DATASHEET

GO-Global

Single Sign-On for Windows Applications

GRAPHON

What is Single Sign-On?

Single Sign-On (SSO) is a user authentication tool that allows users to log in to and access multiple applications, websites, data, and workstations using just one centrally managed set of credentials — a username and password. Organizations use SSO to manage identity access and to improve data security and policy compliance and enhance the user experience. Without SSO, authentication is performed individually by each website or application, with each entity having its own set of credentials that must be managed by the user or IT.

Why Use Single Sign-On?

Unfortunately, passwords are static, don't get changed often enough, and are often reused (59% of users use the same or similar passwords in multiple resources). Ironically, even though passwords are often reused, Gartner estimates that 30 to 50% of all helpdesk calls are for password resets. Relying on passwords for user authentication exposes organizations to undue risk and increases helpdesk costs.

As a result, many organizations have adopted SSO to remove the need for passwords to gain access to applications. Identity providers (IdPs) like Okta, OneLogin, Ping, and others will use protocols like Security Assertion Markup Language (SAML) or the more modern OpenID Connect (OIDC) to implement SSO. These protocols set up a trust between the organization's IdP and integrated applications, whereby users are sent to those applications with a unique access token generated by the IdP that will grant access. SSO removes passwords, makes access credentials invisible to the user, and eliminates the ability for credentials to be compromised.

Using an identity provider for SSO has several usability advantages as well. With SSO, a user typically logs into his IdP once each day with one set of credentials and is presented a portal webpage listing the applications available to him. A simple click on an application within the organizations' IdP portal page allows him to open the application with his trusted token.

Eliminating application logons makes everyone happier. Users can access all their corporate applications with one logon. IT can more easily audit and manage users, for example, provisioning and deprovisioning user resource access. Security teams can define and enforce security policy and maintain regulatory compliance. IT deals with fewer helpdesk calls to reset passwords, especially since many SSO solutions allow users to reset their passwords themselves.

Single Sign-On has made moving to the cloud significantly easier for organizations because it centralizes secure identity access and, by default, centralizes each user' web application access.

Continued on next page

GO-Global

Single Sign-On for Windows Applications

DATASHEET

The Single Sign-On Challenge

There are many times, though, that an organization requires users to use Windows® –not web-based–applications. And, unfortunately, SSO has historically only been available to provide secure access to web applications. Authentication events within Windows OS occur through Winlogon, the Windows authentication module that performs interactive logons for a session–where a user logs directly onto the operating system with a username and a password.

Because Windows requires a username and password to log on, IT cannot include Windows applications in cloud implementations using SSO without a customized Credential Provider. Windows applications installed on remote workstations accessed through Microsoft Remote Desktop Protocol (RDP) have the same limitations.

GO-Global Enables Single Sign-On for Windows

GO-Global's support for OpenID Connect allows organizations to use modern identity providers like Okta, OneLogin, Microsoft Active Directory Federated Services (ADFS), and Microsoft Azure AD Seamless SSO for single sign-on into GO-Global Windows hosts. By enabling users to sign in one time to their identity provider, with the authentication policies and credentials defined there, users can access Windows applications published by GO-Global with the click of a button, providing a better user experience while enforcing the user authentication the organization wants.

GO-Global allows organizations to integrate any IdP that supports OpenID Connect directly into its hosts, allowing them to share windows hosts among users that they authenticate with their IdP solution. GO-Global support for OpenID Connect eliminates the need for domain controllers in the network, for custom credential providers for strong authentication, and for interactive logons.

Organizations that were previously looking for this type of functionality would have to purchase expensive, complex, and unwieldy solutions like Citrix NetScaler Unified Gateway integrated with Citrix Hypervisor, which is expensive to purchase and support. GO-Global provides the functionality at a price point that works for every organization.

To find out more, go to graphon.com.

About GraphOn

GraphOn created GO-Global to enable reliable, secure, multi-user access to Windows applications from any location, device, and operating system. GraphOn GO-Global combines the scalability and performance of multi-user application publishing products with the easy management of remote PC access products, reducing administration and hardware costs, increasing end-user efficiency, and lowering total cost of ownership. GO-Global enables application delivery at 40% less than solutions from Citrix®, VMware® and Microsoft® and can be installed and configured in 15 minutes on Windows PCs or servers.

GRAPHON

GRAPHON CORPORATION

6 Loudon Road, Suite 200 • Concord, NH 03301 USA • **sales@graphon.com**