

# How to Use SAML SSO to Link Your Active Directory to the Cloud

## Executive Overview:

As SaaS, Web Services and cloud-based applications continue to gain traction, organizations are learning the hard way that their access and enforcement mechanisms aren't ready for the Web 2.0 world.

Rather than continue to force employees to remember, reset and inevitably forget a slew of new user names and passwords, stored in proprietary directories of the applications, most organizations are investigating single sign-on (SSO) solutions.

However, legacy SSO solutions aren't able to stitch together the many existing on-premise applications with those beyond the firewall. Access-control platforms, two-factor authentication tools and identity federation all tackle parts of the problem, but unified solutions are elusive. In addition, the existence of multiple extranet IDs and external authentications leave current logging and auditing systems without a mechanism to record the authentication.

To prevent competing solutions from creating too much chaos, standards bodies have stepped in to propose underlying SSO and identity federation standards, such as SAML (Security Assertion Markup Language), OpenID and the Microsoft- and IBM-backed WS-Federation.

Most cloud and SaaS service providers, including salesforce.com, WebEx and Google Apps, favor SAML; thus, the standard has emerged as the go-to SSO protocol for B2B applications. Yet, a standard isn't a solution, and many methods of integrating existing identity stores into cloud-based applications are riddled with flaws and vulnerabilities.

This paper will address how to leverage your existing identity infrastructure, such as Active Directory, to grant access and enforce identities in the cloud. By linking AD to SAML and on to the cloud, your organization will be able to enforce identity for any on-premise, VPN, SaaS or cloud-based application – all while keeping your organization's identities safe, secure and private.

## Table of Contents:

Introduction: Legacy Security Falls Short in Web 2.0 World .....	4
The Identity Challenge: Why SSO and SAML Are Not Enough .....	5
SAML 101 – Understanding the Strengths and Weaknesses of SAML .....	6
HOW SAML SSO Works with Identity Enforcement Platforms .....	7
SAML and Google Apps .....	7-8
SAML and Salesforce.com .....	8
SSO Solutions that Aren't .....	8-9
The Most Often Overlooked SSO Asset: Active Directory .....	9
Texas Auto Center Customers Have Cars Bricked Because of Faulty Password Reset Procedures .....	10
More Benefits of Identity Enforcement Platforms .....	11
The SecureAuth Identity Enforcement Appliance Bridges Your Active Directory to the Cloud .....	12-13

## Introduction: Legacy Security Falls Short in Web 2.0 World

Today's IT security professionals spend more and more time dealing with one cumbersome task: managing user identities. Even for organizations that have adopted advanced authentication mechanisms, identity management is still a time-consuming cost center. Password resets alone take up an undo amount of IT resources.

As more mission-critical applications migrate beyond the firewall and as SaaS, Web Services and cloud-based applications continue to rise, organizations are learning the hard way that their access and enforcement mechanisms aren't ready for the Web 2.0 world.

To combat application sprawl and minimize the impact on end users, most organizations are moving towards single sign-on (SSO) solutions. However, legacy SSO solutions can't stitch together the many on-premise applications with those beyond the firewall. Access-control platforms, two-factor authentication tools and identity federation all tackle parts of the problem, but unified solutions are elusive.

To prevent competing solutions from creating too much chaos, standards bodies have stepped in to propose underlying SSO and identity federation standards, such as SAML (Security Assertion Markup Language), OpenID and the Microsoft- and IBM-backed WS-Federation.

Most cloud and SaaS service providers, including salesforce.com, WebEx and Google Apps, favor SAML; thus, the standard has emerged as the go-to SSO protocol for B2B applications. Yet, a standard isn't a solution, and many methods of integrating existing identity stores into cloud-based applications are riddled with flaws and vulnerabilities.

Finding an appropriate unified authentication and Identity Enforcement Platform (IEP) is the obvious goal. However, as with any technology, not all IEP solutions are created equal. While many promise the sky and the moon, most fall short, forcing you to migrate or synch identity databases to the cloud, outsource identity management to third parties and/or abandon existing infrastructure investments.

