SSO/Rest:

Bringing Traditional Web Access Management to the Cloud

A White Paper

"Web Access Management in the Cloud Does Not Exist"

Conventional wisdom holds that full Web Access Management, with real-time enforcement of security policies and a seamless Single Sign-On user experience, simply cannot be done in the Cloud.

Many believe that you just can't migrate on-premises apps to the Cloud in a cost effective, minimally invasive way while preserving your existing WAM integrations.

You may even have been told that Federation is the only path to Single Sign-On in the Cloud.

Until now, this might have been true.

Enter SSO/Rest.

SSO/Rest, an innovative solution from IDF Connect, bridges the gap between traditional, on-premises WAM and new cloud-based infrastructures and applications, giving legacy-bound IAM leaders a feasible path to the Cloud.

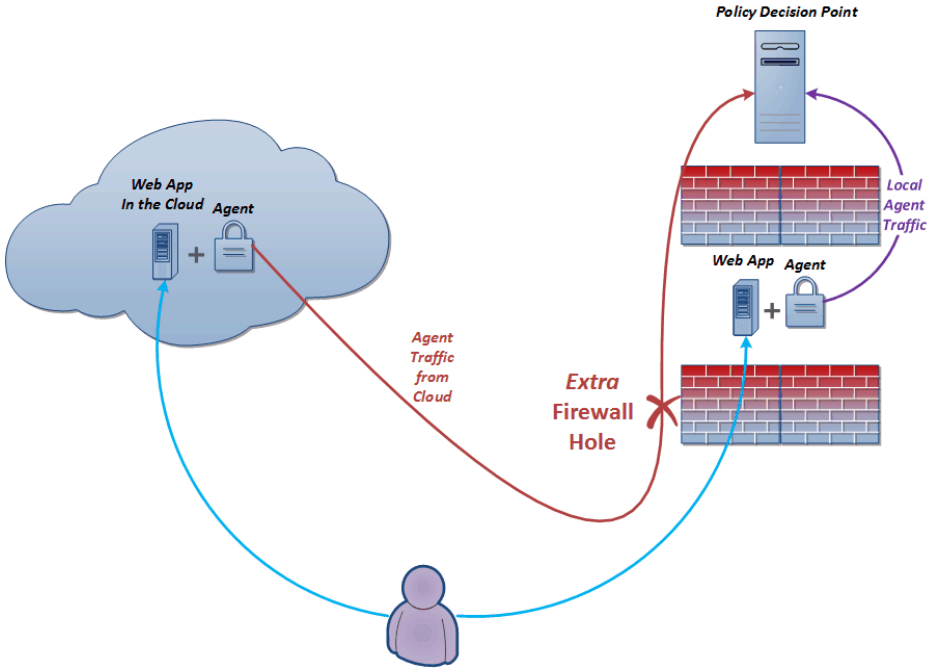
The Challenge

Today's IAM decision makers require the capability to quickly and cleanly migrate on-premises apps to the Cloud, or from one Cloud to another, without impacting users. They need to extend their enterprise's security perimeter to the Cloud, creating a virtual wall of security policies and enforcement for their Cloud-based assets. They want to preserve the full WAM capabilities already deployed on-premises, and must maintain the seamless SSO experience enjoyed by their users. And they want to accomplish all of this in a cost-effective, minimally-invasive way.

Most veteran enterprises, however, face a major obstacle when trying to extend their WAM solutions to the Cloud. The essential problem is that all mainstream WAM products predate the Cloud and rely on technologies that are fundamentally cloud-incompatible. These tools are quite effective within the environment for which they were designed, but were never engineered to function with off-premises systems.

Heavyweight WAM agents just aren't built for the Cloud.

Specifically, all pre-Cloud SSO products depend on heavyweight agents or proxies. These powerful yet often cumbersome software products provide perimeter authentication and access control enforcement, logging people into applications and intercommunicating using vendor-specific, proprietary protocols. When attempting to use these WAM agents or proxies in the Cloud, their "heaviness" degrades performance with the increased network latency. Worse, their reliance on non-standard protocols requires enterprises to open network tunnels or punch new, unsafe holes through multiple layers of firewalls. They simply cannot be implemented in cloud-based applications without significant loss of WAM functionality, complication of perimeter safeguards, and interruption of smooth user experience.



