Staying Ahead of the Access Management Game with Federated Identity Technology
Table of Contents:

2 . . . . Finding an Effective Approach for an Evolving Access Management Landscape

3 . . . . The Elusive Challenges of Identity and Access Management

3 . . . . Federated Identity and Access Management: A Flexible, Practical and Effective Long-term Solution

4 . . . . The Anatomy of a Successful Federated Identity and Access Management Solution

5 . . . . Novell Access Manager: Making Federated Identity and Access Management a Practical Reality

7 . . . . Federated Identity and Access Management Use Cases

11 . . . . Plan Your Move to Federated Identity and Access Management
Identity and access management is certainly not a new topic. Enterprises have been making significant investments in provisioning, single sign-on, password management and other access-related technologies for years in an attempt to lower their IT administrative costs and provide safer, easier and more appropriate access to computing resources.

But cloud computing and other major shifts in the enterprise computing landscape keep changing the identity and access management game—and threatening to make traditional identity and access management investments inadequate and obsolete. As a result, organizations are looking for more flexible and adaptable approaches that can facilitate easy and secure access management among and between internal systems, trusted external organizations, web-based collaboration solutions and (most recently) cloud-based software as a service (SaaS) applications.

**Finding an Effective Approach for an Evolving Access Management Landscape**

Organizations are looking for more flexible and adaptable approaches that can facilitate easy and secure access management among and between internal systems, trusted external organizations, web-based collaboration solutions and (most recently) cloud-based software as a service (SaaS) applications.

![Figure 1](image.png)

*Figure 1. Access management challenges continue to grow in number and complexity.*

Fortunately, a new class of standards-based, federated identity and access management technology is finally making it practical and affordable for enterprises to quickly extend secure, controlled access across all of these environments—without abandoning their investments in traditional identity and access management solutions.
The Elusive Challenges of Identity and Access Management

To understand the full power and appeal of standards-based federated identity and access management, it’s helpful to take a closer look at the evolution of identity and access management technology over the past few years. Identity and access management solutions were originally developed to help organizations reduce IT overhead and simplify user access across a constantly expanding number of internal systems and often-incompatible directory structures. The first few generations of enterprise provisioning solutions focused primarily on automating the process of replicating and provisioning identity information across multiple user accounts and internal directories. Nearly all early access management implementations were project specific, which tended to create unmanageable levels of complexity as organizations worked to extend them to include additional web content. In the end, as organizations became more complex and heterogeneous, traditional user provisioning and access management projects grew steadily more difficult, time consuming and expensive.

Most traditional identity and access management solutions are also limited to internal systems and directories, which has become a significant limitation as organizations work to form closer connections with trusted partners. To stay competitive, enterprises often need to offer their users seamless access to systems and resources from multiple businesses—without time-consuming multiple logins and other access hurdles. This includes the ability to extend collaboration solutions such as Microsoft® SharePoint® beyond corporate boundaries, so people from different organizations can form ad hoc teams and work together effectively on joint projects.

And of course, the emergence and growing popularity of SaaS and other cloud-based technology has added a whole new set of challenging wrinkles to the identity and access management landscape. First, every SaaS provider maintains its own separate, self-contained directory, which means IT administrators have to find ways to create, update and delete user accounts in yet another set of external directory systems over which they have limited control. SaaS services also create new security challenges. Direct user logins over the web can create new openings for phishing attacks and other threats to sensitive corporate data stored in SaaS applications. Finally, the SaaS model threatens yet again to invalidate significant investments in traditional enterprise directories and authentication methods that don’t work outside corporate boundaries.

Federated Identity and Access Management: A Flexible, Practical and Effective Long-term Solution

These identity and access management challenges raise plenty of important questions. What’s the most promising long-term approach for providing fast, seamless and secure access in this ever-changing landscape? How can you build identity and access management solutions that are capable of encompassing and working across a dizzying mix of internal enterprise directories, trusted connections with partners, multi-organization collaboration efforts, and cloud-based services and applications? And how can you make sure the identity and access management investments you make today will apply two years or five years down the road?

For many enterprises and industry experts, the most promising answer to all of these questions revolves around a new generation of federated identity and access management technology. The concept of federated identity has been around for more than a decade. But today, technology vendors are exploring new applications for federated...
Federated identity and access management works seamlessly across the complete gamut of heterogeneous directories, computing platforms and multi-vendor solutions. Identity standards and mechanisms that enable organizations to share identity information and manage access between different internal directories, outside systems, collaboration tools and, most recently, SaaS services.

Federated identity and access management is based primarily on a few core standards that have emerged over the past few years, including the Security Assertion Markup Language (SAML), Web Services Federation (WS-Federation) standards and a set of Liberty Alliance standards. Until fairly recently, business-to-business (B2B) internet single sign-on has been the most common use for this new federated identity technology, which essentially makes it possible for users to access resources from different organizations over the web using a single login.

