IMPLEMENTING MULTI-FACTOR AUTHENTICATION (MFA) IS AN ESSENTIAL SECURITY STRATEGY FOR ANY ORGANIZATION

With **GreenRADIUS,** MFA is easy to deploy, easy to maintain, and easy to use for both admins and end users.

Available to deploy as a virtual machine or containerized solution, **GreenRADIUS** is versatile in a number of ways.

MINIMUM REQUIREMENTS

GreenRADIUS is a lightweight solution with the following minimum resource allocation: 2 CPUs, 4 GB RAM, 80 GB hard drive space.

GreenRocket
Security

greenrocketsecurity.com
1-888-793-3247

USES / INTEGRATIONS

GreenRADIUS MFA can be integrated with a variety of applications and services, such as VPN, Windows logon, Linux servers, websites, ADFS, and more. So long as the application or service supports RADIUS, LDAP, SAML, Web APIs, or integrates with ADFS, GreenRADIUS will be able to integrate with it.

TOKENS

Various tokens can be used as a second factor, such as YubiKeys, Google Authenticator, our own mobile app (which uses push notifications), and others. A user can have multiple tokens assigned, and any of the assigned tokens can be used as the second factor during a login attempt.

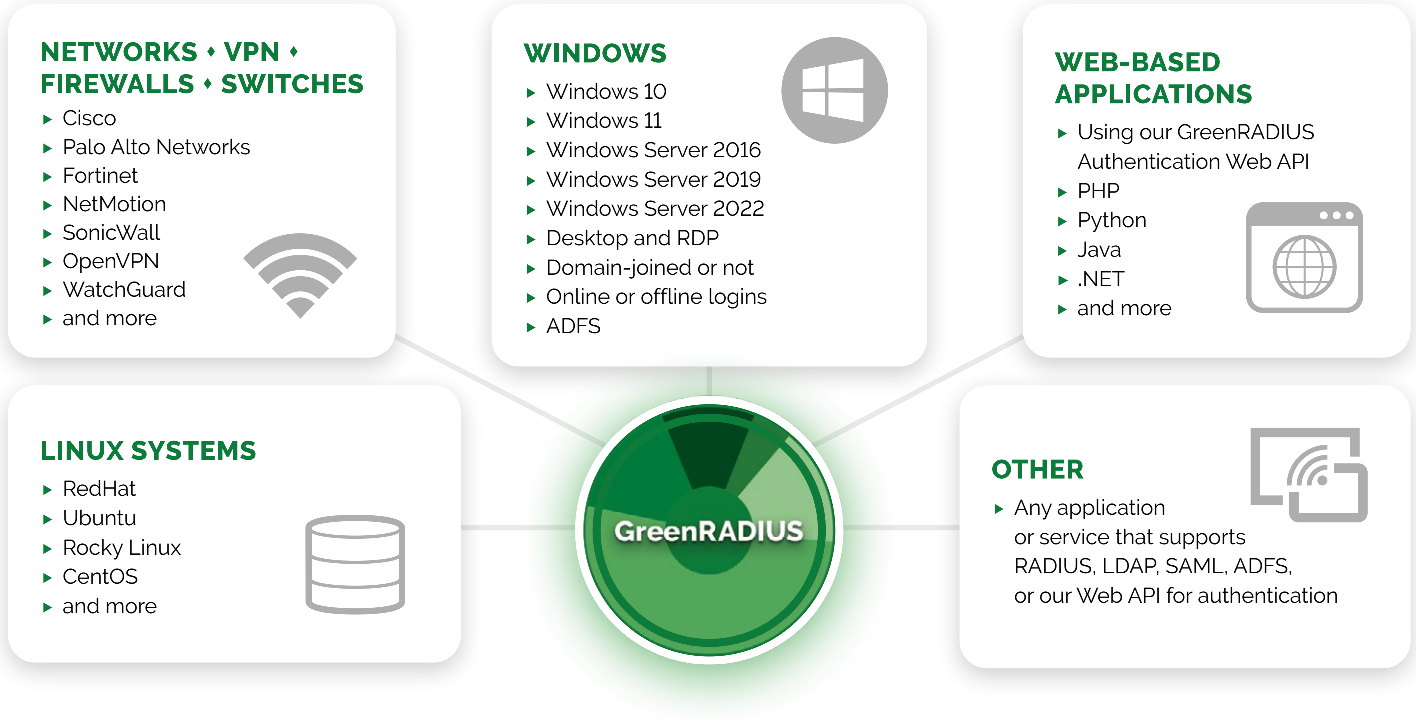
USER DIRECTORIES

Users can continue to be managed in your existing LDAP. Added or deleted users from your LDAP can be automatically synced with GreenRADIUS. GreenRADIUS supports Active Directory, OpenLDAP, FreeIPA, and 389DS. There is also an onboard OpenLDAP in GreenRADIUS for organizations that want a completely self-contained solution.

REPORTING / LOGGING

Authentication requests and token assignment reports can be generated in our Reports screen. This and other data are also included in the output to configured syslog servers.

GreenRADIUS PROVIDES SUPERIOR MFA SECURITY AND A WIDE RANGE OF POSSIBLE INTEGRATIONS



NETWORKS • VPN • FIREWALLS • SWITCHES

- Cisco
- Palo Alto Networks
- Fortinet
- NetMotion
- SonicWall
- OpenVPN
- WatchGuard
- and more

WINDOWS

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Desktop and RDP
- Domain-joined or not
- Online or offline logins
- ADFS

WEB-BASED APPLICATIONS

- Using our GreenRADIUS Authentication Web API
- PHP
- Python
- Java
- .NET
- and more

LINUX SYSTEMS

