

# Boosting interoperability and collaboration across mixed-technology environments

*Standards-based identity federation solutions from Microsoft and Novell*

May 2009

---

## Executive summary

Despite remarkable gains in IT capabilities and collaboration, organizations continue to struggle with administrative complexity, workforce productivity, and data security. Many organizations support a large number of users—including employees, customers, partners, and suppliers—who seek access to a wide variety of applications and services. This can be particularly challenging in mixed-technology and multiple-domain environments where users are spread across technical and business boundaries.

Microsoft and Novell have come together to solve these challenges and boost cross-organizational collaboration. The two companies are building the interoperability bridges that enable customers to reduce complexity, enhance security, and decrease costs. This paper explains the need for standards-based identity federation, and the current and forthcoming solutions that improve the interoperability of mixed-technology directory environments.

---

“They said it could not be done. This is a new model and a true evolution of our relationship that we think customers will immediately find compelling because it delivers practical value by bringing two of their most important platform investments closer together.”

Steve Ballmer  
CEO, Microsoft

## Introduction

Technology advancement and enablement continue at a rapid pace. Traditional applications are being augmented by sophisticated Web services and service-oriented architectures. These technologies have enhanced the collaboration between work teams, partners, customers, and suppliers around the world. They have also contributed to workforce mobility, enabling users to conduct business virtually anytime, anywhere.

Not surprisingly, these developments have led to increased complexity with which IT teams continue to struggle. Many are managing heterogeneous environments with a mix of proprietary-source and open-source directory structures. And they are being asked to support a growing number of users who need access to a wide variety of enterprise applications and Web services, both internal and external.

For these reasons, identity and access management has become an escalating concern. Custom integration, which increases cost and complexity, is often required to achieve application interoperability. Also, IT personnel must spend an inordinate amount of time setting, re-setting, and decommissioning user passwords—not only for employees, but also for customers, partners, and suppliers. Mixed-technology and multiple-domain environments, which are increasingly common, traditionally require these tasks to be performed separately for directories based on different operating systems. With services, users, and security policies in a constant state of flux, these efforts can impede the most proficient IT teams.

In addition to administrative complexity, the challenges associated with identity and access management can have widespread business implications. Workforce productivity can be negatively affected when users have difficulty accessing cross-organizational services and applications. And business risk increases when data privacy and security are compromised.

IT teams face the divergent task of simplifying access while tightening user authentication in mixed-technology and multiple-domain environments.

## Interoperability through claims-based identity federation

The “Identity Metasystem” is a shared industry vision that defines a single claims-based identity model for enterprise and Web applications and services. It represents a unified model that is based on industry standards, works across platforms and vendor solutions, and takes advantage of a few basic building blocks to handle virtually any identity scenario.

A claim is a statement by one subject about another subject. There are no constraints on the semantics of a claim, but they might include an individual's e-mail address, age, employer, role(s), customer number, or access permission rights. Claims are issued by security token services (STS) and used in the Identity Metasystem to help applications

---

"Microsoft and Novell are enabling customers to take advantage of each other's products where it makes sense in their enterprise infrastructure. We jointly believe that our business and patent agreements make it possible to offer the highest level of interoperability with the assurance that both our companies stand behind these solutions."

Ron Hovsepian  
CEO, Novell

make user access decisions regardless of location or architecture. Claims are delivered inside security tokens produced by an STS, and they can disclose identity information selectively.

The Identity Metasystem vision is being realized through industry standard Web service specifications such as WS-\* (WS-Federation, WS-Security, WS-Trust, etc.) and Security Assertion Markup Language (SAML 2.0). The specifications are designed to support interoperability between machines and applications over a network or the Web. An additional set of specifications define interoperable Information Cards, which are designed to give the user better control of their identities.

Using these industry standards, Microsoft and Novell have simplified identity and access management for applications that use the Active Directory® service and other LDAP identity stores, such as Novell® eDirectory™. This is accomplished through claims-based identity federation, which facilitates the technology and business arrangements necessary for connecting users, applications, and systems within and across organizational boundaries.

Participants in federated systems may use different technologies with different security approaches and programming models, yet they can still bring together their users and services without substantial custom integration. In a federated system, each organization continues to manage its own identities, but is capable of securely sharing and accepting claims-based identities from other organizations. The goal of identity federation is to allow work teams and companies that trust each other in the real world to mirror that trust in their identity stores.