The best-in-class IEPs, on the other hand, offer seamless integration with existing identity data stores – such as Active Directory\* – in order to protect both internal and external assets with two-factor authentication, phishing protection, out-of-band enrollment, SSO, group policy enforcement, access control, on-premise logging and more.

The only existing IEP to offer all of these features is SecureAuth IEP. SecureAuth IEP paves the way for any number of Web 2.0 use cases, including cloud computing, SaaS, Web services, remote worker access, and whatever your IT and end users dream up next.

\* Or any other directory service, including LDAP and NDS.

---

### SAML Defined:

Developed by OASIS (the Organization for the Advancement of Structured Information Standards), an organization that handles more than seventy other Web standards, SAML is an XML-based framework that allows for the exchange of security information. SAML enables different organizations (with different security domains) to securely exchange authentication and authorization information.

In other words, through SAML, your organization can deliver information about user identities and access privileges to a cloud provider in a safe, secure and standardized way.

---

## The Identity Challenge: Why SSO and SAML Are Not Enough

If you visit the user forums of Salesforce.com or Google Apps, you'll see questions like: "Does Anyone Have SAML SSO Working for Salesforce CRM Yet?"

Scroll through the answers, and you'll see that most don't, and of the few who do, they'll admit that this was a tricky, arduous task. Moreover, those who have SAML working often complain about missing features, like logging and auditing.

The main problem is that existing SSO solutions don't mesh well with SaaS and the cloud. As a shortcut, many cloud providers suggest that you create two identity databases – one in-house, another in the cloud – and synch the two. Any solution that doubles your risk (by forcing you to protect two of the same assets in two different places) is not a good one.

Another method for achieving cloud and SaaS SSO is to outsource identities to a third-party identity provider (IdP). Outsourcing is a firmly established IT trend, but control of your organization's identities is the one thing you should never outsource. Think of all that can go wrong with a third-party IdP. The company could go out of business, be hit by a DDoS attack, have its identity databases hacked, outsource its own security IT to a poorly trained third- (or in this case) fourth-party, be acquired by one of your competitors and on and on.

Worse, in any highly regulated industry, what happens if your IdP isn't compliant? Clearly, you won't be compliant either – through no fault of your own. Even internal compliance is challenged, since its nearly impossible to integrate a third-party IdP with your own logging and auditing mechanisms.

Yes, attacks can happen to you just as easily as to a third-party, but you've already spent an inordinate amount of time and money to protect your internal assets. You have policies in place for when something goes wrong. You have an idea of what your risks are. You know whom to hold accountable if a boneheaded error exposes you to greater risk. You have the phone number – probably on speed dial – of the IT staffer whose job it is to keep your organization's identities safe.

What it all boils down to is that with user identities who can you trust but yourself?

---

### The 7 Main Challenges of SAML SSO Integration:

1. Understanding that SAML SSO is not a complete access control and identity management solution.
  2. Keeping user identities in-house where they belong.
  3. Avoiding reinventing the wheel each time you adopt a new cloud or SaaS application.
  4. Protecting existing investments into identity solutions, such as Active Directory.
  5. Integrating SAML with your existing investment in Active Directory.
  6. Integrating application servers (from the like of IBM and Oracle) that consume SAML.
  7. Conquering the biggest challenge of any IT organization, regardless of where applications reside and what standards you use: granting safe, secure access to your employees and managing and enforcing their identities and privileges.
-

## SAML 101 – Understanding the Strengths and Weaknesses of SAML

Anyone researching SAML is familiar with the idea of federation. It's a lofty, worthwhile goal. It's also something that's easier said than done.

Organizations have been struggling to create unified SSO and to achieve some semblance of federation, but standards have been emerging to help. The most notable identity-related standards are SAML and WS-Federation.

In simple terms, WS-Federation is the preferred identity standard of Microsoft and IBM. If you know anything about technology, you know that this has vendor-lock (and iffy interoperability) written all over it.

As a result, SAML is regarded as the open-source identity standard. With broader support, SAML is the preferred standard of such organizations as Google, Salesforce.com, WebEx and many others. Now that IBM and, more recently, Microsoft have thrown their support behind SAML, it has risen to the top and become the de facto identity management standard.

