

How to Secure Identities in the Cloud (or anywhere) via STS

Using a Security Token Service (STS) to Enable Application-Based Identity Enforcement

Executive Summary

As computing and applications sprawl beyond traditional network perimeters, enterprises need new solutions to authenticate users. In the past, IT could claim to “know” users with a reasonable degree of certainty. Insiders could be easily separated from outsiders, and authentication mechanisms, roles and privileges could all be adjusted accordingly.

Today, there is no such thing as a trusted insider. With attackers exploiting new vulnerabilities faster than enterprises can patch them, no user, device or domain is truly trustworthy.

These days, trust must be earned.

To cope with these problems, solutions such as Security Token Services (STS) have emerged. Unfortunately, not all STS solutions are created equal, and many only act as Band-Aids on a gaping wound.

This paper will discuss what is needed to achieve true federation and Single Sign On (SSO) through STS. The paper will also argue for why basing STS on Identity Enforcement Platforms (IEP) offers the shortest path between chaos (and a high risk level) and order (along with greatly diminished risks).

Finally, this white paper will discuss the benefits of SecureAuth, the only IEP platform offering Security Token Service, 2-Factor Authentication, SSO, and IdM in a single solution. SecureAuth provides a secure and simple means for end-users to access cloud and on-premise applications and resources in a unified, consistent manner.

Table of Contents

- Introduction: what is STS and why should I care?.....2
- The problem of application sprawl.....2
- Why SAML-based SSO is only a partial solution4
- What is required to provide secure access to the cloud?5
- Four requirements for secure cloud access.....6
- Why to Federate through STS based on IEP.....7
- SecureAuth delivers federation, STS, SSO and more in one solution.....8



Introduction: What is STS and Why Should I Care?

In an ideal world, you wouldn't know or care about Security Token Services (STS). In an ideal world, identity management and authentication would have been solved *before* organizations began rushing to the cloud. In an ideal world, user authentication would involve more than establishing a vague, tough-to-verify sense of "trust" before granting access to your organization's critical data.

In an ideal world, applications wouldn't sprawl.

STS is a direct response to the problems above. IT administrators and security professionals can no longer assume that they will be managing and securing in-house computing assets. They are also having a harder and harder time distinguishing "trusted" insiders from "untrusted" outsiders. Even the rapidly changing end-device landscape, which is increasingly relying on smartphones, tablets and other post-PC devices, poses trust problems.

STS is a tool that passes a user identity from the enterprise to an application in a format the application understands. In essence, STS is a "trust" broker. STS has the ability to communicate trust to applications, end user devices and an organization's security logs. Just as importantly, STS is able to translate trust assertions from one application or data store to another.

To get back to the question posed above (why should I care about STS?): you're already worrying about STS, but you're probably not thinking of the problem in those terms.

The problem is a sign-on and trust problem. Typically, the solution is described as a Single Sign On (SSO) solution, often based on SAML (Security Assertion Markup Language) tokens.

The trouble with this approach is that too many vendors used flawed architectural plans to build their initial SSO solutions. Now, as applications sprawl, they're continuing to build on top of a flawed structure, and trying to patch over serious cracks in the foundation in the process.

In this white paper, we will discuss why application sprawl, cloud-based authentication and the loss of trust in computing are such serious issues.

We'll look at why the answer to these problems starts with end-user identities and the establishment (or re-establishment) of trust. The paper will argue against emerging authentication and identity management solutions that make the problem worse by advocating such things as identity outsourcing, and it will pose an alternative solution, one that allows organizations to maintain control, greatly improve trust, and securely manage applications and end users no matter where they are – in house, in a private cloud or in a public cloud.

Growing Problem: Application Sprawl Creates an Identity Crisis.

Think back fifteen years or so. Remember, back in the mid-nineties when applications were easy to secure? They were in a central data center, protected behind network security perimeters and hacked at, if at all, by precocious computer-savvy kids rather than organized criminals.

Given today's perilous state of IT security, it all seems so quaint, like a Norman Rockwell painting of digital security.

Today, applications can be anywhere. Users are scattered among branch offices, partners, home offices, hotel rooms and wherever else they happen to be at any given moment. Devices aren't consistently IBM PCs with Windows. They can be smartphones, tablets or netbooks. They have different operating systems and on-board security. Each poses



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

different risks to the enterprise.

