How-to Guide to FedRAMP Compliance for Software-as-a-Service (SaaS) Providers

Teleport

How-to Guide to FedRAMP Compliance for Software-as-a-Service (SaaS) Providers

Read this guide if you are:

A security-minded engineer responsible for implementing logical security controls in order to demonstrate compliance with FedRAMP.

Introduction

Growing your SaaS business means bringing on new verticals and selling more to existing customers. The bigger the customers, the higher the stakes. There is often no bigger customer than the federal government, so many SaaS organizations must demonstrate FedRAMP compliance in order to sell into this lucrative vertical. This how-to guide walks you through the logical controls that you must implement in order to pass a FedRAMP audit using the Teleport Access Plane.

Many software engineers roll their eyes when they hear the word “compliance.” It sounds boring, and maybe it is! But when you read through the FedRAMP controls in this document, you realize that they are actually a collection of common-sense recommendations that have been proven to work. A compliance standard is not an annoying obstacle to productivity. And demonstrating compliance is very doable if you approach the project correctly. Your reward will be accelerated growth of your SaaS business and better security.

> **sumo logic**
>
> *Teleport has made obtaining a FedRAMP Moderate that much more achievable via their FIPS 140-2 endpoints, easy integration with our SSO and MFA, and the view into audit logs of remote connection sessions provides the appropriate insight for continuous monitoring.*
>
> *Jeff Gill, Director of Engineering, Sumo Logic*

What is FedRAMP?

The FedRAMP (Federal Risk and Authorization Management Program) was originally proposed as a standardized approach for the federal government to adopt secure cloud services offered by the cloud providers. FedRAMP is a product of collaboration with multiple government agencies, such as NIST, GSA, DOD, and DHS.

While the original focus of FedRAMP was on cloud infrastructure (i.e. things like virtual networks, servers, and firewalls), eventually it was applied to cloud applications as well.

If your organization is currently offering, or planning to offer, cloud infrastructure or cloud software services to the federal government, you must have your software running on a FedRAMP-compliant cloud service provider (CSP) and your software must be able to a pass FedRAMP audit by an independent auditor. This auditor will ask to see how your SaaS application meets a detailed list of controls necessary to demonstrate FedRAMP compliance.

Just like SOC 2, another popular compliance framework, FedRAMP introduces its own vocabulary. The foundational document is called FedRAMP Security Assessment Framework (SAF). This high-level document covers the process of becoming FedRAMP compliant, but the technical details of "getting everything right" are described in the publication Security and Privacy Controls

for Federal Information Systems and Organizations NIST 800-53 maintained by the National Institute of Standards and Technology (NIST).

FedRAMP requirements described in NIST publications are labeled with the severity of their impact: low, medium, or high. Each government agency is free to decide which level of compliance they desire. That is why terms such as "FedRAMP medium" or "FedRAMP high" are frequently used.

Just like with SOC 2, NIST 800-53 groups all requirements into "families" with unique identifiers (ID):

ID	Family	ID	Family
AC	Access Control	**MP**	Media Protection
AT	Awareness and Training	**PE**	Physical and Env. Protection
AU	Audit and Accountability	**PL**	Planning
CA	Security Assessment & Authorization	**PS**	Personnel Security
CM	Configuration Management	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SI**	System and Information Integrity
MA	Maintenance	**PM**	Program Management

What you need to do to pass a FedRAMP audit

Depending on the level of FedRAMP compliance, you will need to demonstrate a certain number of controls across the NIST families. Some families, such as Personnel Security and Program Management, have less of a logical component. So you as a security-minded engineer responsible for implementing logical security controls in order to demonstrate compliance with FedRAMP won't likely have to answer to those controls in front of an auditor.

You will get asked, however, to demonstrate controls around Access Control, Identification, Authentication, and Audit which definitely fall within Teleport's area of responsibilities.

FedRAMP case study in action

Challenge

As a multi-billion dollar publicly traded company, this cloud-hosted database provider is always in search of sustainable growth. The Federal Government has a $92 billion IT budget in 2021 alone, so expanding to serve this lucrative market is smart business. But selling to the federal government also comes with significant responsibility to demonstrate care is taken to protect government data. This company understood that demonstrating compliance with FedRAMP Moderate would allow them to run their cloud service on AWS GovCloud and list their service in the FedRAMP Marketplace, fueling significant business growth.