- RedHat
- Ubuntu
- Rocky Linux
- CentOS
- and more

OTHER

- Any application or service that supports RADIUS, LDAP, SAML, ADFS, or our Web API for authentication

GreenRADIUS
KEY FEATURES AND CAPABILITIES

YubiKey Support:

- Supports YubiKey OTP, OATH, FIDO U2F, and FIDO2
- Auto-assignment of YubiKeys to users (upon first successful login with a YubiKey)
- Validates OTPs internally/locally or with the YubiCloud
- Ability to encrypt token secrets
- Allows users to be assigned multiple YubiKeys
- For users with multiple tokens, no need for users to pre-select which token will be used
- Temporary token feature
- Ability to deploy MFA gradually to users in an automatic way

Other Tokens Supported:

- OATH tokens, such as Google Authenticator, Microsoft Authenticator, and Authy
- Our "Green Rocket MFA" mobile app, available on Android and iOS devices, which sends push notifications to users upon a login attempt
- Other FIDO tokens

Other Features and Capabilities:

- GreenRADIUS can be deployed as a virtual machine, as a containerized deployment, or as an AMI image in AWS
- Able to be set up GreenRADIUS in a HA/failover cluster across data centers
- HA/failover cluster can be set up in a hybrid cloud/on-premise environment
- Supports various integrations – RADIUS, Web API, Windows Logon, LDAP, ADFS, PAM
- Ability to configure RADIUS clients to require a PIN as the first factor (either instead of the LDAP password or in addition to the LDAP password)
- Integrates with a variety of LDAPs – Active Directory, OpenLDAP, 389 DS, or FreeIPA
- There is also an onboard OpenLDAP in GreenRADIUS
- Lightweight server requiring minimal resources (2 CPUs, 8GB RAM, 80 GB disk space)
- Ability to prevent brute force attacks
- Up to two syslog/SEIM servers can be configured for logging output
- Ad-hoc reports include authentication requests report and token assignment report
- Web admin interface for easy administration/management
- Self-service portal for users to assign/register a token and to test a login
- Multi-tenancy, allows for multiple domains to be integrated with different LDAPs and/or different LDAP groups
- Fully supported by a global support team
- Maintained with monthly security updates/patches