In today's competitive and dynamic business environment, identity federation can help facilitate a number of tasks:

- Quickly and securely forming online relationships.
- Rapidly acquiring customers for new services and offerings.
- Reducing the cost and administrative overhead of managing user accounts.
- Granting appropriate access to external users.
- Boosting security by preventing rogue and orphan accounts.

### **Before and after claims-based identity federation**

A common scenario that highlights the need for identity federation can be seen with deployments of Microsoft® Office SharePoint® Server 2007. Countless organizations use Office SharePoint Server 2007 to facilitate widespread collaboration. It 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.

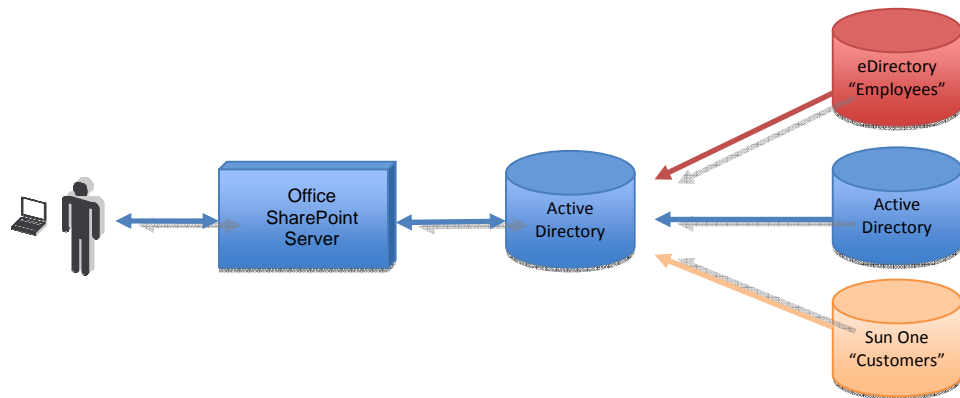
Cross-organizational teams, however, don't always use the same directory service. Without identity federation, each IT team faces the complex and time-consuming task of managing all users—both internal and external—and their associated usernames, passwords, and access rights for all applicable directory environments.

For example, a user whose identity and access credentials primarily reside in a Novell eDirectory service may be asked to access an Office SharePoint Server 2007 application that is hosted by another organization using Active Directory. This is a familiar scenario for large enterprises that have multiple identity stores and user groups, and it is increasingly common for collaboration among partner, supplier, and customer workgroups.

In these intracompany and intercompany scenarios, application access cannot be granted until the corresponding organization recreates—and then maintains—the user's credentials for its own directory system. With a growing number of work teams and business entities using Web services and network-based applications to collaborate across mixed-technology and multiple-domain environments, these redundant identity management tasks are becoming increasingly impractical.

---

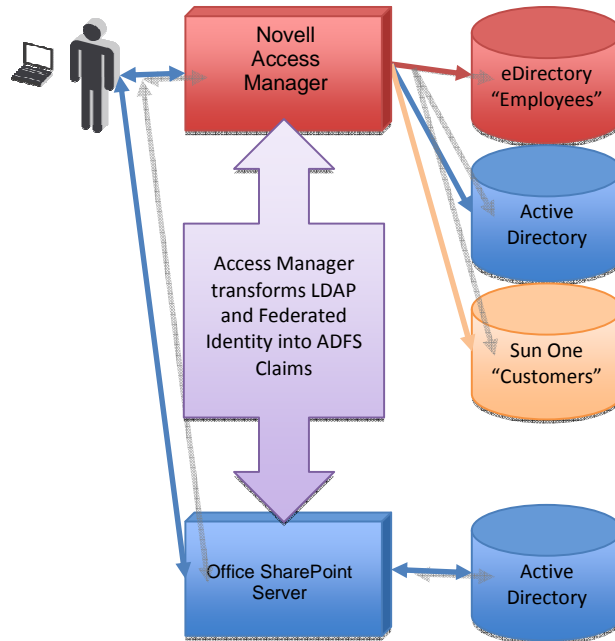
Figure 1: Microsoft Office SharePoint Server 2007 scenario before claims-based identity federation.



Fortunately, identity federation relieves this burden and allows IT teams to manage only their users and the federated relationships with trusted entities.