WAM Agents do not work well in the Cloud

True, there are SSO solutions that run in the Cloud. Mainly these are federation brokers that work by exchanging federation tokens (e.g. SAML, OAuth, OpenID/Connect) between sites. These solutions are fine for many purposes, but it is important to recognize that federation alone provides only a subset of the functionality that an enterprise Web Access Management solution provides, namely Single Sign On. They do not provide real-time access control enforcement or centralized access policies. Session management, such as timeout enforcement and logoff capability, is limited, and by the very nature of federation, comprehensive audit and governance of end-user activities are very difficult. Federation requires programmatic implementation and enforcement by individual apps, so is in some ways less turnkey than the perimeter enforcement afforded by agents or proxies. **For enterprises running applications that require these security controls, removing WAM and replacing it with federation is a step backwards**.

Most well-established enterprises therefore find themselves in a bind: they need the benefits of the Cloud but have already fully-deployed on-premises Web Access Management solutions like CA SSO (formerly known as SiteMinder), Oracle Access Manager, IBM Tivoli Access Manager, or OpenAM. These venerable tools are established and may be working perfectly well. For these organizations, the operational invasiveness, financial cost, and loss of key WAM functionality involved in uprooting and replacing these existing solutions makes a simplistic switch to an all-Cloud, federation-based solution highly problematic.

Removing Web Access Management and replacing it with federation can be a step backwards.

So, is there a way for the IAM decision makers of such enterprises to successfully expand their WAM implementations to the Cloud – *without* compromising centralized management capabilities, interrupting smooth user experience, and ripping and replacing entirely adequate on-premises SSO?

Fortunately, the answer is yes – with SSO/Rest, an innovative solution from IDF Connect.

SSO/Rest is a minimally-invasive way to push applications into the Cloud with the full benefits of Web Access Management

IDF Connect developed SSO/Rest explicitly to provide a minimally-invasive way for enterprises to push applications into the Cloud while seamlessly protecting them with the full power and capabilities of their WAM platform as if they were still in their own data center. SSO/Rest currently provides this capability for CA SSO, with support for Oracle AM and a standalone XACML-based policy engine also in the works.

SSO/Rest is an easy-to-implement protocol that delivers *full* CA Single Sign-On functionality through a simple HTTP-based RESTful interface that has been hardened and secured to safely work in the Cloud. Crucially, its lightweight enforcement plugins, which are drop-in replacements for "traditional" agents, mean that it allows enterprises to bypass the onerous implementation pitfalls which plague other potential solutions, such as latency, firewall rules, VPN tunnels, or even vendor-lock.

WAM gaps in the Cloud solved by SSO/Rest

SSO in the age of the 'Virtual Perimeter'

From the architectural perspective, the challenge posed by moving our WAM-enabled apps to the Cloud is all about the ***perimeter***. In information security, the perimeter is the boundary that ensures all requests reaching protected applications are properly vetted and audited.

Traditional perimeter-based security controls are no longer sufficient. Today we need virtual perimeters.

Earlier generation, on-premises SSO complied with the *physical* perimeter approach to enterprise security that was the state of the art at the time, namely the use of firewalls to build a wall between the 'trusted' inside and the 'untrusted' outside. But as the Cloud formed, the effectiveness of the traditional approach began to degrade. Enterprise application and data resources started to appear outside the enterprise perimeter – no longer as secure, despite needing the same or even more stringent security policies as on-premises resources. Gradually the perimeter began to lose its purpose and eventually its meaning. In today's IT reality, "inside" is untrusted and "outside" is downright hostile – if you can even distinguish inside from outside any more. **While traditional perimeter-based security controls are still necessary, they are no longer sufficient for securing the modern enterprise**.

To safeguard their entire digital landscape, today's enterprises must implement *virtual* perimeters – software-defined and policy-controlled, allowing both people and software assets to be located anywhere the business needs them to be, while still affording them the ability to centrally control, monitor, and audit access to those assets. At the heart of this reinvention of the perimeter: cloud-based Web Access Management.

And SSO/Rest, by enabling enterprises to extend on-premises Web Access Management to the Cloud, is an essential part of this virtual perimeter.