The problem with SAML is that there are many myths circulating about what SAML is and what it does. The main myth that plagues SAML is that it is a complete identity management solution. It is not.

SAML is a framework that enables the exchange of security and identity information. It is not a solution that grants access or enforces identities.

The main difference between SAML and other identity mechanisms is that SAML relies on "assertions" about identities. It is assumed that an IdP is making an assertion and that the IdP is responsible for maintaining user identities, authenticating users and determining privileges.

You know the old saying about "assume." (If you don't, well, do a quick Google search.) The "assume" saying is true of SAML. If you assume that your IdP executes all of these important security functions, you may well end up regretting that assumption. Anybody trusted with handling such sensitive security functions should be one that you have direct control over. Otherwise, you've introduced risk into your network. If you trust an IdP other than yourself, you are implicitly stating that you are comfortable with a high level of risk. You are assuming that you can – now and in the future – trust your IdP. Unfortunately, that assumed trust could come back to haunt you.

Another difference between SAML and other security mechanisms is how identities are enforced. Where other identity-enforcement approaches rely on central certificate authorities to issue certificates ensuring secure communications from point A to point B, SAML is designed in a more Web-friendly manner. Under SAML, any point within the network can make an assertion stating that it knows and has verified the identity of a user or data set. Then, the application being asked to accept a user (or data) must decide whether or not to trust that assertion.

As you can see, the weak link in the SAML identity chain is the integrity of users. Decentralizing control over user identities is a recipe for disaster.

## HOW SAML SSO Works with Identity Enforcement Platforms

Another myth about SAML is that it actually authenticates users. It does not. Some type of authentication solution must perform this task. There are many ways to tackle this problem, but anything other than an Identity Enforcement Platform (IEP) will require a lot of roll-your-own coding, the extensive use of disparate APIs and, often, an increased exposure to risk as third parties get access to your user IDs and their roles and privileges.

What IEPs do is step in and leverage SAML and other existing resources to provide a complete SSO solution. With an IEP in place, a dynamic, two-factor user authentication into the cloud is a simple task. Without one, identities are a weak link in your security chain.

With an IEP, when a user clicks on an application, the application asks the user to authenticate himself or herself. The IEP handles the authentication and converts the local identity into a SAML assertion, communicating that assertion to the service provider or, depending on application designs, the application itself. All of this is accomplished behind the scenes and in a manner that is invisible to end users.

With top-flight IEPs, all that a user does is what they have always done: enter a user name and password. Everything else – two-factor authentication, out-of-band authentication (if required), encryption, phishing protection, etc. – is done transparently.

Moreover, top-tier IEPs require only one instance of user authentication. From that point on, each successive application the user connects to is able to authenticate the user via the IEP behind the scenes. With a top-tier IEP, authentication is dynamic, and each application can be configured independently and to the appropriate level, as mandated by enterprise policies.

The end result is that your organization is able to leverage the IEP to achieve in-house, cloud, SaaS and Web SSO in a safe, secure and centralized way. At the same time, your organization maintains complete control over your most sensitive information asset: your user identities.

## SAML and Google Apps

Google Apps offers a SAML-based SSO service to its customers. Here's Google's description of how it works:

Using the SAML model, Google acts as the service provider and provides services such as Gmail and Start Pages. Google partners act as identity providers and control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts. There are a number of existing open source and commercial identity provider solutions that can help you implement SSO with Google Apps.

There are two important points to note here. Google requires that you use an IdP, which many falsely assume must be a third party. As discussed earlier, the correct IdP for most organizations is you. The reason many organizations don't believe this is possible is because homegrown IdP solutions tend to be difficult to configure and unstable. Using a proven, appliance-based IEP to connect to your internal identity stores, however, eliminates these problems.

The second thing worth noting is that extending SSO to anything on the desktop requires a separate SSO process. At least that's the impression Google is under. Why are they under that impression? Because most SSO solutions are piecemeal, cobbled-together legacy systems that aren't designed for the Web 2.0 world. Conversely, most new SSO systems handle the Web well enough, but fail to properly integrate on-premise applications.

