Novell® Access Manager™

Comprehensive Access Management for the Enterprise

Novell®

Simple, Secure Access
to Network Resources

Business Driver 1: Cost

Novell Access Manager helps drive down operating costs, improve productivity and streamline the supply chain.

- Deliver secure single sign-on as easily to your partners as to your employees
- Eliminate the headaches of managing security for remote users
- End vendor lock-in and high migration costs

Business Driver 2: Compliance

Align business operations, IT controls and reporting capabilities to meet industry-specific regulations and standards.

- Deliver and monitor role-based access control for sensitive data
- Support advanced authentication
- Automatically report who accesses your data, and when they access it

Networks are becoming increasingly complex as organizations add new applications, infrastructure components and users—day after day, year after year. At the same time, today's networks extend far beyond the corporate campus, often because business users need to work remotely in a secure environment. To keep costs down and stay competitive, organizations need to simplify their networks—and their network managers' lives. More specifically, enterprises need a solution that protects the IT infrastructure from Internet-based threats; secures the privacy of users in the office, at home and on the road; enables simple, secure access for employees and trusted partners alike; and complies with business policies and government regulations. And, they need a solution that does all this while maintaining peak operational effectiveness.

Can any one solution address all of these complex, multilayered issues? Novell® Identity and Access Management solutions are equal to the task. The solutions deliver access management capabilities that grant all users— whether employees, partners or customers— appropriate access while safeguarding resources. Novell Access Manager™ is the technology that enables these capabilities. With Novell Access Manager, IT managers can control access to Web-based and traditional business applications. Network users can conduct business confidentially and securely over the Internet. And in every case, users aren't total strangers. Access is authorized based on users' roles within the organization or their relationship to it. What's more, access can be simplified while the network remains secure—even as the organization reduces costs, addresses regulatory requirements and gains a greater level of control.

Access-related Challenges

Today's IT managers face formidable challenges. There is constant pressure to use resources more effectively, enhance network access to authorized users, tighten security, comply with policies and regulations—and do it all while reducing costs. But before this transformation can take place, IT managers must first resolve several key issues.

Access Control

Novell Access Manager provides access management for network content, applications and services across a broad range of platforms and directory services. It delivers this functionality with components based on industry-leading standards, including Security Assertions Markup Language (SAML), Web Services Federation (WS-Federation) and Liberty Alliance. The seamless integration of Novell Access Manager components across HTTP and non-HTTP environments enables secure access for employees, partners and customers anywhere, at any time. And with Web single sign-on, users can easily access all the services they're authorized to use based on their roles.

From the end user's point of view, Novell Access Manager is convenient. It features a single Web login that provides seamless access to all authorized internal and external services. Each federated identity provider counts on Access Manager for precise policy enforcement. It delivers the same rights users would have if they signed into the individual systems directly. And for all users, Novell Access Manager delivers complete security, locking out anyone who tries to attack business operations or IT infrastructure over the Internet.

Password Management

Forgotten passwords keep helpdesk personnel gainfully employed worldwide. And, as you would expect, there is a direct correlation between the number of passwords users must remember and the number of calls the helpdesk receives. More importantly, there is a correlation between the number of passwords and the likelihood that one of them will be stolen.

To improve both IT and end-user productivity while simultaneously enhancing security, organizations can adopt a single sign-on tool. Such a tool would help establish user identities, automatically track passwords and make compliance efforts less obtrusive and expensive. Single sign-on is the foundation for efficient password management; it leverages identities to provide authorized internal and external users with secure access to resources.

With Novell Access Manager, your organization can deploy standards-based Web single sign-on, which means your employees, partners and customers only have to remember one password or login routine to access all the Web-based applications they are authorized to use. That means far fewer helpdesk calls—and the reduced likelihood of users resorting to vulnerable written reminders.

By simplifying the use and management of passwords, Novell Access Manager helps your organization enhance the user's experience, increase security, streamline business processes and reduce system administration and support costs.

Regulatory Compliance

Regulatory compliance will always be a challenge, but an agile, automated IT infrastructure can substantially cut costs and simplify compliance efforts. By implementing network access tools based on user identities, your enterprise can protect users' privacy and confidential information. At the same time, you can reduce the amount of paperwork needed to prove that proper access-control measures are in place.

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

Through its powerful functionality and easy-to-use interface, Novell Access Manager can turn compliance requirements into opportunities to develop and implement processes that improve business practices.

Business Policy Enforcement

It is the essence of secure identity management: granting users secure access to appropriate IT resources, according to their business relationships and roles. After all, you don't want employees outside of the accounting department accessing payroll data, and there are intellectual properties you aren't even ready to share with a trusted partner. Systematically establishing identity enables your company to enforce policies as you protect both valuable information and the IT infrastructure. With Novell Access Manager, your IT personnel have the tools they need to easily establish secure, hassle-free access to server-based applications. You set the policies by which users gain access, and Novell Access Manager enforces them. And for Web-based applications, you can specify authentication requirements down to a specific URL.

