

5 Things to Keep in Mind when Choosing a Single Sign-On Solution



Content

Move to Hybrid Cloud and SaaS.....	3
Single Sign-On and Remote Network Access.....	6
Secure User Identity when Accessing SaaS Applications	7
Integration with Multi-Factor Authentication (MFA) Mechanisms.....	8
Fits in the Existing Customer Environment	9
Monitoring and Troubleshooting Tools	10
Introducing Citrix Gateway for Single Sign-On visibility	11-14

Move to Hybrid Cloud and SaaS

Applications are evolving every day. Enterprises are moving from traditional client-server architecture, or locally installed applications, to more distributed architectural frameworks. Now locally installed applications and traditional client-server applications are being replaced by virtual applications that are streamed to end user devices or applications delivered as a service (SaaS) that are easier to manage and are part of a hybrid cloud infrastructure. Having said that, traditional applications, like web and enterprise applications, still have a majority of the application footprint. As a result, enterprise customers not only have to ensure the secure delivery of these new forms of applications, but they also need to maintain the delivery of traditional applications, which are vital to their end users.

In effort to securely deliver access to these different application types, a plethora of vendors have gone to market with single sign-on solutions for one or a subset of application types. Some traditional vendors offer SSO to on-premise applications, while a new generation of IDaaS vendors offer SSO to cloud and SaaS applications only. Given that enterprise customers have a need to securely deliver all of their apps whether in a datacenter, cloud or delivered as SaaS, they typically have no choice but to go with a multi-vendor solution to cover the complete landscape of their application types.

A single sign-on solution is meant to reduce cost of management, provides better security and an improved user experience.

However, most multi-vendor solutions fail to deliver these advantages due to their redundancies, costly investment price, the amount of resources required to manage them and poor integration, which leads to user experience issues and reduced productivity.

With the wide array of application types that are now part of most enterprise customer infrastructures, organizations are looking for the most efficient and effective way to deliver access to these applications—end-to-end—regardless of their location.

This eBook will identify the **5 things you should prioritize** when selecting a single sign-on solution to overcome these challenges.

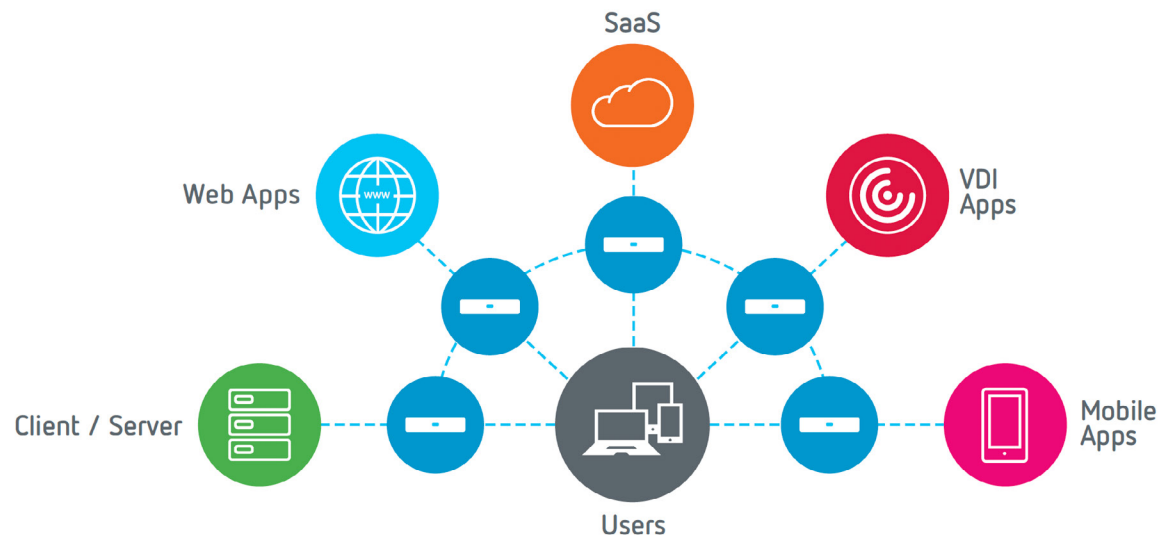


5 Things to Prioritize when Choosing a Single Sign-On (SSO) Solution

1. Single Sign-On and Remote Network Access to Any Application in the Datacenter or Cloud

Applications are deployed in a datacenter, a cloud or as SaaS. Every business application requires users to be authenticated before they are given access to a resource. In the pre-SSO days, every time a user needed to move between applications, they had to login with a set of credentials. Most of the time, every application had a separate set of credentials and it resulted in poor user experience, failed logins as a result of forgotten credentials, inconsistent access control policies, and higher cost to support these applications. That said, SSO solutions changed the way users interact with and access their applications.