By using an IEP in order to connect your existing directory services to the cloud, this entire muddle is sidestepped. Google Apps and desktop services are simply integrated by the IEP.

## **SAML and Salesforce.com**

Salesforce CRM and Force.com applications accept either delegated or federated authentication for SSO. In a nutshell, delegated authentication allows customers to use an external Web Service to validate user credentials. As salesforce.com readily admits, delegated authentication has several drawbacks versus federated SSO:

First, delegated authentication is inherently less secure than federated authentication. Even if encrypted, delegated authentication still sends the username and password (possibly even your network password) over the internet to Force.com. Some companies have policies that preclude a third party from handling their network passwords. Second, delegated authentication requires much more work for the company implementing it. The Web services endpoint configured for the org must be developed, hosted, exposed on the Internet, and integrated with the company's identity store.

Federated authentication and SAML SSO works similarly for Salesforce.com as for Google Apps. And the same hurdles appear when it comes to third-party IdPs.

## **SSO Solutions that Aren't**

As mentioned above, the other major drawback of using a third-party IdP paradigm is that it does nothing to address your existing application infrastructure. Do you really want to have one SSO regimen for on-premise applications and another for SaaS and cloud-based ones?

Many organizations, often due to regulations like FFIEC and PCI DSS, are busy trying to implement two-factor authentication for existing applications. Given that many of these systems have been around for years, or even decades – with legacy infrastructures like Siebel, SAP, PeopleSoft, Oracle, etc. – the idea of just retrofitting a two-factor authentication system into these architectures is daunting.

Enterprises struggle with creating a common authentication experience across their disparate resources. Mostly this is the fault of the authentication solutions, which are unable to abstract themselves from the application. Most two-factor authentication solutions require an enterprise to integrate cumbersome APIs.

Add up the various APIs needed to secure on-premise, cloud, SaaS, VPN and other resources, and it's a harrowing proposition. But it's daunting only if you look at two-factor authentication and SSO as an app-by-app solution, and not as a platform. Identity Enforcement Platforms abstract all of these problems from IT, giving you a true cross-application, distributed SSO platform for all of your applications, be they on-premise, in the cloud, accessed via VPN or whatever other use case your technologists dream up.

## The Most Often Overlooked SSO Asset: Active Directory

Because of application sprawl, two new types of security service have emerged: Identity as a Service (IaaS) and Authentication as a Service (AaaS). Both promise to federate identity and stitch together various applications into a unified whole. One thing to be wary of, though, is any service asking you to cede the control of your identities to someone else.

Where so many IaaS, AaaS, cloud, SaaS and Web 2.0 SSO vendors most often go wrong is with existing data stores. Active Directory, LDAP, SQL, and the like have been tested, optimized and customized over years and years.

These directory services work.

They're paid for. Your IT staff understands them. They are secure, and – it bears repeating – they just plain work.

Your users already exist in Active Directory; thus, you don't have to recreate them for each new app or use case.

Identity Enforcement Platforms regard Active Directory as the foundational technology that it is. Rather than offering “Active Directory alternatives in the cloud” or “Active Directory synching mechanisms,” IEPs refuse to reinvent the wheel. They take what works – and works well – and integrate it with SAML SSO, two-factor authentication and a number of other security protections.

By leveraging Active Directory, you can also leverage existing attributes, such as out-of-band authentication (via phone, SMS, PIN, etc.) Users are able to maintain their roles and privileges as apps evolve – without successive calls to IT. At the departmental and workgroup level, using Active Directory as the basis of cloud SSO means that groups are intact, as are group privileges.

---

### 6 Things Your IEP Vendor Must Be Able to Do

1. Protect existing infrastructure investments by leveraging native data stores (Active Directory, LDAP, SQL, etc.).
  2. Have built-in two-factor authentication option as well as other authentication options as part of the SSO architecture.
  3. Allow for and automate self-enrollment and self-remediation.
  4. Have the ability – without extensive retrofitting – to map the native directory to any cloud, SaaS, or on-premise application
  5. Avoid the use of complicated APIs that must be attached to, and vary with, each and every new application integrated with the SSO solution.
  6. Provide centralized logging for each identity and each resource accessed.
-

## Texas Auto Center Customers Have Cars Bricked Because of Faulty Password Reset Procedures

If you choose not to use an IEP solution, don't be surprised when user and group privileges start to diverge. Each time user identities and privileges are moved, synched or replicated, you've introduced the possibility of error.

