onelogin

PRODUCT DATASHEET

OneLogin Cloud RADIUS

Easily administer RADIUS with Multi-Factor Authentication in the cloud

Many organizations today have a mix of cloud services and on-premises infrastructure living behind the firewall, which is commonly referred to as the Hybrid Enterprise. An organization's VPN and WiFi access points are essential to supporting the modern workplace, where users need access to corporate applications anytime of the day, wherever they are located. However, applying modern security controls over VPN and WiFi connections is challenging, especially when RADIUS is required for authentication. Not to mention the additional security burden of preventing unauthorized access to sensitive corporate data that is stored on-premises with only traditional username and password authentication to access.

OneLogin Cloud RADIUS
OneLogin's Cloud RADIUS solution provides seamless and reliable Multi-Factor Authentication (MFA) across on-premises network appliances and applications, such as your corporate VPN and WiFi access points. Users can leverage their corporate username and password with flexible MFA authentication including push notifications to securely access their applications. Admins benefit from a simplified administrative experience, decreased costs, and increased security, visibility, and productivity.

KEY BENEFITS OF ONELOGIN CLOUD RADIUS

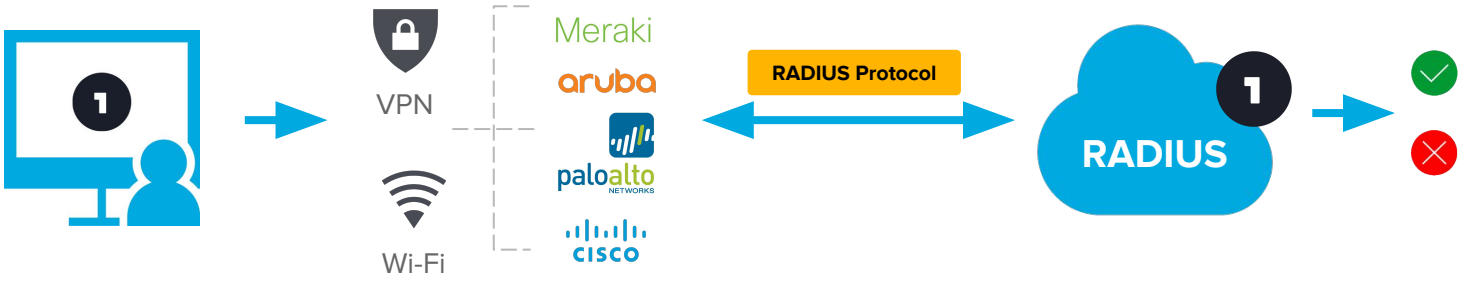
Zero on-premises footprint
Standing up your own RADIUS servers can be complex and costly to maintain. Eliminate the burden of managing on premises RADIUS servers with a 100% cloud-hosted solution. No on premises software is required.

Leverage the same credentials everywhere
Use the same user credentials that your users are using at OneLogin and within your corporate network to login to SaaS and on-premises applications.

Quickly and flexibly apply strong security policies
Easily setup and administer MFA policies to protect your network perimeter when authenticating users to your VPN or WiFi. Require users to submit a password, password+OTP, OTP only, or accept a push notification using OneLogin Protect. Support for customer-specified and vendor-specific attributes in the RADIUS Access-Accept message provides further authorization based on attributes like user groups and roles.

Industry leading support for RADIUS security protocols
Leverage best-in-class support for RADIUS authentication methods to integrate with most Network Access Services (NAS), including PAP, EAP-TTLS/PAP, and EAP-PEAP/MSCHAPv2 for a secure, performant, and reliable monitored service. And if your NAS supports RADIUS Access Challenges, OneLogin Cloud RADIUS has you covered.

Easy configuration and set up
Create and manage any number of RADIUS configurations using a modern and flexible web UI. No need to hire trained staff to administer a RADIUS server, such as FreeRADIUS. Event logging provides comprehensive RADIUS authentication monitoring and reporting. And adding MFA is a snap, including push notifications with OneLogin Protect.



How OneLogin Cloud RADIUS Works

With OneLogin, easily configure a secure RADIUS server with desired access points all within a centralized web-based admin console. You can connect your RADIUS endpoint to either your existing user directories, such as Active Directory or a single source of truth, like Workday, via the OneLogin Cloud Directory.

Policies restrict users based on their role and determine whether or not they can connect with RADIUS authentication. Configure the IP address and an associated secret key as well as the RADIUS Network Access Services (NAS) with the preferred type of RADIUS authentication.

Connect to OneLogin via secure RADIUS TLS tunnels using EAP-TTLS or EAP-PEAP and choose either the widley used PAP authentication method or MSCHAPv2, which is popular for Enterprise WiFi access points like Meraki and Aruba, for RADIUS inner tunnel authentication.

Select whether users need to submit either their password, an OTP code, a combination of the two or a push notification. If the RADIUS NAS supports it, you can optionally implement the RADIUS challenge where a user enters their username and password first before prompted to enter the OTP code.

Layer on MFA using a variety of authentication factors, including OneLogin's Protect authenticator app, available on iOS and Android, or integrate with Yubikey, Symantec VIP, and more.

OneLogin Cloud RADIUS supports standard RADIUS and Vendor-Specific Attributes (VSA) that return information via the RADIUS Access-Accept message to your NAS in order to make authorization decisions based on the user's identity.

"Now we have peace of mind knowing departing employees can't access our resources. Our applications and our Wi-Fi network are protected once we toggle off their access."

FRANK SCHLESINGER | CTO, orderbird

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

AIRBUS pandora Steelcase STITCH FIX