But the promise and potential of federated identity goes far beyond these common B2B scenarios. Together, federated identity standards make it possible to create a kind of identity metasystem for both enterprise and web applications and services. With this standards-based model, enterprises can use a few flexible building blocks to handle nearly any identity, access management, authentication or provisioning scenario. Federated identity and access management works seamlessly across the complete gamut of heterogeneous directories, computing platforms and multi-vendor solutions. It dramatically simplifies the process of extending identity and access management capabilities beyond organizational boundaries. And it preserves, leverages and extends existing investments in traditional enterprise identity, access management and provisioning solutions.

This has especially important implications as enterprises begin to rely more heavily on SaaS and other cloud-based services. With the right federated identity and access management foundation in place, organizations can quickly extend their existing enterprise provisioning, access management and single sign-on solutions to SaaS environments, which solves a variety of security, compliance and administrative challenges and dramatically simplifies user access to cloud-based services.

The Anatomy of a Successful Federated Identity and Access Management Solution

The benefits of a federated approach to identity and access management are straightforward and compelling. But exactly what does an effective solution look like? And what core characteristics and components do all successful federated identity and access management solutions share in common?

Building a Capable, Complete Identity and Access Management Solution

First and foremost, every effective federated identity framework has to start with a capable, complete enterprise access management solution that fully supports the latest identity federation standards. This core solution must be able to provide complete access management capabilities for all of your enterprise network content, applications and services across a broad range of internal platforms and directory services—and then use federation standards to quickly extend those capabilities to external partners, collaboration solutions and SaaS applications. Here are a few of the essential capabilities you should look for:

- Complete, centralized and unified access control that offers your employees, partners and customers fast, secure access to a full range of HTTP and non-HTTP environments, resources and applications from any location.
- Efficient password management including a web single sign-on component that automatically establishes user identities, tracks passwords and provides internal and external users with secure, authorized access to resources.
Staying Ahead of the Access Management Game with Federated Identity Technology

- **Regulatory compliance tools** that provide deep visibility into network access information and generate detailed reports based on user behavior.
- **Business policy enforcement capabilities** that make it easy to set and enforce identity- and role-based access control policies across all your internal, external, and SaaS systems and applications.
- **Fully integrated, out-of-the-box support for identity federation**, including full support for SAML 2.0, WS-Federation, Liberty Alliance and other key federation standards.

Implementing a True Claims-based Federation System

After you implement a core enterprise identity and access management solution that supports federated identity standards, you can implement a claims-based identity federation model that extends those capabilities to virtually any other service that supports the same specification. In this context, claims are essentially identity-based statements made by one subject about another subject. They are typically issued by security token services (STS), and they contain the information various applications and systems need to make user access decisions regardless of location or architecture and without human intervention.

This claims-based identity federation approach essentially facilitates all of the technology and business arrangements that are necessary to securely connect users, applications and systems within and across organizational boundaries. With this type of claims-based federated model in place, you can quickly bring a wide range of users and services together without custom integration—even when they’re all using different technologies, security approaches and programming models. In this scenario, your organization continues to manage its own identities through your identity and access management system, but you can also securely share and accept claims-based identities with and from other organizations. This makes it possible for work teams, companies and SaaS providers that trust each other in the real world to mirror that trust in their identity stores.

**Novell® Access Manager™**: Making Federated Identity and Access Management a Practical Reality

It’s easy to talk about all of the theories and concepts behind a successful federated identity and access management solution. But Novell is also ready to turn those concepts into a practical, cost-effective reality for your enterprise. Novell Access Manager is the only identity and access management offering that provides both a mature, robust enterprise access management solution and fully integrated standards-based identity federation right out of the box.

In practical terms, this means you gain all the advantages of a robust, centrally managed role- and policy-based access management solution that extends across internal systems and directories, collaboration solutions such as Microsoft SharePoint, trusted partner systems, SaaS providers and more. With Novell Access Manager, your IT staff can define access policies and provision users one time in your central enterprise directory—and then automatically extend access out to any federated system, service or application. IT can also quickly and automatically change access rights across all those systems and services the moment an employee’s role changes or ends. And, of course, users can gain secure, protected access to all the resources and services they need with a single login. In most cases, they won’t even know if they’re accessing services and applications from an on-site system, a trusted partner database or a SaaS provider.

**Novell Access Manager Features**

Novell Access Manager provides all of the advanced access management capabilities you need—including fully integrated identity federation—in one highly integrated infrastructure. This includes:

- Support for SAML, WS-Federation, Liberty Alliance and CardSpace standards
- Web single sign-on (SSO)
- Role-based business and IT policy enforcement
- Integrated secure sockets layer virtual private network (SSLVPN)
- Advanced authentication
- Regulatory compliance visibility
“With Novell Access Manager, a single web-based authentication process provides access to all applications, enabling our users to work more efficiently and from any location they choose.”