So much has changed; yet with authentication and identity management, so much has stayed the same. And that's not a good thing.

Many organizations authenticate into cloud, SaaS and other emerging application environments in pretty much the same way they did back when all applications resided in an in-house data center.

Multifactor authentication may be in place, but all that it does in many instances is make up for the failings of user names and passwords. Hardware-based tokens are better than user-name/password authentication at first glance, but once IT overhead, the expense of provisioning and replacing them and integration costs are factored in, many organizations will decide they'd rather take their chances with user names and passwords and a higher risk exposure.

If they need 2-Factor authentication for compliance reasons, they'll often use inferior, clumsy and inflexible second factors, such as phone-based SMS. 2-Factor solutions sitting in front of an application or even SSO, provide only a binary logical step when not integrated into an Identity platform. In other words, it's not the second factors that are the issue. It's trust that is the issue. Or, more accurately, it's trust plus convenience that is the issue. A strong method of authentication that users can't use and IT can't manage is secure (if users can't get in, it's certainly secure), but it's hardly worth the productivity losses your organization will experience.

How do you provide secure, convenient access to applications in private clouds, hybrid clouds and public clouds? How do you provide access to traditional on-premise applications, while also delivering access to apps delivered as services? How do you manage all of this in a unified manner that doesn't undercut your security posture, place too many restrictions on end users, or overwhelm IT with management and maintenance burdens?

The common answer today is that you don't. Many organizations have mid-nineties era identity enforcement solutions serving as the gateways to cloud- and SaaS-based applications.

Some organizations have adopted tokens and tried to integrate them into this new computing reality. Many have abandoned tokens not too long after implementation.

A few proactive organizations have turned to emerging multifactor authentication vendors, hoping to find an answer with them. Unfortunately, with many of these vendors the solution is a mirage. Yes, they offer a solution that works for the cloud, but it is different than how you will authenticate in house.

Worse, many of these new authentication schemes require you to outsource identity management. Important assets residing outside of the enterprise perimeter is a serious problem. It's like fighting fire with fire. You may well put the fire out, but you'll burn the building down in the process.

And once the fire is out, you'll probably also learn that you're not even close to being in regulatory compliance. Outsourcing identities and authentication workflows can easily undermine efforts to comply with such regulations as PCI DSS, FFIEC, HIPAA, FISMA and plenty of others.

Another reason not to outsource identities and authentication is that you'll have a difficult time differentiating outsiders from insiders, and setting roles and privileges accordingly. Your IT staff will have a far better idea of when someone is accessing something they shouldn't than a third-party provider. These days, internal applications often need to be securely accessed by users outside the perimeter from "network-enabled" devices, such as a smartphone. It's a tricky, risky matter, authenticating these users. Do you really want to trust a third party to do so in a secure and consistent manner?



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

SAML-based SSO: The Answer that Solves only Part of the Problem

To attempt to solve the many challenges of cloud-based computing and application sprawl, security vendors have been rolling out various SSO solutions. Legacy SSO solutions, of course, aren't able to stitch together the many existing on-premise applications with those beyond the firewall. Access-control platforms, 2-Factor authentication tools and identity federation all tackle parts of the problem, but unified solutions have been elusive.

In addition, the existence of multiple extranet IDs and external authentications leaves 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, making it the de facto standard for cloud and B2B SSO. 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.

Not all cloud and SaaS providers use SAML, however, which is why it's important to have an STS in order to automate the translation and solve this issue before it becomes a serious issue.

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

Even though SAML is achieving the acceptance of an industry standard, it's important to remember that a standard isn't a solution. Many methods of integrating existing identity stores into cloud-based applications are riddled with flaws and vulnerabilities.

In brief, many SAML/SSO solutions require you to re-engineer your existing security. They force you to:

- Install and integrate SAML modules
- Integrate with non-SAML (.NET, J2EE) on-premise web session mechanisms
- Integrate with existing web-sessioning systems (assuming you have one)
- Integrate with 2-Factor authentication systems
- Integrate with logging systems
- Integrate with Identity Management tools for:
 - Password resets
 - User self-management tools
 - Help desk tools
- Worst of all, many SAML/SSO solutions force you to outsource your identities, which is a surefire way to introduce new security risks

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. They'll also admit that they have a cobbled-together solution built of pieces that don't fit together all that well. Moreover, those who have SAML working often complain about missing features, like logging and auditing.