Business Driver 3: Security

Protect users and data by providing reliable, role-based access from any point in the enterprise— for both local and remote employees as well as trusted partners.

- Ensure that remote workers are secure workers
- Revoke network access in minutes, not days
- Gain low-cost, real-time reporting of network security events

Business Driver 4: Agility

Drive business decisions quickly into the IT infrastructure, with minimal disruption of service.

- Take advantage of open standards such as SAML, WS-Federation and Liberty Alliance
- Deliver complete access control— with seamless secure sign-on—to your trusted business partners
- Let business decisions drive IT—not the other way around

By simplifying the use and management of passwords, Novell Access Manager helps your organization enhance the user's experience, increase security, streamline business processes and reduce system administration and support costs.

Novell Access Manager provides:

- **Comprehensive access management, with Web single sign-on and role-based access for Web, enterprise and J2EE applications**
- **Simple identity federation, with automated user provisioning and easy mapping of federation credentials to policy definitions**
- **A plug-and-play security infrastructure for reduced deployment and management costs**

Federated Identity

Many of today's enterprises are collaborating closely online to achieve new levels of profitability and success. More than ever before, they are working together to develop compatible technologies and market new, complementary offerings. But in order for this cross-pollination to happen, one trusted business partner must be able to access resources from another partner in a secure manner. And that's where federated identity delivers value.

Novell Access Manager is built on a solid foundation, one that leverages identity federation standards, including SAML, WS-Federation and Liberty Alliance. This foundation minimizes—or even eliminates—interoperability issues among external partners or internal workgroups. In fact, Novell Access Manager features an identical configuration process for all federation partners, whether they are different departments within the same organization or external business partners. Either way, information flows the way it's supposed to—secure and barrier-free.

Privacy Protection

It's an integral part of regulatory compliance and trusted business partnerships: the ability to establish user-based policies—including Always Allow, Ask Permission or Never Allow—on the exchange of identity. Novell Access Manager offers this level of built-in privacy protection for your employees and partners alike, wherever they are working. With Novell Access Manager in place, your organization can guarantee and document user confidentiality. And for federated provisioning, Access Manager adheres to those same policies and protections. It requires any service to obtain explicit permission from your users before it creates accounts for them.

Novell Access Manager Components

Novell Access Manager is flexible enough to work in even the most complex, multivendor computing environments, integrating seamlessly to provide access control at all levels. Novell Access Manager includes support for the industry-leading Novell eDirectory™, as well as for Active Directory* and Sun* One* Directory identity stores. It creates secure identity and access policies with the following components:

- *Identity Server*
- *Access Gateway*
- *Java* Application Agents*
- *SSL VPN*
- *Policy Engine*
- *Centralized Management Console*

Identity Server

Identity Server is the Novell Access Manager component that authenticates users and provides role information to facilitate authorization decisions. It offers both direct and federated authentication, using a variety of authentication techniques: user IDs and passwords, X.509 certificates (mutual authentication), tokens (one-time passwords via RADIUS) and Novell Modular Authentication Service (NMAS™). Your administrator can specify any one of these methods, or a combination of methods, that users must complete successfully in order to authenticate to your systems.

Identity Server features full support for SAML, WS-Federation and Liberty Alliance Web Service Framework. With this support, your organization can easily configure user authentication processes and the distribution of identity information among different security domains—whether they are different departments within your organization or trusted external partners. Your organization can leverage the standard Liberty Alliance Employee and Person profiles available in Identity Server or define custom attributes and use them in policy enforcement.

Identity Server also facilitates seamless federated provisioning, which automatically creates user accounts on a federation request. Without this feature, users would need to register (create a user account) with a service provider before they could federate their identities.

Access Gateway

Access Gateway is the HTTP proxy component of Novell Access Manager. As the access point for Web applications, it provides security via authentication, authorization, Web single sign-on, identity injection and data encryption—without requiring modification to Web applications. URLs for protected resources, as defined by your administrator, can link to specific Web servers, allowing a single gateway to protect multiple Web servers. The administrator simply changes any DNS entries for specific services from the IP addresses of the corresponding Web servers to the IP address of Access Gateway.

Your administrator can configure different single sign-on policies for each resource and require different Authentication Contracts. When a user attempts to access a resource with an authentication requirement, Access Gateway redirects the user to Identity Server with a request for a specific Authentication Contract. After Identity Server provides the

Access Gateway is the HTTP proxy component of Novell Access Manager. It secures Web applications by providing authentication, authorization, Web single sign-on, identity injection and data encryption—without requiring modification to Web applications.

required validation, the user automatically returns to Access Gateway with a successful authentication and role information. The role information—which can be supplemented by additional queries of the user's identity—determines whether the user is authorized to access the requested resource.

