

THE OPTIMALCLOUD FOR CLOUD BASED APPLICATION VENDORS





Background:

More and more IAM vendors are taking what they classically sold as an on premise solution and delivering their applications via the cloud.

While this makes a lot of sense both for the vendors as well as their customers, it does introduce a problem with authenticating users.

With the on premise solutions, they likely used Windows integrated authentication for web applications to seamlessly log the customer's users into their web application, or they simply authenticated using the customers on premise Active Directory.

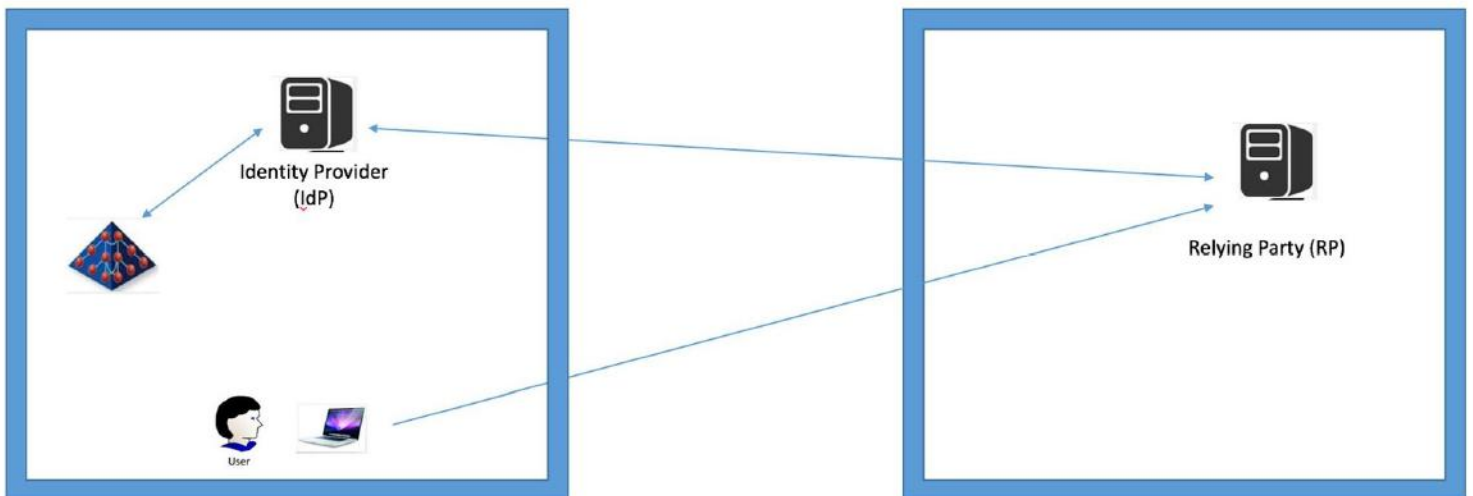
"While this makes a lot of sense both for the vendors as well as their customers, it does introduce a problem with authenticating users."

Identity Federation and Single Sign-On (SSO)

Now that web applications are hosted in the cloud, how do these cloud applications authenticate the users? One answer is to create separate user accounts and passwords into the cloud application. This works, but is not user friendly because users now have another account and password for each cloud application. With a SSO approach, the user is able to use their existing corporate credentials to access the cloud applications without requiring separate accounts for each application.

The industry standard to provide this Single Sign-On is known as Federation, or Identity Federation. Identity Federation is where two organizations establish a trust between two security realms. A federation server on one side (Identity Provider or IdP) is responsible for authenticating the user and issuing a token. A Federation server on the other side (Relying Party or RP) accepts the token and validates the token containing the identity of the authenticated user. A rely party (RP) is the term in Federation for the cloud based application that the end user is accessing.

When the user attempts to access the cloud application (RP), the user is redirected back to their company's IdP to authenticate with their existing corporate credentials.



Conclusion:

This setup provides controlled access to applications by authenticated users without requiring the user to have another account and password within the cloud application.

