GreenRocket Security

Meeting Regulatory Compliance with GreenRADIUS MFA

- HIPAA
- ISO 27001
- PCI DSS 4.0
- FIPS 140-2

greenrocketsecurity.com

1-888-793-3247

info@greenrocketsecurity.com

Why MFA Is Central to Regulatory Compliance

Regulatory frameworks like HIPAA, ISO 27001, PCI DSS 4.0, and FIPS 140-2 share a common thread: They require organizations to implement strong access controls ensuring only authorized individuals can access sensitive systems, with MFA commonly required or strongly recommended for high-risk access scenarios. Passwords alone are generally insufficient to meet these requirements. Credential theft, phishing, and brute-force attacks have made password-only authentication a recognized compliance liability.

Multi-factor authentication (MFA) has become a widely adopted control used to satisfy access control and authentication requirements across these frameworks. However, deploying MFA across a heterogeneous IT environment — legacy systems, on-premise infrastructure, hybrid cloud, remote access — is where most organizations struggle.

GreenRADIUS, developed by Green Rocket Security, is designed to address this challenge. It brings robust, flexible MFA to across your environment regardless of whether your infrastructure lives on-premise, in the cloud, or somewhere in between.

GreenRADIUS acts as a **policy-driven authentication layer** integrated with your directory services, enabling granular MFA enforcement across users, groups, and systems without requiring application rewrites.

Compliance Standards and How GreenRADIUS Supports Them

HIPAA

MFA/2FA Requirement

HIPAA requires strong access controls and user authentication mechanisms (45 CFR §164.312). MFA is commonly implemented to meet these requirements and reduce unauthorized access risk

How GreenRADIUS Helps

GreenRADIUS enforces MFA on VPN, Windows Logon, and web portals — protecting all pathways to electronic patient health information. Detailed authentication logs satisfy HIPAA audit control requirements.

PCI DSS 4.0

MFA/2FA Requirement

Req. 8.4 — MFA required for all access into the cardholder data environment (CDE)

How GreenRADIUS Helps

GreenRADIUS enforces MFA for access into the cardholder data environment (CDE), including remote access, administrative access, and system logins, aligning with PCI DSS 4.0 Requirement 8.4.

ISO 27001

MFA/2FA Requirement

A.9.4 — System and application access control; A.9.3 — User responsibilities for authentication

How GreenRADIUS Helps

GreenRADIUS supports implementation of strong authentication controls aligned to ISO 27001 Annex A (A.9), enabling organizations to apply risk-based access policies and demonstrate control effectiveness during audits.

FIPS 140-2

MFA/2FA Requirement

Cryptographic modules must meet FIPS 140-2 standards for federal and regulated environments

How GreenRADIUS Helps

GreenRADIUS supports FIPS-validated authenticators such as YubiKeys and can be deployed in environments requiring FIPS-compliant cryptography. GreenRADIUS can operate with FIPS-validated cryptographic modules depending on deployment configuration.

Flexible Deployment Across Regulated Environments

A critical differentiator between GreenRADIUS and cloud-only MFA solutions is deployment flexibility. Many regulated industries — healthcare, federal agencies, financial services — operate environments where sensitive workloads cannot simply be handed off to a third-party cloud service. GreenRADIUS meets your infrastructure where it is:

On-Premises

Ideal For: Healthcare, Government, Finance with air-gapped or sensitive environments

Key Compliance Benefit: Full data sovereignty — authentication events and logs remain within your environment. Ideal for HIPAA and FedRAMP-sensitive environments.

Hybrid

Ideal For: Organizations transitioning to cloud while maintaining legacy systems

Key Compliance Benefit: Bridges on-prem Active Directory with cloud apps, ensuring consistent MFA enforcement across all environments without compliance gaps.

Cloud / AWS

Ideal For: SMBs and IT teams seeking managed infrastructure

Key Compliance Benefit: Scalable MFA enforcement with the same policy controls, audit logging, and token support as on-prem deployments.

What GreenRADIUS Protects

GreenRADIUS enables MFA enforcement across critical access points required by compliance frameworks:

- **Windows Workstation & Server Logon**
  2FA at the endpoint, not just the perimeter
- **VPN & Remote Access**
  Enforce MFA before users enter the network
- **Linux SSH**
  Secure administrative access to servers and infrastructure
- **ADFS / SAML Applications**
  Extend strong authentication to cloud and web apps
- **Network Equipment**
  Protect routers, switches, and firewalls via RADIUS
- **Web Applications**
  Integrate MFA via RADIUS, LDAP, or the GreenRADIUS Web API

GreenRocket Security

Supported Authentication Methods

GreenRADIUS supports a range of authentication methods to meet varying security and compliance requirements, including hardware-backed FIDO2 authentication and widely adopted OTP-based methods

1. YubiKey and other Hard Tokens

OTP, OATH-HOTP, and FIDO2/WebAuthn (phishing-resistant, hardware-backed)

2. OATH Tokens

OATH-HOTP and OATH-HOTP standards are supported

3. Green Rocket 2FA Mobile App

Push notification authentication for iOS and Android

Audit Logging & Reporting

Demonstrating compliance to auditors requires more than having MFA in place — it requires evidence. GreenRADIUS provides centralized, tamper-resistant authentication logging so that every access attempt, successful or failed, is recorded with user, timestamp, method, and result. These logs are a direct input to HIPAA audit control requirements, ISO 27001 monitoring obligations, and PCI DSS logging mandates.

Administrators manage GreenRADIUS through a web-based interface accessible from any browser, with policy controls organized by user and group — aligning with the role-based access controls demanded by all four frameworks.

Logs can be exported to SIEM systems and retained according to organizational compliance policies.

What GreenRADIUS Does Not Do (But Enables)

GreenRADIUS does not replace your compliance program or governance processes. Instead, it provides the authentication enforcement and audit visibility required to support regulatory compliance initiatives.

Ready to Strengthen Your Compliance Posture?

Download GreenRADIUS and evaluate it free with an included trial license.

greenrocketsecurity.com

1-888-793-3247

info@greenrocketsecurity.com