Think about how risky that can be. If a disgruntled employee leaves for a competitor, are you sure that you've suspended all of that person's accounts and privileges? What if the person is computer-savvy, the person who informally helps others with their computing problems? Have you reset all of the accounts that this person could use to harm your organization? If you're replicating identity data stores, you're probably not.

This isn't a theoretical scenario used to gin up fear. Corporate espionage, IP theft and data leaks are often the direct result of unexpired user credentials – or user credentials stolen in plain sight.

In just one example, a revenge-seeking laid off Texas Auto Center employee used the company's Webtech Plus software, which is meant to aid with repossessions, to disable customer vehicles, cause horns to blare all day long and flood the dealership with angry calls and towing requests (<http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/>).

Predictably, Texas Auto Center had not understood how dangerous unprotected user credentials can be. It suspended only the Webtech Plus passwords for the employees it laid off, so the employee, who was Texas Auto Center's informal IT guy, simply used another employee's credentials that he remembered to log in and wreck havoc.

Clearly, a lack of strong authentication and weak security policies were the main culprits. Typical SSO and authentication solutions wouldn't have prevented the problem. If Webtech hadn't been manually integrated into the SSO system – and with today's IT staffs already overworked, it's a good bet it wouldn't have been – the attack would have still been possible.

An IEP, though, would have abstracted strong authentication away from the application, and when an employee tried to access Webtech Plus from an unknown IP address on an unknown device, alarms would have gone off. Policies could be set to address any high-risk scenario, such as a rash of layoffs, and authentication would follow the policies.

With an IEP, the attack would have been prevented and the former employee could have been reported to the police long before he did any damage.

## More Benefits of Identity Enforcement Platforms

The IEP approach has a number of benefits beyond what we've already discussed. To recap, though, IEPs allow you to leverage existing – and already paid for – infrastructure investments.

By leveraging existing security infrastructure, you avoid the trouble of migrating user identities to the cloud. IEP eliminates the security risks inherent with having multiple identity stores or syncing various identity databases.

IEPs also represent a lower TCO versus other SSO solutions, and since they build on top of existing infrastructure, the typical deployment time is days, not weeks or months.

IEP solutions that leverage Active Directory are also the most user-friendly SSO solutions you will find. Users don't have to juggle multiple user names and passwords. IT doesn't have to learn and manage a complicated new technology. And your organization doesn't have to worry about losing its compliance because users (or IT) unknowingly violate corporate policies just because they want to be efficient at their work and use a cloud-based app.

---

### 10 Reasons Active Directory is the Right Way to Enforce Identities in the Cloud

1. User identities and roles are already established and managed in Active Directory. No migrating or syncing is required.
  2. With AD as a foundation, two-factor authentication can be integrated across applications without extensive development efforts.
  3. AD gives you the ability to enforce policy-based group authentication.
  4. You've already paid for AD; thus AD-based IEPs offer a much lower TCO.
  5. Your IT staff knows AD inside and out and isn't forced to learn, manage and maintain yet another technology.
  6. By leveraging AD for SAML SSO, your cloud, SaaS and on-premise applications are protected through a single platform.
  7. Using AD as a foundational technology, cutting-edge IEPs are starting to be available as appliances that can simply be dropped into your network, meaning a complete SAML SSO solution can be deployed in days, not weeks or months.
  8. Your user identities remain where they belong: in-house.
  9. IEP solutions leveraging Active Directory have built-in logging and auditing capabilities, meaning that compliance is a cornerstone of the system rather than something IT must lose sleep over at audit time.
  10. With AD linked to the cloud, cloud-based apps can be easily integrated with existing SIEM (Security Information and Event Management) systems.
-

## The SecureAuth Identity Enforcement Appliance Bridges Your Active Directory to the Cloud

The SecureAuth Identity Enforcement Platform (IEP) is the industry's first identity enforcement platform to integrate strong authentication, SSO, access, and user management services for every cloud, Web, and VPN application. This unique approach ensures that any organization can easily adhere to security and compliance regulations with a single solution that is configurable to meet your specific security requirements.