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

Can you cobble together a solution that works from various vendors offering various pieces of this puzzle? Yes.

Will the total solution work seamlessly together? Probably not, but it may work the way a twenty-year old car works. It'll get you from place to place – sometimes but not always.

Will you break your budget by having to buy many point products, invest in costly engineering services and spend heavily on system management and maintenance? More than likely.

(For more on this issue, please refer to our SAML white paper.)

What is needed is a complete, unified solution that makes it secure and simple for end-users to access cloud and on-premise applications and resources.

What are the Steps to Provide Secure Access to the Cloud?

One of the advantages of cloud computing is that it allows organizations to deploy applications and devices in a more user-centric manner. Gone are the days of overprovisioning licenses and limiting application access because of security fears.

Those days are gone, that is, if organizations utilize the proper user-centric security, so that convenient, “anywhere” access doesn't introduce inappropriate risks.

In order to provide secure access to the cloud, an authentication and access control solution must perform four steps.

First, it must be able to consume identities from various resources. Enterprises utilize many different types of identities including browser login, web SSO, tokens, SAML, X.509 certificates, Kerberos, CAC Cards, etc. To be effective, the system must be able to consume identities from any resource.

Second, it must be able to input and map identities. The system must be able to input user identities in a standardized, secure form (SAML, OpenID, OAuth, etc.) and then map those identities to relevant data stores, such as Active Directory or an LDAP directory.

Third, a secure cloud access solution must provide a flexible authentication workflow. A rigid workflow leaves authentication as a binary option – red light vs. green light – that cannot take into account differences in users, devices and applications.

Flexible authentication workflows authenticate to both internal and external resources, and for both internal and external users. They have both public and private modes, and offer a range of 2-Factor authentication choices, depending on an organization's needs. Those are able to adhere to whichever regulatory requirement (PCI-DSS, HIPAA, FFIEC, etc.) the organization must comply with.

Authentication solutions with flexible workflows are able to chain policies together. For instance, if an internal user with limited privileges is accessing an application that has HIPAA ramifications, the policies that apply to each scenario must work together – often heightening authentication requirements along the way and often requiring additional authentication factors.

Finally, flexible solutions provide a workflow that is easy to use for both end users and the IT staff overseeing the solution.

Fourth, the solution must be able to assert/translate the identity (retrieved from Active Directory, etc.) to the application and log the event. The solution should be able to do this for on-premise solutions (i.e. Microsoft SharePoint or IBM WebSphere), network devices (such as Juniper SSL VPN); public, multi-tenant cloud.