Protocols, Trusts, Certificates, Assertions, Encryption, Signing, Oh My

Now that we've determined that Federation is the right solution, the only thing left to do is build Federation support into the cloud SaaS application, right? The answer is not that simple. While Identity Federation is built on open standards there are many moving parts.

Identity Federation is simply the broad term for how the single sign-on is performed.

The first item that must be decided and agreed upon by both the IdP and the RP is what protocol to use. Think of the protocols as different languages. In Federation the most common standards are WS-trust, WS-Federation, SAML 1.0, SAML 2.0, and Shibboleth. As an application vendor are you going to add support for all of these so that customers can choose the protocol they want to use?

The complexities continue with having to decide technical details such as what data elements should be sent in the assertion, the details around signing and encryption, as well as the trading of SSL certificates. Things get even more complicated if the customer does not have a certain data element you need or have it stored in attribute named something different.

All of these items need to be ironed out for each and every federated trust with a new customer.

That, however, is not the biggest issue. The biggest issue is the ongoing and growing cost to continue to maintain and grow an increasing infrastructure of a Federation service. As you add new customers, you add additional cost and maintenance of your service. Beyond server maintenance, patching, and monitoring, certificate maintenance is a huge manual task in and of itself. Certificates often have an expiration of 1 to 2 years, at which time new ones need to be manually generated and traded between IdP and RP.

Simply Put,

YOU ARE NO LONGER JUST IN THE BUSINESS OF WHAT YOUR CLOUD APPLICATION DOES. YOU ARE NOW IN THE FEDERATION BUSINESS, RUNNING A GLOBAL AUTHENTICATION SERVICE THAT IS CONTINUOUSLY GROWING BOTH IN COMPLEXITY AS WELL AS COST. THE GOOD NEWS IS THAT IT DOESN'T HAVE TO BE THAT WAY.