Most of the vendor solutions today provide SSO, but are limited in the scope of application landscape they cover. Some of the on-premises solutions provide SSO to web and enterprise applications but cannot do the same for VDI or SaaS applications. On the other hand, some of the IDaaS vendors provide SSO to cloud and SaaS applications, but cannot do it for applications that are on-premises. Complicating matters, none of the traditional SSO or IDaaS vendors have a solution to provide access to network resources like network fileshare, etc.

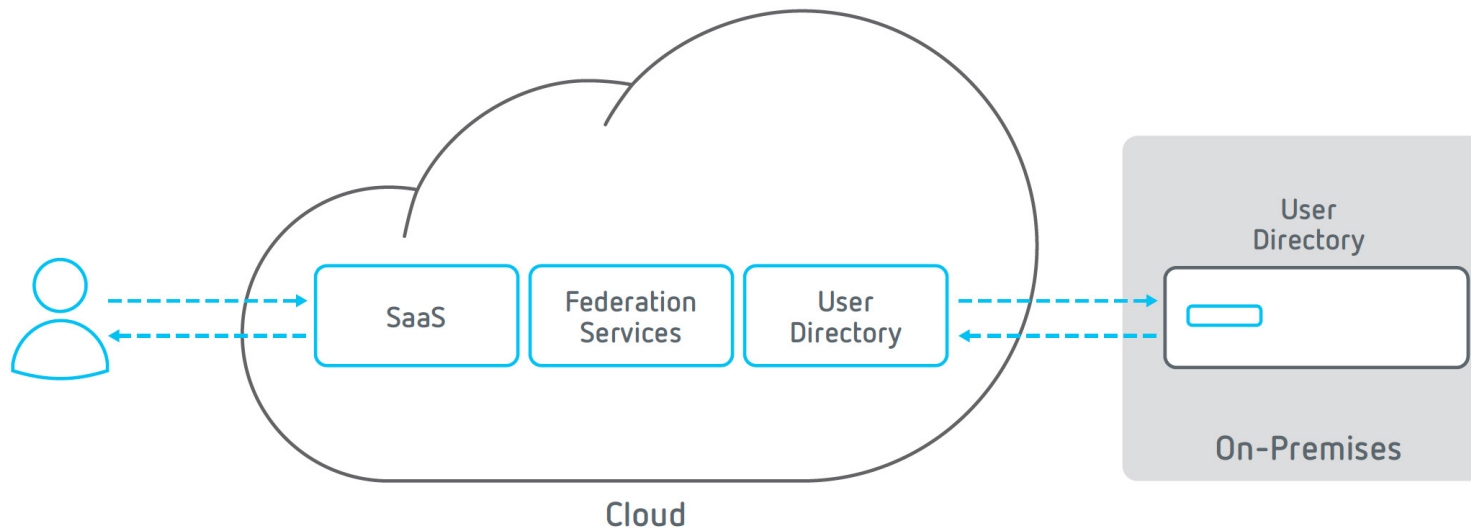


A solution should provide SSO to all applications irrespective of whether it's a VDI (Citrix Virtual Apps, formerly Citrix XenApp, Microsoft RDP, VMware Horizon), web (SharePoint, etc.) or an enterprise application (OWA) deployed in a datacenter or cloud; or a SaaS application like Office 365, Salesforce, Workday etc. and provide a complete network access for users looking to access data from a remote location.

When evaluating an SSO solution, you should prioritize the capability to not only provide SSO experience across all VDI, enterprise, web and SaaS applications but also network access to other corporate resources like network fileshare etc.