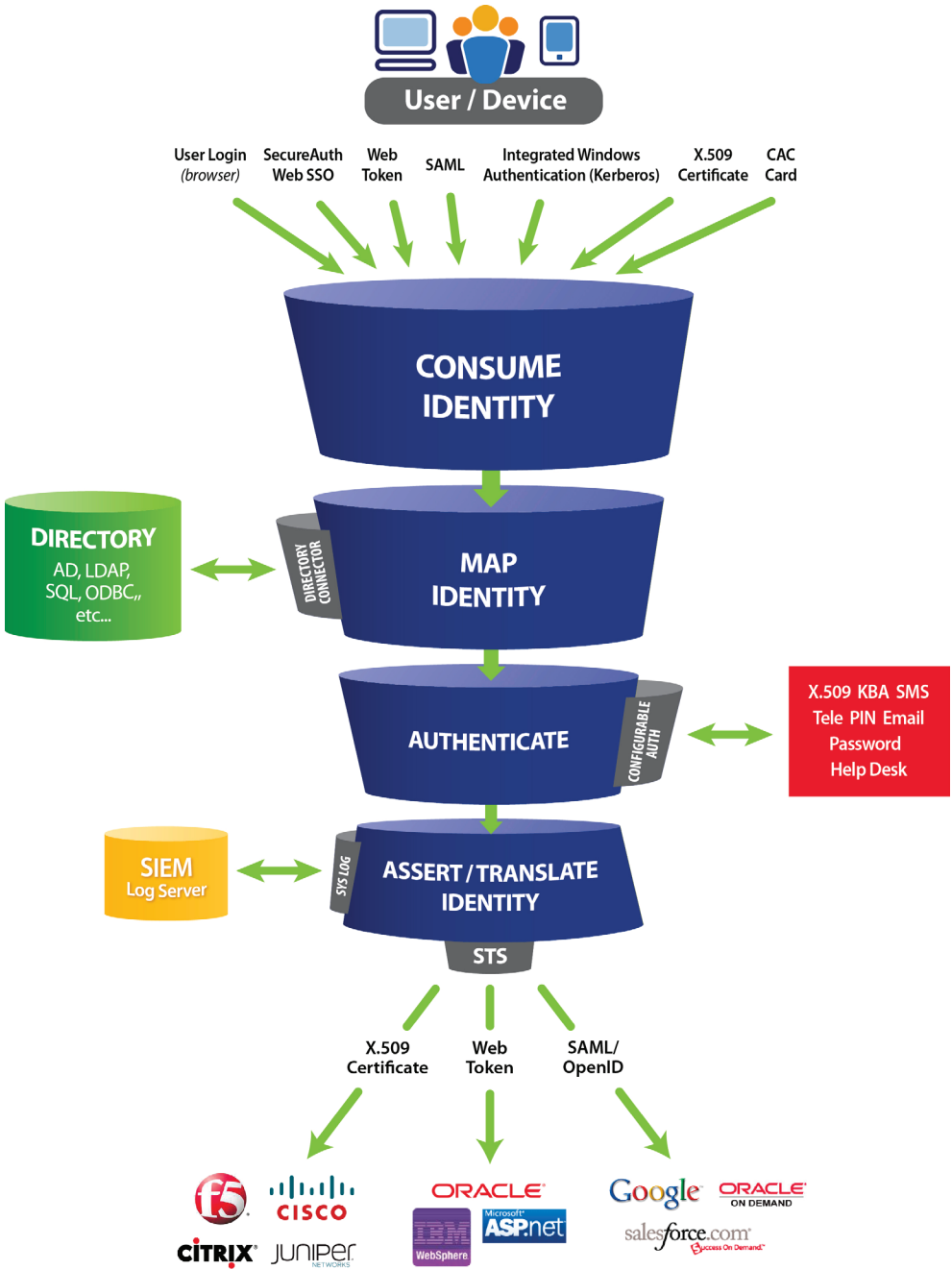


or SaaS applications (salesforce.com, Postini, etc.), and hybrid applications living in the cloud delivered on a Platform as a Service (PAAS) such as Amazon Web Services (AWS) or Azure.

When asserting the ID, it's important that the solution be able to assert various authorizations (x user is a member of y group with z privileges), and it should give the organization the ability to configure multiple custom attributes for various roles. When required, the system must be able to automatically translate the identity to meet the requirements of the recipient resource. Lastly, the solution must log access events. Without logging, there is no compliance. The log should keep track of UserID, time and date, authentication event, company name, appliance name and realm.

4 Steps to Secure Cloud Access

- 1. Ability to consume identity from various resources.
- 2. Ability to map IDs from in-house directory service to application
- 3. Ability to provide an authentication workflow that enforces policies, satisfies regulatory requirements (specifically for 2-Factor authentication), and is easy to use
- 4. Ability to positively assert/translate an identity in a standardized format (such as SAML) to an application (or other resource) after authentication and log the event



Corporate Headquarters
 8965 Research Drive
 Irvine, CA 92618
 949 777 6959
 www.gosecureauth.com

Federation through STS based on an Identity Enforcement Platform (IEP)

All of the requirements discussed above add up to one thing: federation. Single Sign On (SSO) and federated identity solutions have been the Holy Grail for some time, but few of the solutions reaching for the Holy ID Grail are able to deliver consistent access and consistent security across a variety of applications (on-premise, through a VPN, in the cloud) and across various user groups.

To achieve federation, consistency and completeness are the keys. In its simplest form, STS acts as a “trust” broker. Both the application and the end user’s device rely on the STS to assure them that they can trust each other. The application “knows” the user has the privileges needed to be granted access. The user, in turn, will be told whether or not the application is trustworthy. STS eliminates the threat of phishing and malware-invested websites.