Chezy Gal
Administration Systems Engineer
Tel Aviv University

**Business Benefits of Identity Federation Powered by Novell Access Manager**

- **User convenience.** With Novell Access Manager federated identity capabilities, users can log in one time through a convenient browser interface to access all the systems, services and applications they need.

- **Reduced IT complexity and cost.** Novell Access Manager allows IT administrators to provision users as needed, and then use identity federation to automatically enable access to any applications covered by the federated agreement—either on the network or over the web.

- **Enhanced security.** With Novell Access Manager, IT teams no longer have to worry about the tedious manual cleanup work typically involved in decommissioning employee credentials or changing access rights. When IT administrators change a user’s role or access rights, Novell Access Manager immediately uses that information to adjust and determine appropriate levels of access to federated systems. It also forwards updated claims that can be used to control access within federated applications.

- **Improved regulatory compliance.** Federated and interoperable identity infrastructures dramatically simplify the task of monitoring and documenting policy compliance.
Federated Identity and Access Management Use Cases

To make the benefits and advantages of Novell Access Manager federated identity capabilities more tangible and concrete, it’s helpful to examine some typical use cases.

Federation within Organizations

Federation can play an invaluable role in large, complex organizations with multiple identity stores, a wide range of heterogeneous systems and applications, and large numbers of mobile users who need to access resources from inside and outside the firewall.

Federated Identity in Government Agencies

For example, government agencies often use Novell Access Manager federation capabilities to enable and manage access to services across many different departments—many of which require their own government-level validated authentication. In one actual case, an agency with hundreds of separate departments, each with its own federation-enabled service, struggled to manage the large volume of trusted federated links. To solve the problem, they are looking at implementing the Service Provider Brokering feature in Novell Access Manager, which makes it possible to create a single trusted link to the broker and eliminates the need to maintain and manage a separate link for each department. This change will dramatically simplify access administration, while still allowing each department to use different policy specifications.

Federation between Organizations

Using federation across organizational boundaries—often called B2B federation—is perhaps today’s common federation use case. B2B federation makes it possible for different enterprises to port identity information across otherwise autonomous security domains. In these scenarios, trusted partner organizations agree to accept and trust each other’s authentication processes. Each entity still manages the credentials of its own user population, but it also has the ability to accept certain credentials from partner organizations.

Many business, government and educational organizations use B2B federation to provide a broader range of service options for their customers, citizens or students. Others use it to streamline business processes between partners and distributors. In either case, federated B2B solutions are especially attractive to organizations that need to move beyond simple single sign-on and put higher identity assurance controls in place. This is one reason why B2B federation is more common in industries where strict access and compliance requirements are necessary, such as finance, travel, education, health care and government.

At the same time, B2B federation is a worthwhile option for any organization that could benefit from secure access to external resources. For example, if your business relies heavily on outside distributors, manufacturers or other business partners, B2B federation makes it possible to implement more integrated and efficient processes that can accelerate your time to market, increase revenues and raise productivity in both organizations.

Federated Identity and Microsoft SharePoint

One common scenario that highlights the need for identity federation across organizational boundaries revolves around Microsoft SharePoint. Countless organizations use SharePoint to facilitate widespread collaboration. This popular application provides a single, integrated location where employees and teams—as well as their customers, partners and suppliers—can work together, find organizational resources, manage content and workflow, and leverage business insight to make better-informed decisions.

"Implementing Novell Access Manager has guaranteed compliance with the identification requirements of Spanish IT security laws.”

Eugenio Garcia
Head of Security and Logistics
Spanish Public Employment Service
Novell Access Manager supports federated relationships with trusted external entities. In situations where two different organizations need to collaborate using SharePoint, you can simply establish a federated identity relationship between the two environments to ensure seamless, appropriate access for your respective users.

Cross-departmental and cross-organizational teams, however, rarely use the same directory store. Even within organizations, IT teams often create separate directories to accommodate specific SharePoint communities. That means administrators face the complex and time-consuming task of bringing all these different users and directories—both internal and external—together into a single directory store that SharePoint can leverage.

Figure 3. Increased overhead of managing multi-user community access to Microsoft SharePoint.