Competing SSO, authentication and identity management products only provide one security function – such as authentication, SSO, access or user management – and can't support cloud, Web, and VPN applications in a single platform.

### SecureAuth IEP delivers the following benefits:

#### ✓ Increased Security

- Delivers secure access to every cloud, web, and VPN application – all from a single platform.
- Prevents identity theft by protecting every application, including cloud-based applications, with mutual authentication.
- Keeps user identities and access controls in-house – where they belong.

#### ✓ Ease of Use

- An intuitive, familiar user experience instills confidence and speeds adoption.
- No tokens to carry, manage, or lose.
- Automated self-enrollment enables users to gain immediate access from any location at any time.
- Desktop (IWA) SSO provides authenticated users with instant, transparent access to cloud-based applications.

#### ✓ Automatic Infrastructure Integration

##### *On and Off-Premise*

- Automatically translates different identities for cloud and local applications.
- Delivers a transparent user experience with secure SSO between applications.

---

### How an Identity Enforcement Platform Works

- IEP pulls the identity from the enterprise data store (AD, LDAP, SQL, etc)
  - It then conducts either:
    - Secure Desktop SSO (Intranet)
    - Secure 2-Factor Authentication (Extranet)
  - IEP passes the identity on to:
    - Hosted Web Apps (Microsoft, IBM, J2EE)
    - VPNs
    - SaaS applications (salesforce.com, Google Apps, Postini, etc.)
  - And provides added security in the form of:
    - SSO between resources
    - Policy-based group authorization
    - Unified SSO across apps both on-premise and in the cloud
-

- Integrates directly with Active Directory and other industry-leading directories to reduce management overhead and the number of user names and passwords that users have to remember and IT has to manage.
- Leverages user identity and role information without any data migration or synchronization.

*On Premise Only*

- Integrated desktop [Integrated Windows Authentication (IWA)] SSO provides easy user access to cloud and hosted web applications.

✓ **Streamlined Deployment and Maintenance**

- Go from installation and deployment to production in days, not weeks or months.
- Eliminates hardware tokens, deployment of client software, upgrades, or user training.
- Integrated SSO reduces calls to the help desk for lost or forgotten passwords.
- Web-based automated provisioning and de-provisioning of authentication credentials reduces management overhead.
- User self services reduces the tedious task of registration, user account management, and password resets.

✓ **Low TCO**

- You purchase only one product to secure and simplify access to every cloud, web, and VPN application.
- Configurable to meet your strong authentication needs today and address your SSO, access, and user management services in the future.
- Lower administrative overhead by streamlining the tedious task of user account management
- Meets every PCI DSS, NCUA, FFIEC, HIPPA, HITECH criteria for two-factor authentication while eliminating investments for hardware tokens, data servers or infrastructure.
- SecureAuth is a fraction of the cost of hard and soft tokens.

## Stop Thinking about SSO and Act

With SecureAuth SSO, you can solve your user access, authentication and logging and reporting problems in a matter of days, versus weeks or even months with competing solutions.

If you have unique SSO challenges that this white paper has not addressed, call us at 949-777-6959 or email us at [ssoquestions@gosecureauth.com](mailto:ssoquestions@gosecureauth.com).

As with any new technology purchase, we encourage you to try before you buy. Visit <http://www.multifa.com/contact-multi-factor-authentication-company/trial-request.aspx> to sign up for a free 30-day trial.

---

“Being in education, when we were looking at moving to Google Apps over our summer break one of the big issues was username and passwords having to be issued while everyone was gone. With SecureAuth this didn't happen as we continued to authenticate everyone with the username and password they all knew. Over the coming months we will be looking at implementing SSO into more of both our in-house and outsourced applications. Thanks to SecureAuth our move to Google Apps and SSO was uneventful!”

– Chris Johnson, Director of IT at Roseville City School District, Roseville, California

---