The STS is able to deliver secure access across applications because of its ability to translate among various trusted protocols and authentication schemes – in theory, anyway.

In practice, most solutions cut corners somewhere or other. They require organizations to deploy different systems for different usage scenarios or different applications. They necessitate complicated coding and integration. They require you to store identities in more than one place, synching them together. Or, worst of all, they ask you to outsource identities.

A better approach is to use the STS feature of an Identity Enforcement Platform (IEP). That’s right, STS is simply a feature of the larger solution set delivered by IEP. Of course, it’s important to be clear on what an IEP should deliver, since there are many inferior solutions. An effective, secure, flexible IEP solution must deliver STS, SSO and 2-Factor authentication all as a single, unified solution.

Instead of using different access schemes for different applications, instead of synching identities and instead of outsourcing identities, an IEP will simplify access to all cloud, on-premise, Web and VPN-accessed resources.

The key to this kind of consistency is reusing a resource your organization already knows, has optimized and has invested in: Active Directory (or other directory services like LDAP).

Where so many SSO vendors 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 (or whatever other directory services your organization uses, such as LDAP); 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.

In other words, STS based on IEP means that your “trust broker” is basing that trust on a truly trusted service, and one that has been tested and proven for years.

By leveraging Active Directory, you can also leverage existing attributes, such as out-of-



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

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 federation means that groups are intact, as are group privileges.

Federation and STS through SecureAuth IEP

The foundation for SecureAuth's STS solution is the SecureAuth Identity Enforcement Platform (IEP). SecureAuth IEP includes a Security Token Service, 2-Factor Authentication, SSO, and IdM in a single solution to make it secure and simple for end-users to access cloud and on-premise applications and resources.

The solution is both consistent and complete.

SecureAuth's unique approach solves the problem of authenticating users from an existing directory like Active Directory and extending those identities to on-premise web applications, VPNs, mobile devices, and cloud applications such as Google Apps, salesforce.com, Success Factors, Oracle OOD CRM, etc. Until now, enterprises have struggled to deploy a solution that could handle all of these disparate resources.

SecureAuth IEP STS addresses the security interoperability challenge between applications in different identity domains through standards. By providing a standards-based method of converting a security token from one application into the format that another application understands, the solution is able to offer complete access control and authentication for on-premise, private cloud, public cloud and VPN-accessed applications.

For example, SecureAuth IEP will convert X.509 Certificates to SAML assertions and vice versa. Architected to provide a common access control infrastructure for a group of applications, SecureAuth IEP STS negotiates trust between client applications and Web services, removing the need for a direct relationship.

SecureAuth IEP STS makes assertions based on evidence that it trusts. The applications receiving the assertion know they can trust SecureAuth, and to communicate trust, SecureAuth provides a signature to prove knowledge of a security token or set of security tokens.

Establishing a Secure Identity Infrastructure

The SecureAuth IEP STS establishes a secure identity infrastructure for exchanging one type of security token for another. The infrastructure isn't dependent on any one mechanism, such as the Kerberos protocol or X.509 to secure messages. This makes it easier to enable different authentication protocols to interoperate, by adding a level of abstraction on top of existing protocols. SecureAuth IEP's 2-Factor authentication and SSO work seamlessly with the STS, which eliminates the need to enter additional passwords or use another security protocol for authentication and authorization.

This unique approach makes SecureAuth IEP easy to implement, while reducing administrative overhead and strengthening security by ensuring that only authorized users are accessing applications.

SecureAuth IEP STS Is all Inclusive

The original promise of the cloud is that it would be like a utility - nobody should care where it is physically or what type of hardware it runs on, as long as the application works well. Unfortunately, poorly designed security solutions have hindered that promise.

SecureAuth works not just for cloud or SaaS environments. Yes, SecureAuth can handle public, multi-tenant cloud applications, such as Google and salesforce.com, but it is also equally adept at securing private clouds from the likes of Terramark and Rackspace, as



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

well as applications in Platform as a Service (PaaS) environments, such as Amazon Web Services and Microsoft Azure – all while handling on-premise applications too.