Access Gateway also forwards identity information to the Web server, and you can use this information to personalize content or perform additional policy enforcement. For example, the policy-enabled identity injection feature of Access Gateway, can leverage the Liberty Alliance Web Services Framework to extract identity information and then inject it into Web headers or query strings.

With Access Gateway, your existing Web applications can support new identity services without any modification, and you can narrow authorization requirements down to a specific URL. Access Gateway can encrypt Web server content, so there's no need to install SSL certificates on each server. Access Gateway is available as a dedicated NetWare® service as well as a Linux* service that can host additional services, such as the Secure Sockets Layer Virtual Private Network (SSL VPN). And because the single sign-on process is browser based, there's no client to install on end-user machines.

**Novell Access
Manager Components**

- Identity Server
- Access Gateway
- Java Application Agents
- SSL VPN
- Policy Engine
- Centralized Management Console

Java Application Agents

Novell provides Java application agents (J2EE* agents) for IBM* WebSphere*, BEA* WebLogic* and JBoss*. The latest versions of these agents are available for download at any time and are not tied to Novell Access Manager release schedules.

In the same way that Access Gateway protects standard Web applications, these Java application server agents provide authentication and access control by redirecting authentication processing to Identity Server. They then leverage the role information from Identity Server to enforce policy. The agents use standard Java Authentication and Authorization Service (JAAS) and Java Authorization Contract for Containers (JACC) for authentication and authorization. These standards provide fine-grained authorization control to Enterprise JavaBeans* (EJBs) and servlets.

SSL VPN

The Secure Sockets Layer Virtual Private Network is a remote-access security technology. Through Web browsers, it provides clientless, policy-driven remote access to non-HTTP-based enterprise applications.

To use SSL VPN, your administrator defines the resources a user can access, typically by specifying an IP address and port ranges. The administrator also defines authorization policies by mapping specific roles, as generated by the Identity Server, to specific authorization policies. By applying these policies, Novell Access Manager determines which users are authorized to access back-end applications over SSL VPN.

Once the user authenticates, the SSL VPN client service delivers an ActiveX plug-in or Java applet, and then verifies the existence of required software such as firewalls and virus-scanning software. To ensure confidentiality, a desktop cleanup feature deletes documents accessed during the SSL VPN session.

Policy Engine

One of the greatest strengths of Novell Access Manager is its ability to manage and enforce policies. In fact, role-based access control is an essential part of all Access Manager components, which rely on policy enforcement and logging for regulatory compliance reporting.

The Novell Access Manager Policy Engine is highly extensible and provides full control over policy decisions. It allows third parties to integrate customer-decision processes. It also provides policy-statement resolution and supports the definition of policies in terms of roles as well as customized policy decisions. Finally, it provides policy enforcement for Java applications, even down to the EJB and servlet levels.

Centralized Management Console

The browser-based Management Console provides a central place for your administrators to view, configure and manage all installed components and policies. It's also where your IT manager can monitor the health of the network in real time and automate certificate distribution. And, for large implementations, it is where you can group multiple Access Gateways and then deploy configuration changes to them simultaneously. Novell Access Manager replicates all component and policy configurations in a secure, fault-tolerant store.
To meet your administration needs, Management Console is extraordinarily flexible. It allows you to delegate administration for:

- *Identity Servers*
- *Access Gateways (for products running on both Linux and NetWare)*
- *SSL VPNs*
- *Java Agents*

- *Devices*
- *Policies*

A Secure Access Management Foundation

Reducing costs. Raising productivity. Safeguarding intellectual property. Fostering innovation and collaboration. Meeting product-release expectations. Driving sales. These days, the success or failure of all these endeavors depends on the right people receiving prompt, secure access to network resources. Trusted employees, partners and customers—wherever they work—need unimpeded access. Hackers and thieves need to be kept out. And IT managers need simplified, automated access control, regardless of the network

environment or situation.

Novell Identity and Access Management solutions deliver the flexible, comprehensive access management capabilities your organization demands. A key component of this capability, Novell Access Manager provides access control to enterprise networks and applications of all kinds—Web-based and otherwise. And it removes barriers to access for trusted individuals—whether local or remote—while enhancing security at the same time.

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

"Novell Access Manager is a full-featured Web Access Management offering that benefits from full administration features as well as built-in SSL VPN, SLL concentration and federation capabilities. Novell has emerged as a leader in the Identity and Access Management market."

Gartner

Novell.

Novell Identity and Access Management solutions deliver the flexible, comprehensive access management capabilities your organization demands. A key component of this capability, Novell Access Manager provides access control to enterprise networks and applications of all kinds—Web-based and otherwise. And it removes barriers to access for trusted individuals—whether local or remote— while enhancing security at the same time.

www.novell.com

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

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

Novell.