onelogin

PRODUCT DATASHEET

OneLogin for RDG Server/RDWeb

Secure, Authenticate and Unify Access Management for Remote Users

Does your organization use Microsoft Remote Desktop Gateway (RDG) Server or Remote Desktop Web (RDWeb) to access on-premises Windows servers or desktops? Are you relying on complex, costly, and difficult-to-manage configurations to provide only username and password access for remote RDP users? Now you can secure your RDG Server and RDWeb access with OneLogin SmartFactor Authentication™ to provide your users with a secure single sign-on (SSO) experience.

Introducing OneLogin for RDG Server and RDWeb

OneLogin for RDG Server and RDWeb empowers enterprises to simply and reliably secure access to on-premises Windows servers and desktops in local or remote data centers or private clouds (i.e. AWS and Microsoft Azure). With OneLogin, choose options that do not require client software deployment and that work seamlessly with the OneLogin user portal. Configuring multi-factor authentication (MFA) is as simple as configuring the user policy at OneLogin. Your users enjoy a secure, simple SSO login experience to access Windows servers. In addition, administrators can setup configurations using either the OneLogin admin user interface or APIs and configuration management tools like Terraform.

KEY BENEFITS

Streamline access through a unified cloud portal

Seamlessly enable SSO access between OneLogin and on-premises Windows systems, regardless of the user's location.

Enforce security contextually in real-time

Secure access via user access policies and risk-aware MFA with OneLogin SmartFactor Authentication, powered by Vigilance AI™, the OneLogin AI/ML risk engine. Layer security in front remote VPN access to Windows servers hosted in local or remote data centers, or private clouds.

Minimize legacy dependencies and administration

Remove aging or costly solutions that attempt to protect remote access to systems with MFA, while eliminating tools that are complex to operate and expensive to maintain.

Gain one dashboard for easy administration

Centrally manage remote access to Windows servers as well as create, modify, enforce, and review policies through a modern dashboard.

Power access management with DevOps tools

Use OneLogin APIs to create, read, update and delete configurations, and leverage configuration management tools like Terraform for automation..

Delight end-users with a simple experience

Authorize end-users (i.e. employees and contractors) to easily and securely access Windows systems through SSO at the OneLogin portal for both SaaS and Windows systems, from any device, anywhere.

Over 2,500 enterprise customers globally secure their applications with OneLogin

AAA AIRBUS pandora Steelcase STITCH FIX

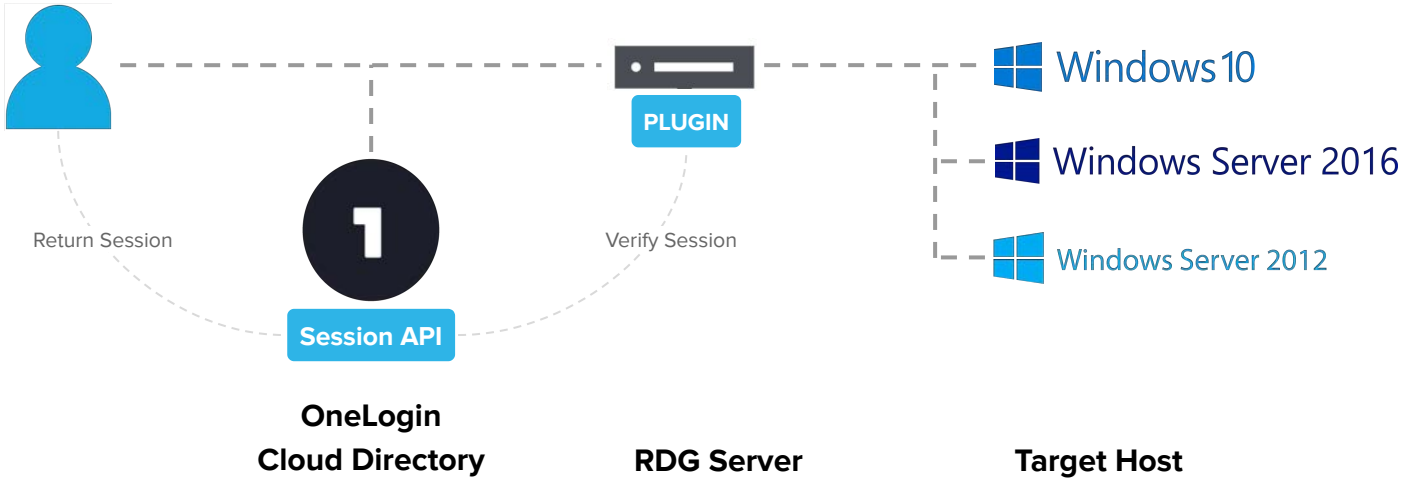

Figure 1: *When the OneLogin RDG Server solution is integrated as an application tile in the OneLogin user portal, a user policy requires MFA authentication for access. The authorized user clicks on the tile, which is associated with a specific Windows system in the customer's internal network. A user session token is returned in a .rdp file and passed through file extension association to the MSTSC client and then to RDG Gateway for validation by the OneLogin RDG Server authentication plugin.*

How OneLogin for RDG Server Works

OneLogin provides two solutions for RDG Server. The first solution is shown above in Figure 1 and is the recommended option to take full advantage of the OneLogin portal user experience and zero client installation. A second option allows installation of a custom Windows or Mac client that uses SAML to authenticate the user at OneLogin according to their user policy. The resulting user session is sent to RDG Server for OneLogin API validation by the RDG Server authentication plugin.

With both options, the user is securely authenticated using OneLogin credentials and MFA (if required by the user policy). RDG Server allows access to the target host, usually a Windows Server. The user is not yet logged into the Windows domain and must still supply valid credentials to log into the target Windows system. With this solution, the client software can either be installed silently by Windows, other MDM software, or interactively by the user from a download.

How OneLogin for RDWeb Works

RDWeb users browse directly to the RDWeb server where they are prompted for authentication. The user enters a username, password, and optionally MFA, if required by the user policy, which is validated through OneLogin APIs.

Upon successful authentication, the user is presented with authorized resources and the system made available through RDWeb.

To learn more about OneLogin for RDG Server and RDWeb, visit https://www.onelogin.com/product/onelogin-access