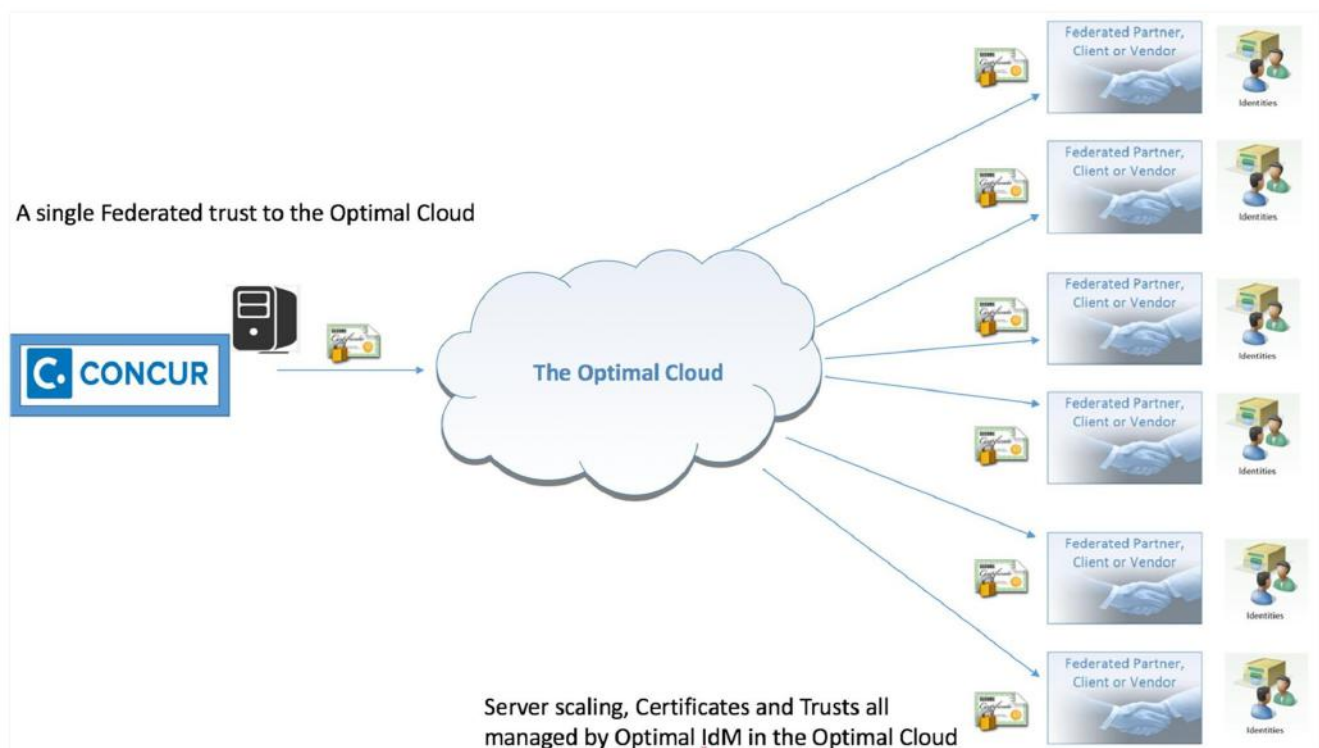


The OptimalCloud - Your cloud, Your Way

With The OptimalCloud, any cloud based application can deliver their Software as a Service (SaaS) application with the benefit of Single Sign-On (SSO) to their customers without the hassle of dealing with setting up and configuring Federation with each of their customers.



With a single Federated trust from the SaaS provider to The OptimalCloud, the cloud application can now provide SSO quickly and easily to all of the applications customers.



Contact us at sales@optimalidm.com or learn more at www.optimalidm.com

With The OptimalCloud:

- You get a private, dedicated cloud Federated broker for all of your customers
- You get a custom, private cloud that adapts to your needs instead of you adapting to it
- You get scaling and growth with NOTHING to do on your side
- No need to add servers geographically around the globe
- No need to worry about name mappings
- No need to upgrade and change certificates for each customer once or twice a year
- No need to create and manage federated trusts with each and every customer
- No need to troubleshoot why customers are not federating properly
- Get your customers up and running quickly, easily and painlessly! – We are Federation experts.
- Easily support features such as SCIM without having to scale hardware to handle the volume
- You have one single Federated trust – to The OptimalCloud.
- You never have to worry about Federation again, lower costs and nothing to manage

Get out of the Authentication Business

Adding Federation support to both on premise and cloud applications makes perfect sense. It provides your customers with SSO and is all built on open industry standards. Does it make sense, however, for you to build out an entire global Federation service infrastructure complete with banks of servers, redundancy, load balancing, monitoring, support and maintenance?

Optimal IdM does not believe that you want to be in that business. You are in the business you are in, whether that is cloud based logging and monitoring or a cloud based expense reporting system. That is why we believe that cloud based application service providers should use The OptimalCloud service for their Federation service. It is precisely what we do for our global customers who utilize our Federation service so they don't need to build a complicated, expensive and infrastructure that must be constantly managed and maintained. They outsource that to us. It is what we do and we do it very well.

Pricing Model

The OptimalCloud is the only cloud federation and single sign-on solution priced at a flat affordable monthly fee which is ideal for large complex enterprise organizations. Anyone dealing with enterprise-level companies knows that a per user, per month fee can quickly add up and makes it difficult, if not impossible to afford.

If you are using an on premise Federation solution, they may charge you a hefty fee per Federated trust. With The OptimalCloud it is a simple flat monthly fee. Using a flat monthly fee, the service is affordable, allowing you to offer Single Sign-On to your customers without the expensive cost and headache of building and maintaining an authentication service.

Contact us at sales@optimalidm.com or learn more at www.optimalidm.com

Conclusion

With The OptimalCloud you have a scalable, completely outsourced Federation cloud based system that scales to your needs and allows you to focus on what your business does best. Bottom line, it makes a lot of sense to add Federation support to your solution, but does it make sense for you to run a Federation service? Come to The OptimalCloud and turn all of that management over to us, the Federation experts. We hope that this white paper provided you with just a few of the reasons that customers are selecting The OptimalCloud.

Millions of users worldwide depend on our solution for their authentication needs and so should you.



Contact us at sales@optimalidm.com or learn more at www.optimalidm.com