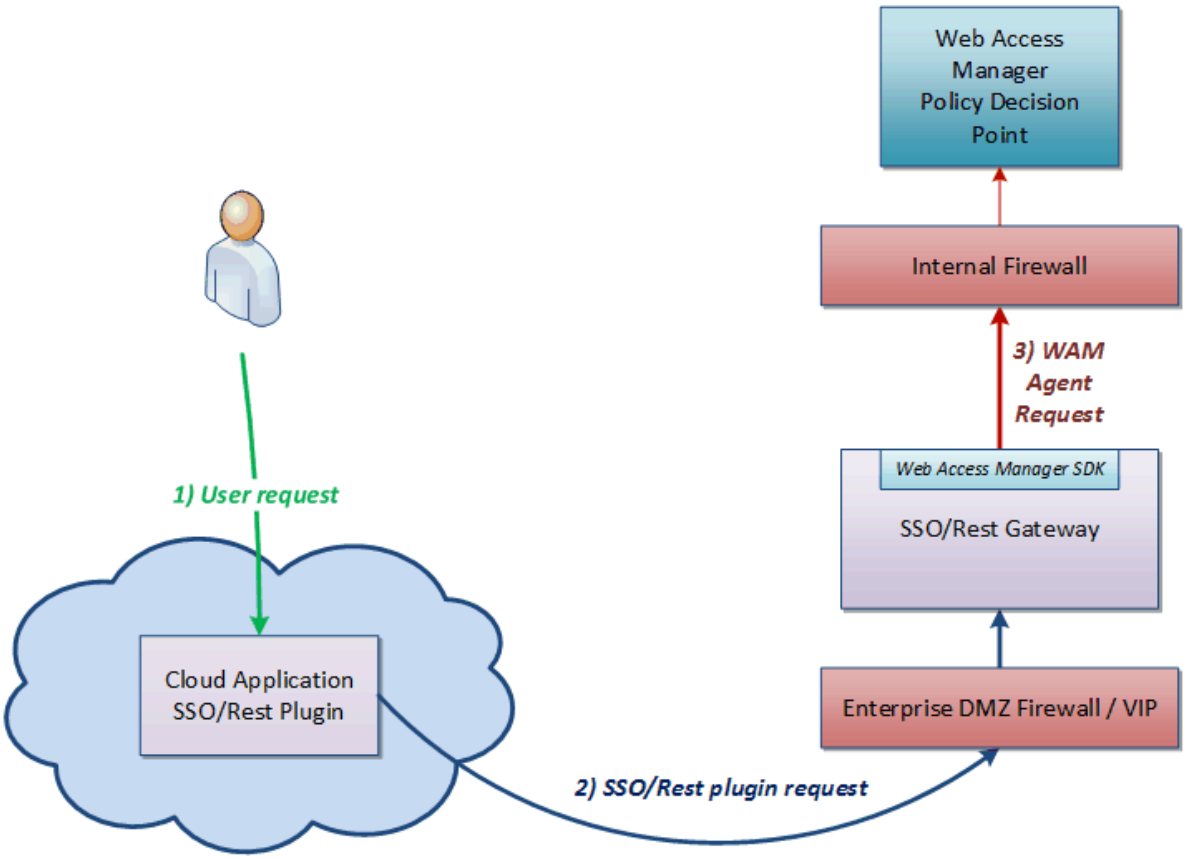
Protecting Apps from On-Premises to the Cloud

How does SSO/Rest allow enterprises to extend their perimeter to Cloud-based assets, without forcing them to uproot what is already working just fine for on-premises systems? It achieves this by providing full Web Access Management *as a set of REST-based Web services*. SSO/Rest provides lightweight, drop-in replacements for agents (the SSO/Rest *plugins*) that communicate via RESTful, HTTPS-based interactions. Because of the plugins' small footprint and HTTP-based communication (which means no new firewall ports!), enterprises can deploy them on applications both inside and outside the enterprise perimeter, thereby creating a virtual perimeter to encompass any cloud-based services the organization wishes to secure. The hardened SSO/Rest Gateway sits protected in the enterprise DMZ, securely mediating communication between the plugins and Policy Decision Points (PDPs, such as CA SSO Policy Servers).

SSO/Rest's lightweight plugins let you build a virtual perimeter.

In addition, SSO/Rest plugins don't perform any processor-consuming cryptographic operations or token validations (these are deferred to the SSO/Rest Gateway), which makes the plugins resistant to zero-day vulnerabilities. As a result, applying patches to the plugins is infrequent and rarely urgent, significantly lightening the burden on security patching and breaking (once and for all!) the endless "agent upgrade" cycle.