Now, business decisions can determine where your applications reside, rather than security obstacles. With SecureAuth, you can run each of your applications where it makes the most sense from a cost, security and logistical perspective.

Delivered as an appliance, SecureAuth IEP's Security Token Service includes everything that is needed to create an independent trust relationship across diverse types of applications and environments. SecureAuth IEP STS includes:

- An appliance-based web server that automatically handles redirected authentication requests.
- Data connectors to on-premise directories including Active Directory, ADAM, LDAP v3, SQL, ODBC and more.
- Executables to conduct a configurable 2-Factor authentication, including the creation, refreshing, validation, and revocation of digital certificates. Registration options include UserID/Password and/or SMS, Telephony, X.509 digital certificates, KBA, Pin, and Help Desk.
- Built-in, customizable form pages securely collect profile information and provide user friend self-enrollment interface.
- The ability to automatically assert the identity in the appropriate format that is the relevant to on-premise web applications, VPNs and SaaS applications. This includes support for SAML 1.1, SAML 2.0, Microsoft FBA, IBM LTPA, CA SiteMinder, URL Identity Passing, and X.509 digital certificates.
- STS Extensions to establish a secure conversation that provides configurable SSO and strong authentication.
- Automated logging to a local or cloud-based Security Incident and Event Manager (SIEM). The syslog event includes the appliance ID number, the realm number, the event code, date, time, and user ID.

SecureAuth IEP STS for Web, VPN and SaaS Resources

SecureAuth utilizes a revolutionary new approach to X.509 v3 technology that delivers the promise of strong authentication without the complexities and cost of PKI and hardware tokens. SecureAuth IEP's innovative architecture enables SecureAuth to conduct 2-Factor authentication utilizing industry-endorsed, browser-based X.509. v3 certificates.

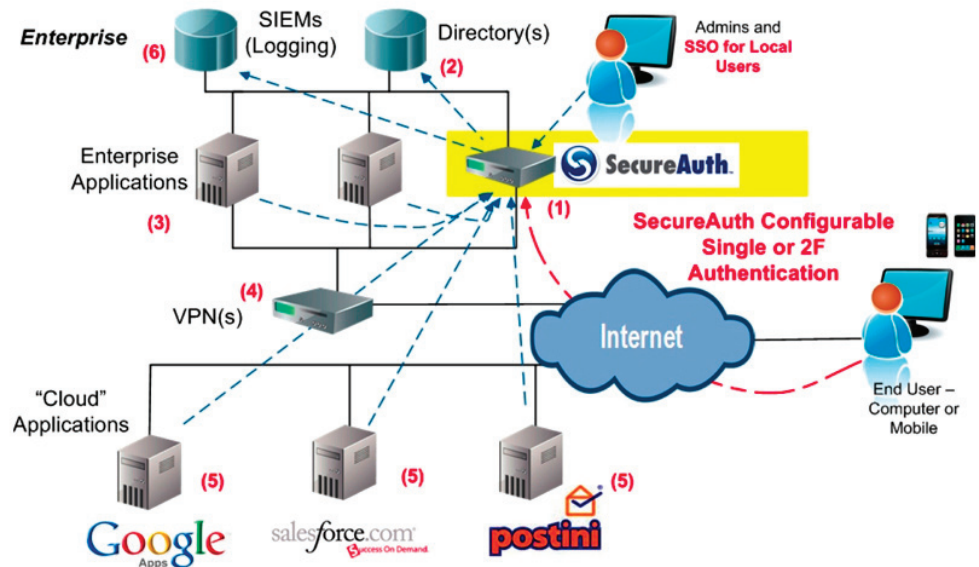
Because SecureAuth is conducting the authentication, a more secure second-factor authentication is enforced.

The way this works is that the SecureAuth IEP STS receives an authentication request and verifies the identity against the local user store (Active Directory, etc.). It then asserts the identities to local Web, VPN, and SaaS and cloud resources. Most importantly, SecureAuth IEP conducts the authentication locally and logs to the enterprise logging resource collector.



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

SecureAuth (1) allows you to assert the authentication for your internal and external users from your directory (2), to your on-premise Web applications (3), to your network devices (4) and to your SaaS resources, (5) and then log the entry locally (6).