In the aforementioned Office SharePoint Server 2007 scenario, for example, the two organizations merely need to establish a federated identity relationship between their environments to ensure seamless, appropriate access for their respective users. Once federation has been established, the Novell eDirectory service can share a requesting user's claims with the other organization's application, and vice versa. The receiving system can then review the claims to determine and grant appropriate access to Office SharePoint Server 2007 without human intervention.

Figure 2: Microsoft Office SharePoint Server 2007 scenario after claims-based identity federation.



### Claims-based identity federation solutions available today

Using the WS-Federation specification, Microsoft and Novell have partnered to enable identity federation between applications using Active Directory and other LDAP identity stores, such as Novell eDirectory. Microsoft implements WS-Federation in Active Directory Federation Services (AD FS) and Novell implements WS-Federation in Access Manager™. The collaboration between Microsoft and Novell on federation standards means that authorized users can seamlessly access enterprise applications and Web-based services with one set of passwords and policies, whether their user accounts principally reside in Novell eDirectory or Active Directory.

### Microsoft Active Directory Federation Services

Active Directory Federation Services (AD FS) in the Windows Server® 2003 R2 and Windows Server 2008 operating systems enables organizations to securely exchange claims-based identities across enterprise boundaries, providing seamless access to applications for customers, partners, suppliers, and mobile employees.

AD FS enables federated identity and access management by securely sharing claims-based identities across security and enterprise borders. It takes the information available in an enterprise directory and, using secure Web services protocols, selectively exposes certain attributes to cross-organization work teams and trusted business partners so they may rely on that information to streamline authentication, grant appropriate access, and personalize the user experience.

It requires two organizations (intracompany or intercompany) to set up a federated relationship. In most cases, this includes an exchange of public-private keys, which are used to sign and validate messages one party passes to the other.

Once trust has been established, federation servers at the account provider (“home” organization of the user) and resource provider (target application provided by a partner) exchange a set of claims (user authentication context and attributes) in the form of security tokens. These tokens are securely passed over the Internet using the WS-Federation protocol.

When a user, who has authenticated to their account provider, attempts to access a partner application, the Account and Resource Federation servers will exchange the security token and then the user will be granted access to the partner application without being prompted to authenticate. In addition, the partner application can grant proper privileges and personalize the user experience based on additional information contained in the security token.

### **Novell Access Manager 3.1**

Novell Access Manager 3.1 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, such as WS-Federation. The seamless integration of Novell Access Manager 3.1 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 are authorized to use based on their roles.

Novell Access Manager 3.1 is built on a solid foundation, one that leverages identity federation standards, including WS-Federation, WS-Trust, and SAML 2.0. This foundation minimizes—or even eliminates—interoperability issues among external partners or internal workgroups. In fact, Novell Access Manager 3.1 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.

Identity Server is the Novell Access Manager 3.1 component that authenticates users and provides claims-based 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), Novell Modular Authentication Service (NMASTM) and the Windows CardSpace™ identity selector. Administrators can specify any one of these methods, or a combination of methods, that users must complete successfully in order to authenticate to their systems.

## Forthcoming claims-based identity federation solutions

Forthcoming solutions from Microsoft and Novell will also offer identity federation capabilities. These include Microsoft code name “Geneva” and future Novell Access Manager products.

### Microsoft Code Name “Geneva”

Microsoft code name “Geneva” builds on AD FS and extends it to become an open platform for simplified user access based on claims.

Code name “Geneva” supports industry standards such as WS-\* (WS-Federation, WS-Security, WS-Trust, etc.) and SAML 2.0 for open and interoperable identity. It enables claims-based and non-claims systems to interoperate by translating between claims and non-claims token formats. It also includes support for Information Cards through the forthcoming code name “Geneva” CardSpace component.

Code name “Geneva” implements the Identity Metasystem vision for open identity interoperability through a single, simplified user access model that works across different applications and systems to enable security-enhanced collaboration. It is open and adaptable to enable user identities to interoperate seamlessly.

Code name “Geneva” improves application developer productivity by simplifying and externalizing access logic from applications. It also reduces development effort with pre-built security logic and Microsoft .NET Framework tools.

With code name “Geneva,” IT teams will be able to reap the benefits of simplified user account administration, consolidated access management, reduced custom integration work, and consistent security. Consumers and information workers will be relieved of the burden of managing unique user names and passwords for multiple applications and Web services.