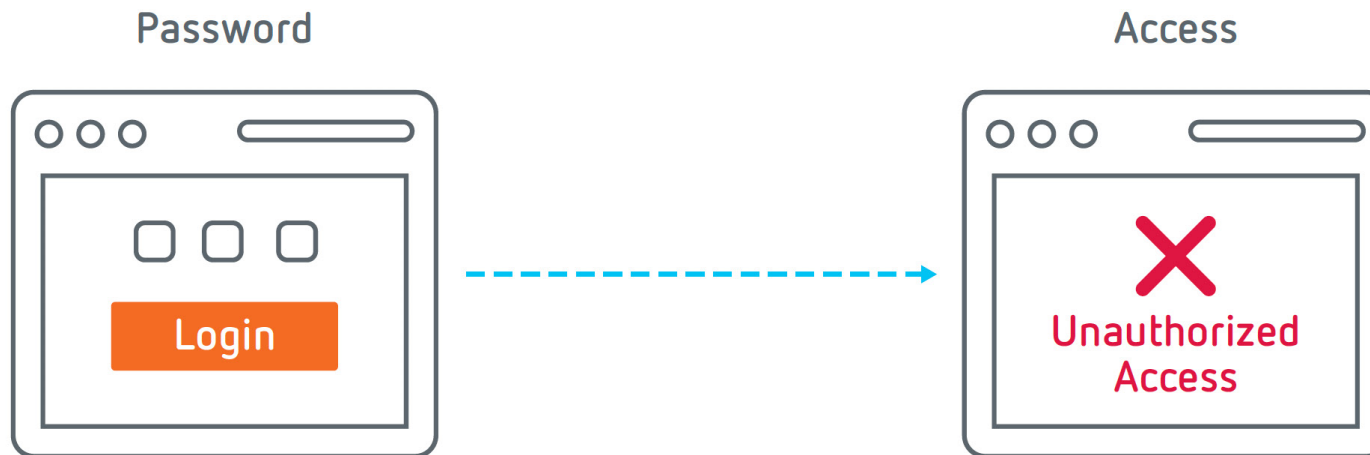
2. Secure User Identity when Accessing SaaS Applications

SaaS applications like Office 365, Salesforce, Workday, ADP etc. are getting a lot of traction from enterprise customers. Since these applications are delivered from a cloud and are outside of the datacenter network, to achieve SSO to these applications, most of the solutions require customers to move their user directory to cloud. This, to many enterprise customers, is a concern and a high-risk task for any enterprise. This is why you should look for a solution that allows you to keep user directory on-premises.



3. Integration with Multi-Factor Authentication (MFA) Mechanisms

User authentication is becoming very important, especially in light of BYOD and the rise of users working from remote locations. Many enterprise customers also have a need for their partners and contractors, who are not a part of local user directory, to access their business applications from remote locations. This makes it crucial to quickly and rightfully identify the user and authorize their access to corporate resources. Enterprise customers, therefore, should not rely on just username and passwords but should also look for a solution that provides flexibility to use authentication schemes based on the state of end user device, user location, application they are trying to access, etc. This makes it important to select an SSO solution that supports any authentication mechanism as well as authentication protocols like RADIUS, Kerberos, Microsoft NTLM, Certificate Services, etc.



4. Fits in the Existing Customer Environment

An SSO solution has a lot of touchpoints in a customer environment. Starting from a user directory, to authentication mechanisms, to integrating with applications as well as end user devices. Finding a solution that is easy to integrate with your existing environment is crucial. Making the wrong choice may result in huge costs down the road, and lead to poor end user experience.

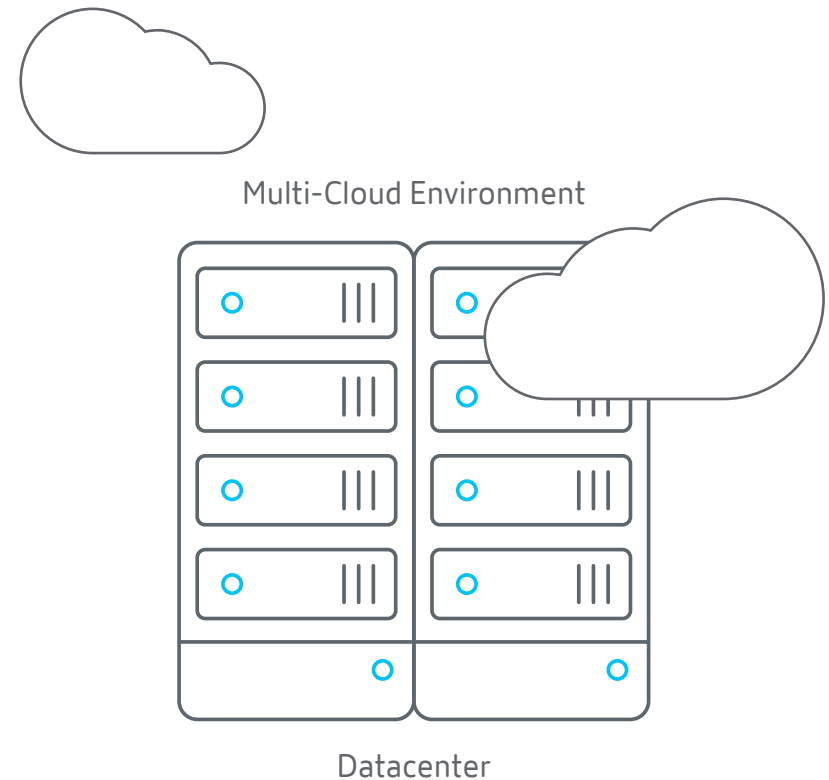
The SSO solution you select should support the following:

- ↓
All end user devices
(Windows, Mac, Linux,
iOS and Android)
- ↓
All authentication
mechanisms (RADIUS,
Diameter, Kerberos,
Microsoft NTLM, TACACS,
form-based, etc.)
- ↓
All SSO protocols
(SAML, OAuth, OpenID)

- ↓
Configurable application
portal pages per the
customer branding
and colors

5. Monitoring and Troubleshooting Tools

Increased productivity is probably the biggest value add of an SSO solution for end users. In the current IT environment, especially with proliferation of BYOD and mobile, users and employees want to access applications from anywhere, using any device. While this enables them to be more productive, it also increases the probability of errors and issues that can affect the user experience and user productivity. In most enterprises, IT has defined strict SLAs, but with multiple vendors providing SSO to different applications, it is hard for them to refer to multiple monitoring tools and be able to resolve issues quickly. This is why you should prioritize an SSO solution with monitoring tools that look across these issues for all applications irrespective if they are in a datacenter, cloud or delivered as SaaS.





Introducing Citrix Gateway for Single Sign-On

Citrix Gateway, formerly NetScaler Unified Gateway provides Single Sign-On to applications in the datacenter, cloud or delivered as SaaS.

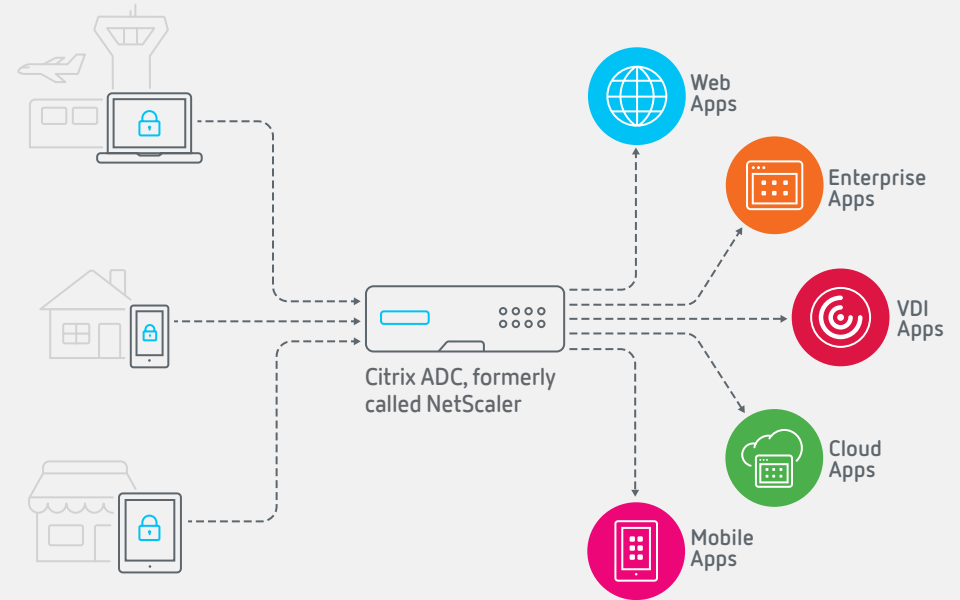
It consolidates your remote access infrastructure and allows users to access any app, from any device, securely. It delivers all of the key features you need for a future proof solution, including:

- ✓ Provides Single Sign-On (SSO) Access to All Applications
- ✓ SAML Based Federated Identity and On-Premises User Directory
- ✓ Multi-Factor Authentication
- ✓ A Tight Fit to Your Existing Environment
- ✓ Monitoring and Troubleshooting Tools



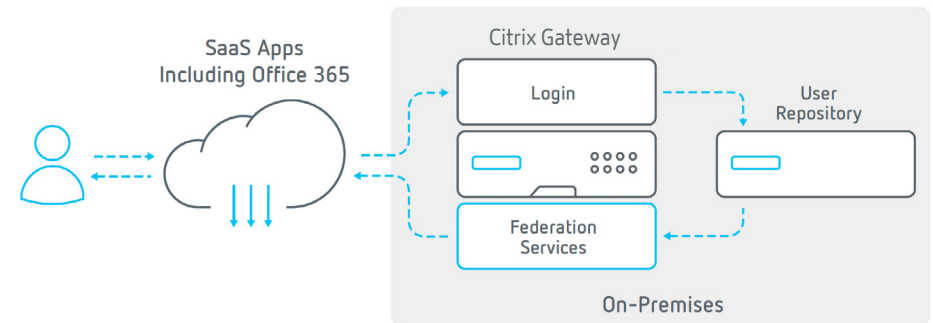
Provides Single Sign-On (SSO) Access to All Applications

These can be VDI applications (Citrix Virtual Apps and Desktops, formerly Citrix XenApp and Citrix XenDesktop, Microsoft RDP and VMware Horizon), web applications (SharePoint, Internal employee portals etc.), enterprise applications (Outlook etc), or a SaaS application (Office 365, Salesforce, Workday etc.). It also provides a comprehensive SSL VPN based remote access to networks for users looking to access network resources from a remote location.



SAML Based Federated Identity and On-Premises User Directory

Enterprises can migrate applications to the cloud and continue to authenticate users exclusively against an on-premises enterprise directory. Citrix Gateway accomplishes this through identity federation, using internal SAML or ADFS federation services to provide the cloud service with a secure trusted token containing a series of claims about the authenticated user, including his or her identity, that are in turn validated by the cloud services own federation services.





Multi-Factor Authentication

Citrix Gateway integrates with and supports all authentication mechanisms and protocols. It provides a very flexible and a policy based authentication framework that allows IT admins to create dynamic policies for authenticating end users.



A Tight Fit to Your Existing Environment

Citrix Gateway enables you to have just one solution for all your remote access and SSL VPN requirements, allowing it to tightly fit to your current environment. Its flexible solution provides:

- A fully configurable portal for publishing applications
- Support for all end user devices from Windows, Mac, Linux to iOS and Android platforms
- Support for all authentication mechanisms and protocols (RADIUS, Diameter, Kerberos, Microsoft NTLM, TACACS, form-based, etc.)
- All SSO protocols (SAML, OAuth, OpenID)



Monitoring and Troubleshooting Tools

Since Citrix Gateway meets all requirements to provide SSO to all applications, it can provide the complete end-to-end visibility required for monitoring and troubleshooting issues related to application delivery, and user experience. With Citrix ADM, formerly NetScaler MAS, Citrix Gateway enables collecting metrics around Citrix Virtual Apps and Desktops performance (HDX Insight) as well as collecting user experience issues across all applications (Gateway Insight).



Your apps are evolving, and the only way to ensure true end-to-end secure Single Sign-On access and a seamless user experience to your users is with the right solution. Citrix Gateway is a future proof SSO solution with all of the features you need to support a distributed architectural framework while reducing cost, simplifying management, securing user identity and improving user experience, so you can say yes to the future of business.

Learn more about Citrix Gateway at citrix.com/gateway.



[Back to contents](#)