In addition, the SecureAuth IEP also includes comprehensive IdM functionality that connects to local resource, maps local IDs, groups, attributes and provides self-service end user enrollment.

SecureAuth's Security Token Service is one of many functions of the SecureAuth Identity Enforcement Platform which provides Identity Enforcement plus 2-factor authentication, SSO, and IdM services in a single solution.

Why Is SecureAuth IEP STS Better than Alternative Methods?

This is a simple question with a simple answer. With SecureAuth IEP STS, you don't need to cobble together various solutions to deliver access to a range of applications. You don't need several different vendor solutions that you have to get to work together. You don't even need different solutions from the same vendor. Finally, should user credentials get lost, need to be reconfigured or if new types of applications must be rolled in, you only have one point of contact for support.

To sum up: 1 vendor + 1 solution + 1 support team = complete, consistent federation

Only SecureAuth IEP delivers all of that in a single, appliance-based solution.

Conclusion

Organizations need next-generation authentication and identity enforcement solutions in order to keep up with next-generation computing environments, such as SaaS, cloud and mobile applications.

Many organizations are investigated Security Token Services (STS) to address this need. STS is a good start, but unfortunately, many STS solutions are only partial solutions.

In order to provide secure, convenient access to cloud, SaaS and even on-premise applications in a unified, consistent way, STS services must be able to: 1) map user identities from internal directories to applications and resources 2) provide flexible authentication workflows, 3) positively assert an identity in a standardized format (such as SAML) to an application (or other resource) after authentication and 4) log event for compliance.



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com

The most successful STS solutions are actually not discrete solutions at all. Next-generation Identity Enforcement Platforms include STS as a feature, and deliver far more complete solutions. IEPs, such as SecureAuth, deliver complete access and identity enforcement solutions for applications anywhere, accessed by any type of user, anywhere, and on any type of device.

SecureAuth IEP includes a Security Token Service, 2-Factor Authentication, SSO, and IdM in a single solution to make it secure and simple for end-users to access cloud and on-premise applications and resources.

SecureAuth IEP is not just for cloud or SaaS environments. While SecureAuth IEP is designed handle public, multi-tenant cloud applications, such as Google and salesforce.com, it is also equally adept at securing private clouds from the likes of Terramark and Rackspace, as well as applications in Platform as a Service (PaaS) environments, such as Amazon Web Services and Microsoft Azure – all while securely handling on-premise applications too. All of your applications, no matter where they are, are handled together as if it all were one big infrastructure.

Now, business decisions can determine where your applications reside, rather than security obstacles. With SecureAuth IEP, you can run each of your applications where it makes the most sense from a cost, security and logistical perspective.

Try SecureAuth IEP Today! Contact SecureAuth to see if you qualify for a no-cost proof of concept. Unlike other solutions, which require heavy coding and re-architecting, SecureAuth IEP is an appliance that can be dropped into many networks in an hour or two. Even large, complicated networks can be accommodated usually in a couple of days.

Visit <http://www.gosecureauth.com/contact/free-trial.aspx> to request a no-cost, no-obligation proof of concept and free trial. Or call (949) 480-9465 to speak to a representative.

About SecureAuth Corporation

SecureAuth is the market leader in identity enforcement for all cloud, web, VPN, and mobile resources. SecureAuth makes it safe and simple for organizations of any size to extend their enterprise to the cloud. With SecureAuth, organizations of all sizes can increase end-user productivity with transparent access to multiple applications, shore up security with bilateral authentication, and reduce administration with self-service user provisioning and password reset. Unlike standalone SSO and authentication products, SecureAuth is known world-wide for its all-in-one Identity Enforcement Platform, SecureAuth IEP. SecureAuth IEP delivers integrated 2-Factor Authentication, SSO, and IdM for less than the cost of a token-based solution. Strategic partners and customers include leaders in finance, government, healthcare, manufacturing, retail, technology, and services.

Visit www.gosecureauth.com for additional information.

SecureAuth, SecureAuth IEP and the SecureAuth logo are registered trademarks of SecureAuth Corporation. All other products or company names mentioned herein are trademarks or registered trademarks of their respective owners.



Corporate Headquarters
8965 Research Drive
Irvine, CA 92618
949 777 6959
www.gosecureauth.com