Interoperability testing of code name “Geneva” and Novell Access Manager is well underway. Microsoft and Novell have verified that Novell Access Manager can be used as an Identity Provider (IdP) with a code name “Geneva” Server Service Provider (SP) over WS-Federation or SAML 2.0 protocols. It has also been confirmed that a code name “Geneva” Server IdP can be used with a Novell Access Manager SP over WS-Federation or SAML 2.0 protocols.

### Novell Access Manager

Future iterations of Novell Access Manager will continue to deliver advanced identity and access management federation services. In addition, Novell and Microsoft are working to ensure interoperability between current and future versions of Novell Access Manager and Microsoft code name “Geneva.”

## Reaping the benefits of interoperability

Joint efforts from Microsoft and Novell on identity federation benefit business users, IT teams, and consumers. Improved interoperability across mixed-technology directories provides easier sign-in access to enterprise applications and Web services, easier authentication management, lower IT costs, and enhanced security for business systems.

- **User convenience.** With interoperable identity systems, users do not need to remember multiple user names and passwords to access business applications throughout the day. They can use a Windows®-based workstation, notebook computer, or mobile device to open a Web browser and access an application safeguarded by Access Manager without signing in again. Conversely, users can sign in to an eDirectory account and access an enterprise application or Web service for the Windows operating system without signing in again.
- **Reduced IT complexity and lower IT costs.** IT teams need to provision users in only one enterprise directory structure; through identity federation, users can access any application covered by the federated agreement on the network or over the Web. This reduces the expensive burden of account life cycle management and related helpdesk costs.
- **Enhanced security.** IT teams no longer have to worry about the duplicate cleanup work involved in decommissioning employee credentials or having employees change roles within an organization. IT personnel need only make user authentication changes once, rather than multiple times across multiple enterprise systems.
- **Improved regulatory compliance.** With interoperable identity management infrastructures, organizations are better able to produce documentation required for identity management audits and comply with federal and industry privacy regulations.

## Summary

More than ever, IT teams must support a growing number of users who need access to a wide variety of enterprise applications and Web services. This becomes increasingly difficult when users and applications are spread across mixed-technology and multiple-domain environments.

To enable seamless access and secure interoperability, Microsoft and Novell are delivering identity federation capabilities for Active Directory and other LDAP identity stores, including Novell eDirectory. The federation abilities of Microsoft AD FS and Novell Access Manager 3.1—as well as the impending Microsoft code name “Geneva” and forthcoming Novell Access Manager solutions—are based on industry supported protocols, providing simplified and secured identity federation and application access.

The benefits of standards-based identity federation extend well beyond access to applications and Web services. It improves the collaboration and productivity of cross-organizational work teams. It reduces the complexity and cost of IT administration. And it bolsters the security and interoperability of enterprise applications and Web services.

To learn more about Microsoft and Novell interoperability efforts, visit:  
<http://moreinterop.com/>

---

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

© 2009 Novell Inc. All rights reserved. Novell, the Novell logo, SUSE and ZENworks are registered trademarks and Bandit and eDirectory are trademarks of Novell, Inc. in the United States and other countries.

Linux is a registered trademark of Linus Torvalds. All other third-party trademarks are the property of their respective owners.

All other trademarks are property of their respective owners.

## Novell and Microsoft: building bridges

On November 2, 2006, Novell and Microsoft announced a series of agreements to jointly build, market, and support new solutions to make Microsoft and Novell products work better together. Since forging the five-year agreement, the two companies have rolled out six interoperability initiatives and an interoperability lab where they are testing and optimizing the joint solutions. The aim is to help customers reduce data center costs, gain new levels of flexibility, and streamline operations—all with complete peace of mind around licensing and integration.

To learn more about Microsoft and Novell interoperability efforts, visit:  
<http://moreinterop.com/>

### Microsoft Disclaimer

These notes support a preliminary release of a software program that bears the project code name "Geneva."

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

### Novell Disclaimer

The information set forth in this document may not be construed as a promise by Novell to develop, deliver, or market a product or functionality. It is not a commitment to deliver any material, code, or functionality. Due to changing market and industry conditions, this document should not be relied upon in making purchasing decisions. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Novell reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. This document is for informational purposes only. NOVELL MAKES NO EXPRESS OR IMPLIED WARRANTIES AS TO THE INFORMATION IN THIS DOCUMENT.