onelogin

PRODUCT DATASHEET

OneLogin for RD Gateway

Unified and Secure Access Management for Remote Windows Users

Does your organization use Microsoft Remote Desktop Gateway (RDG) to access Windows servers or desktops that are behind the firewall? Are you relying on complex, costly, and difficult-to-manage configurations that provide only username and password access for remote RDP users? Now you can secure your RDG servers with multi-factor authentication (MFA) to provide your users with a secure login experience.

OneLogin for RD Gateway

OneLogin for RD Gateway empowers organizations to simply and reliably add MFA when using RDP to access Windows servers and desktops in local or remote data centers or in private clouds, like AWS and Azure. Enforcing MFA is as simple as configuring the user policy within the OneLogin administrator portal, and without installation of any client software. At the same time, end-users enjoy a simple login experience to securely access Windows servers wherever they are.

KEY BENEFITS

Streamline access through a unified cloud portal

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

Enforce contextual security in real-time

Layer MFA in front of remote access to Windows servers. Choose from a wide variety of authentication factors, like SMS, email, voice, or OneLogin Protect. Configurable user policies and context-aware SmartFactor Authentication™ adjusts authentication requirements depending on the risk level of each login.

Utilize 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.

Minimize legacy dependencies

Remove aging or costly solutions that attempt to protect remote access to systems, while eliminating infrastructure, such as IPsec VPN, that are complex to operate and expensive to maintain.

Power access management with DevOps tools

Use OneLogin APIs to create, read, update and delete configurations, and leverage configuration

ion.

"We needed a more reliable solution that was easier for our users. OneLogin's solution for Remote Desktop Gateway (RDG) was the perfect alternative."

Tommy Cradock | Information Technology/Sr. Unix/Linux Engineer, Bic Graphic

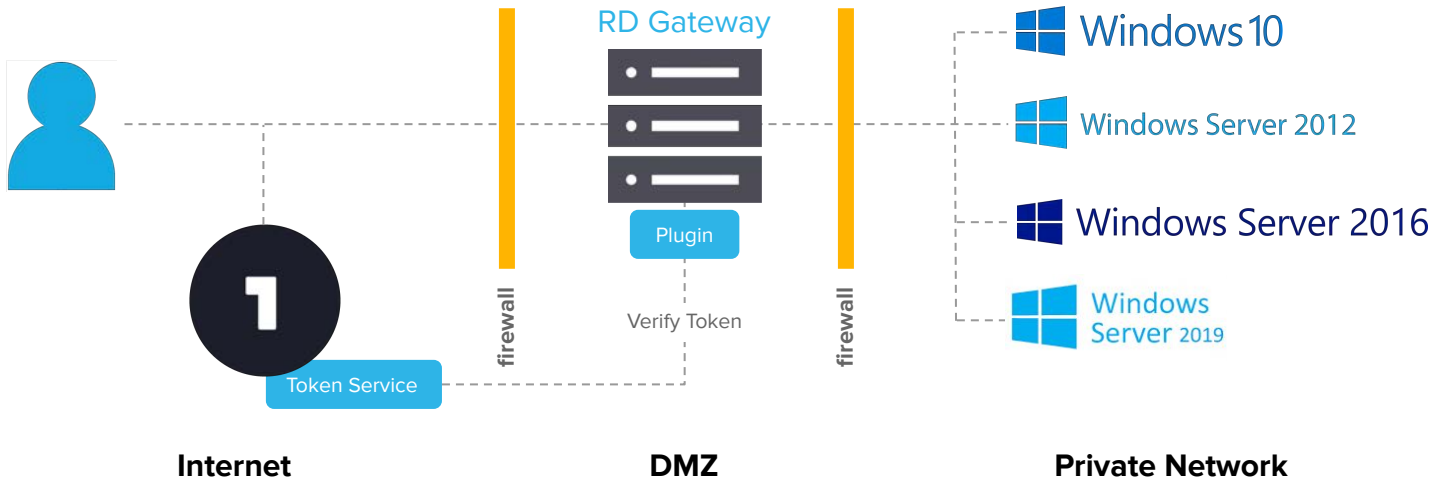

Figure 1: *When the OneLogin for RDG Portal Flow solution is integrated as an application tile in the OneLogin user portal, a user policy requires MFA authentication for access. An authorized user clicks on the tile, which is associated with a specific Windows system in the private network. A secure, one-time token is returned in a .rdp file and passed through file extension association to the MSTSC client and then to RDG Server for validation by the OneLogin RDG authentication plugin. The user then domain authenticates to the target host.*

How OneLogin for RD Gateway Works

OneLogin provides two solutions for RDG. The first solution, the Portal Flow, is described in Figure 1 and provides the full advantages of the OneLogin user portal experience, single sign-on, and zero client installation. A second option, the Desktop Client, requires installation of a OneLogin Windows or Mac client that uses OpenID Connect (OIDC) to authenticate users.

For both solutions, the user is securely authenticated using OneLogin credentials and MFA, as required by the OneLogin user policy. One-time tokens are sent to RDG for validation by the OneLogin RDG authentication plugin.

Once authenticated, RDG allows access to the target host, a Windows server or desktop. The user is not yet logged into the Windows domain and must supply a valid domain password for their account to log into the target Windows system.

The Portal Flow does not require OneLogin software on the user's system. The Desktop Client can either be installed silently by Windows, other MDM software, or interactively by the user. Both solutions require the Microsoft Terminal Services Client (MTSC) to be on the user's system.