Novell Access Manager addresses this problem in two important ways. First, it supports multiple directory stores within the same organization, so you can easily manage SharePoint access rights across different internal SharePoint communities with different directories. Second, Novell Access Manager supports federated relationships with trusted external entities. In situations where two different organizations need to collaborate using SharePoint, you can simply establish a federated identity relationship between the two environments to ensure seamless, appropriate access for your respective users. As soon as federation has been established, your organization can share users’ identity information with partners in the form of claims, and vice versa. This makes it possible to determine and grant appropriate access to SharePoint without human intervention.
Staying Ahead of the Access Management Game with Federated Identity Technology

A rapidly maturing class of cloud-based SaaS providers and applications are exploding in popularity, because they offer enterprises an attractive “pay-as-you-go” model that decreases infrastructure costs and software licensing fees and makes it possible to deploy services and applications quickly. Enterprise cloud computing also creates a powerful new need for federated identity and access management technology—by introducing a whole new set of directory structures that have to be maintained, managed and provisioned. Every SaaS provider and application maintains its own directory of users and access rights. Without the kind of federated identity and access management capabilities available in Novell Access Manager, your IT staff would be faced with the daunting task of manually provisioning and managing users separately in each SaaS directory.

Visit www.novell.com/communities/node/11195/integrating-salesforcecom-and-novell-access-manager-using-saml2 for more information on how Novell Access Manager works with cloud-based services and applications.

Figure 4. Simplified Microsoft SharePoint access using Novell Access Manager.
And of course, users would also be forced to login to each SaaS application individually. Instead, Novell Access Manager uses federation to make SaaS applications a natural extension of your centralized identity and access management solution—complete with automated, policy-based user provisioning, via Novell Identity Manager, and the role-based policies, single sign-on capabilities and other benefits Novell Access Manager provides.

Here are two examples of how Novell Access Manager works with specific SaaS providers and applications:

**Salesforce.com**
Novell Access Manager uses SAML 2.0, LDAP and other industry-standard protocols to automate and simplify Salesforce.com user management. For example, Salesforce.com users can authenticate to Novell Access Manager using the LDAP credentials provided in your corporate directory. Then, salesforce.com can authenticate users via SAML without using the standard Novell Access Manager Access Gateway or other federation protocols. This is one example of how Novell Access Manager can enable access to cloud-based resources using only standard protocols and the Novell Access Manager Identity Server. This approach gives your users the convenience of SSO without the security risks of synchronizing your internal LDAP identity information and passwords with salesforce.com’s directory.

**Google Apps**
The federated identity and access management capabilities in Novell Access Manager also make it easy to provide fully federated single sign-on access to Google Apps using SAML 2.0.

---

**Working with Cloud-based Services and Applications**

**Huntington Bank**
Huntington Bank provides an excellent real-world example of how enterprises are using Novell Access Manager to provide and manage secure access to cloud-based resources. Huntington is a full-service bank with 600 banking offices and offers a wide range of services, from commercial and consumer banking to mortgage, brokerage and investment services. Huntington’s IT organization recently turned to Salesforce.com to help it consolidate a wide range of customer data, create a more unified and productive customer view, and meet the ever-changing regulatory requirements in the banking industry.

As part of its Salesforce.com deployment, Huntington chose Novell Access Manager and Novell Identity Manager to streamline identity and access management across a variety of cloud applications and help it maintain the highest levels of security. According to Mark Edson, the Manager of Enterprise Desktop and Directory Services for Huntington Bank, “Novell Access Manager fit perfectly with our existing identity management program. It provides federated identity management to cloud applications so that we can authenticate our colleagues, without ever sharing their passwords with cloud providers.”

Thanks to the fully integrated federated identity and access management capabilities of Novell Access Manager, Huntington was able to quickly extend robust authentication security and access management controls to its Salesforce.com solution without custom integration or complex directory synchronization. “Novell’s identity and access management
solutions have given us an incredibly secure way to protect identities in the cloud,” said Edson. “That’s huge. Huntington’s ability to adopt new cloud solutions has become much more of a turnkey operation.”

**Plan Your Move to Federated Identity and Access Management**

Secure, efficient and effective enterprise-wide identity and access management has always been a top priority for smart enterprises, because it can have such a major impact on IT costs, user productivity and effective regulatory compliance. But providing those services has become increasingly expensive and complex—especially given the explosion of multiple directory systems, the need for more productive partnerships and the advent of cloud-based services. Fortunately, the right kind of federated identity and access management can address these new identity challenges relatively quickly and inexpensively—and provide a flexible, standards-based foundation for the future. Best of all, Novell Access Manager—working together with established federated identity standards and protocols—is ready to provide you with exactly the right combination of mature enterprise identity and access management capabilities and fully-integrated identity federation technology.

“Novell’s identity and access management solutions have given us an incredibly secure way to protect identities in the cloud.”

**Mark Edson**  
Manager of Enterprise Desktop and Directory Services  
Huntington Bank

---

![Diagram](image.png)

**Figure 5.** Novell Access Manager solves your access management challenges.

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