Furthermore, the plugins are self-contained (requiring no external code libraries) — which, most importantly, enables admins to either install them either at the server level (like traditional, heavyweight agents), or *bundle them directly into applications*! The bundling option is especially important in PaaS (Platform-as-a-Service) environments such as Microsoft Azure or Google App Engine, where installing a heavyweight agent at the web server level is off-limits anyway. The diagram below shows what this looks like with CA SSO:



The SSO/Rest Solution

It's important to note that none of the interactions in the diagram above use federation tokens such as SAML or OAuth. We are all familiar with federation-based login mechanisms, of course - if you've ever logged into a web site using your Facebook ID (or Twitter, LinkedIn, or Google IDs, for that matter), then you've used token-based federation. Federation technologies are "claims-based": user identity, authentication information, and optionally roles and entitlements are issued within the ticket (the "claims"). It is the responsibility of the consuming applications to use these claims properly.

A tighter perimeter is especially crucial for applications with higher security requirements

Federation architecture is perfectly fine for many applications, especially those that are consumer-oriented or don't otherwise have strict security and compliance requirements. Enterprises, however, frequently require more fine-grained control over access policies – including their creation, enforcement, and auditing – than federated login systems can easily provide. Perimeter enforcement enables this functionality by performing *direct* access control enforcement. **A tighter perimeter is especially crucial for applications with higher security requirements**; e.g. online banking, ERP apps, PCI-related apps, etc.

With perimeter enforcement, administrators can assign fine-grained policies to individual users, store them in the on-premises PDP (as in the diagram above), and enforce them at the Policy Enforcement Point (PEP), which is the SSO/Rest plug-in. The result: fine-grained policy control, cloud-friendly WAM, and a seamless user experience — all without having to rip-and-replace your on-premises SSO.

Strategic Business Benefits of IDF Connect SSO/Rest

As is the case with most organizations, IDF Connect has one foot in the modern, cloud-centric, software-defined digital world, and the other in the traditional, on-premises enterprise IT environment. Large, established enterprises simply cannot (and should not!) try to entirely transform their entire infrastructures overnight in the push to get to the Cloud. IDF Connect recognizes this practical reality and has, with SSO/Rest, built a bridge that enables a smooth, manageable path to the Cloud for enterprises that rely upon on-premises SSO.

SSO/Rest is a bridge to the Cloud for enterprises that rely upon on-premises SSO.

SSO/Rest, by providing comprehensive WAM as a service through easy-to-install, lightweight plugins and a specially-engineered protocol, allows enterprises to have the best of both worlds. SSO/Rest provides IAM leaders with a way for their enterprises to reap all the benefits of Cloud technology without having to significantly re-engineer or migrate their on-premises systems, diminish centralized management capabilities, or degrade the end-user experience. **By neatly solving the Web Access Management integration issues between the on-premises enterprise WAM controls and the Cloud, SSO/Rest significantly lowers the cost and barriers to entry for enterprises into Cloud computing**.

The bottom line is this: splitting the SSO strategy into on-premises and Cloud doesn't meet the needs of users. Ripping out the on-premises SSO to move entirely to the Cloud is rarely the most cost-effective, business-driven choice. The better option is to extend SSO to the Cloud while maintaining the usability and centralized management that users and admins require. IDF Connect makes that option a reality.

About IDF Connect

IDF Connect solutions and services for Identity and Access Management help enterprises and other large organizations enable IAM for cloud-based applications. Our solutions are specially engineered to bridge the gap between traditional "on-premises" IAM technologies and new cloud-based infrastructures and applications.

IDF Connect's product suite allows enterprises to leverage all the benefits of Cloud technology without significant re-engineering or migration of on-premises systems. IDF Connect's technology effectively lowers the cost and barriers to entry for enterprises into Cloud computing by solving the IAM integration issues between the on-premises enterprise IAM controls and the Cloud.

Our Vision

Our company vision is to offer IAM technologies that lower the costs and barriers to entry for Cloud computing. Our product suite enables organizations to leverage public cloud infrastructure by extending the reach of your existing IAM solutions, and our managed services bring enterprise-grade IAM solutions to Cloud customers.

IDF Connect, Inc.
2207 Concord Pike #359
Wilmington, DE 19803
Phone: (888) 765-1611
Fax: (888) 765-7284

www.idfconnect.com

@IDFConnect
@rsand2

www.linkedin.com/in/rsand

www.facebook.com/IDFConnect