novell Access Manager features Secure Sockets Layer Virtual Private Network (SSL VPN), which provides secure access to non HTTP-based applications. The SSL VPN supports client-integrity checking to ensure that required corporate software—such as firewalls and virus scanners—is enabled before access is granted. To ensure confidentiality, a desktop cleanup feature deletes documents accessed during the SSL VPN session.

Java Application Agents

In Novell Access Manager, the IBM* WebSphere*, BEA WebLogic* and JBoss* agents provide policy-controlled authorization and access to servlets and Enterprise JavaBeans* (EJBs). These agents use Java* Authentication and Authorization Service (JAAS), Java Authorization Contract for Containers (JACC) and internal Web-server APIs for authentication. Together, they deliver precise, policy-controlled authorization and access to servlets and EJBs.

Management Interface

This easy-to-use interface configures and manages all product components and policies in Novell Access Manager. It also presents the status of all devices and policies to all administrators, making warning or alert conditions visible across the enterprise. Through this interface, administrators manage each of the components listed above, plus applicable devices and policies.

Access Manager enables many existing Web applications to support the new identity standards without change.

Novell Access Manager comprises several tightly integrated components, each with an important role to play in controlling access to network content, applications and services.

www.novell.com

Application Integration

Novell Access Manager 3.1 was built with interoperability in mind. Its architecture provides cross-platform support for any standard HTTP Web server, including Microsoft IIS and Apache. Access Manager also seamlessly integrates with the following applications (among others):

- *Microsoft SharePoint**
- *IBM WebSphere*

- *BEA WebLogic*
- *JBoss*
- *SAP* Portal*

To Learn More

For more information about Novell Access Manager, please visit: www.novell.com/accessmanager



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA