Single sign-on the way it should be

6 ways Citrix Workspace delivers seamless access to all apps while improving security and the user experience
Contents

Single sign-on (SSO) solutions .................................................................3
Secure access to everything .................................................................5
Granular controls for SaaS apps and the web ........................................6
Control over your user identity .............................................................7
Security beyond user names and passwords ........................................8
Seamless integration with your existing environment .........................9
Resolving issues faster with end-to-end visibility .................................10
Single sign-on (SSO) solutions were designed to make life easier for employees and IT.

They’re meant to reduce the cost of management and provide better security and an improved user experience. However, many solutions fall short, covering only one type or a subset of application types. This forces you to implement several SSO solutions from different vendors to cover your entire application landscape — negating the productivity and user experience benefits you hoped for.

Citrix Workspace helps you unify all apps and data across your distributed IT architecture to provide single sign-on to everything people need to be productive. Working with your existing infrastructure, Citrix Access Control, a key component of Citrix Workspace, consolidates multiple remote access solutions, simplifying management for IT and providing simple access for employees.
6 benefits of the Citrix Workspace SSO solution
1. Secure access to everything

Many SSO solutions are limited in the scope of the application landscape they cover. If you have a solution that covers only your virtual and enterprise apps, for example, you’d need a separate identity as a service (IDaaS) solution to provide access to your web and SaaS applications.

Citrix Workspace with Citrix Access Control gives you access to all your apps — plus other corporate resources, like network file shares.

SSL VPN-based remote access allows users to connect to network resources from remote locations, so they can be productive wherever they are. Citrix Workspace also includes MicroVPN technology for a secure connection to these resources on mobile devices.
2. Granular controls for SaaS apps and the web

Your SSO solution should go beyond basic access and provide you with granular, contextual controls over SaaS apps.

Unmonitored internet browsing also opens your organization up to risk. It’s not uncommon for some organizations to completely ban internet browsing, but this can hamper productivity.

Citrix Workspace with Citrix Access Control offers enhanced security policies for SaaS and web apps. Restrict actions like copy/paste, printing, and downloading. Gain control over the navigation bar, back/forward buttons, mobile access, and watermarking. You can blacklist and whitelist URL categories to allow or deny access to websites. You can also disable URLs launched from SaaS apps, and present unknown SaaS apps or web links in a secure browser to isolate them from corporate network or resources.

Citrix Access Control supports well-known SaaS apps — including SalesForce, G Suite, Office 365, Zoom, Workday, Expensify, and more — in its out-of-the-box catalog. You can use preconfigured application templates to easily publish apps and configure single sign-on policies.
3. Control over your user identity

SaaS applications like Microsoft Office 365, Salesforce, Workday, and ADP are becoming essential to how we work today. In fact, the average enterprise uses 1,427 distinct cloud services\(^1\).

To provide SSO to these apps, which are delivered from the cloud and are outside of the data center network, most solutions require you to move your user directory to the cloud. But with Citrix Access Control, you have the freedom to choose to keep it on-premises.

This is accomplished 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. These claims are in turn validated by the cloud services’ own federation services.
4. Security beyond user names and passwords

User authentication is becoming increasingly important, especially with more employees working from an array of devices and locations. Many organizations also have a need for partners and contractors, who are not a part of the local user directory, to access business applications and data from remote locations. This makes it crucial to quickly and rightfully identify the user and authorize their access to corporate resources.

For these reasons, Citrix Access Control doesn’t rely on just user names and passwords. It supports multifactor authentication, which allows IT to have granular control over who’s accessing the corporate network, what’s being accessed, when it’s accessed, and the device used to access it.

Citrix Access Control integrates with and supports all authentication mechanisms and protocols, such as RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0, and OpenID 2.0. It also supports Azure Active Directory for multifactor authentication, as well as on-premises Active Directory for two-factor authentication using native OTP.
5. Seamless integration with your existing environment

A single sign-on solution has a lot of touch points within your environment, from the user directory, to authentication mechanisms, to applications and even end user devices. Citrix Access Control easily integrates with your existing infrastructure so you can ensure a great user experience while simplifying IT management.

- Customize your front-end application portal with your organization's own branding

- Support all authentication mechanisms, including RADIUS, Diameter, Kerberos, Microsoft NTLM, TACACS, and form-based

- Support all end user devices, including Windows, Mac, Linux, iOS, and Android platforms

- Support all SSO protocols, including SAML, OAuth, and OpenID

Ease of integration with existing systems was the most important factor when considering enterprise authentication solutions.
6. Resolving issues faster with end-to-end visibility

Because Citrix Access Control provides access across your entire application landscape, it’s also able to provide the visibility you need to monitor and troubleshoot application delivery and user experience issues.

Citrix Analytics, another key component of Citrix Workspace, together with Citrix Access Control bring you complete end-to-end visibility into all TCP and HTTP user sessions. Insight captures authentication errors whether because of an expired password, locked-out account, or endpoint scan failure, and any SSO or application launch failures so you can troubleshoot issues faster.

With risk indicators and criteria to help detect user anomalies, you can configure the policy controls to quickly identify and get alerted about bad or risky user behavior, such as users accessing or uploading/downloading information from malicious and risky websites. Also see historical views by user and website.
Give people the freedom to get work done their way. With Citrix Workspace, you can deliver true single sign-on across all applications for simpler IT management, better security, and an improved user experience.

Explore Citrix Workspace

Sources:
1. 12 Must-Know Statistics on Cloud Usage in the Enterprise, Skyhigh Networks.