Teleport solution

Teleport enables SaaS providers to easily demonstrate Access, Identification, Authentication, and Audit controls necessary to show FedRAMP compliance. Additionally, the Teleport software itself builds against a FIPS 140-2 compliant library, a key requirement in FedRAMP compliance. For SaaS providers serving the Federal government, the Teleport Access Plane consolidates the four essential infrastructure access capabilities every security-conscious organization needs: connectivity, authentication, authorization, and audit. Our unique approach to FedRAMP compliance is not only more secure; it improves developer productivity. By providing an identity-aware access solution that

developers love to use, you can easily implement FedRAMP security and compliance without worrying about backdoors that outmoded solutions encourage.

Business impact

With Teleport, this publicly traded company was able to pass their independent FedRAMP audit enabling them to run their cloud service on AWS GovCloud and list their service in the FedRAMP Marketplace. Additionally, because Teleport makes it simple to implement security best practices without getting in the way of developer productivity, their entire offering is more secure, enabling them to demonstrate security and compliance to other important verticals like Financial Services, Healthcare, and more.

> *"Without Teleport we would not have gotten through the FedRAMP Moderate audit. Every time we do a demo, it's very easy to get the auditors over the hump. It hit all the flags that they were looking for. It saved us a ton of time.*
>
> *Publicly traded cloud-hosted database provider*

FedRAMP compliance for infrastructure

The table below connects Teleport features to FedRAMP requirements. It previews how to tighten controls for Linux & Windows servers, databases, Kubernetes clusters, and internal applications like CI/CD environments when preparing for FedRAMP audits.

FEDRAMP REQUIREMENT NIST 800-53	TELEPORT CONTROLS
AC-02 Account Management • The organization employs automated mechanisms to support the management of information system accounts. • The information system automatically removes temporary and emergency accounts. • The information system automatically disables inactive accounts. • The information system automatically audits account creation and modification. • The organization requires that users log out after a defined time-period. • The organization establishes, administers, and audits privileged user accounts in accordance with a role-based access scheme. • The information system enforces organization-defined usage conditions for organization-defined system accounts. • The organization monitors information system accounts and reports atypical usage.	Teleport addresses AC-02 controls when integrated with an SSO provider such as GitHub, Okta, Google, etc. Role-based access control (RBAC) for the protected resource must be enabled. Teleport certificate-based authentication and audit logging comply with these requirements without additional configuration.

AC-03 Access Enforcement • The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. • Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems.	Teleport supports robust role-based access control (RBAC). RBAC can be used to: • Control which SSH nodes a user can or cannot access. • Control cluster-level configuration (session recording, configuration, etc.). • Control which UNIX logins a user is allowed to use when logging into a server. • Control which user groups have access to Kubernetes resources. • Do much more
AC-07 Unsuccessful Logon Attempts The information system: 1. Enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period; and 2. Automatically locks the account/node until released by an administrator; delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	Teleport supports two types of users: from a local database and SSO-based accounts (GitHub, Google Apps, Okta, etc.). For local accounts, by default Teleport locks accounts for 20 minutes after 5 failed login attempts. For SSO-based accounts, the number of invalid login attempts and lockout time period are controlled by the SSO provider.

AC-08 System Use Notification The information system displays to users an organization-defined notification message before granting access to the system that provides privacy and security notices consistent with applicable federal laws, executive orders, and other directives.	Teleport integrates with Linux Pluggable Authentication Modules (PAM). PAM modules can be used to display a custom message on login using a message of the day (MOTD) module within the Session management primitive.
AC-10 Concurrent Session Control The information system limits the number of concurrent sessions for each organization-defined account and/or account type to a defined number.	Teleport supports both a maximum number of connections (`max_connections`) and the maximum number of simultaneously connected users (`max_users`) under the `connection_limits` configuration parameter.
AC-12 Session Termination The information system automatically terminates a user session after organization-defined conditions are met and provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources.	Teleport user sessions are automatically terminated when a certificate expires. Users can exit a Teleport interactive session at any time by typing exit or sending an interrupt signal to the process for remote execution of a program. Logout of all sessions (destroying credentials) indicates termination of all sessions and includes an explicit logout message.

AC-17 Remote Access The organization: establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. It authorizes remote access to the information system prior to allowing such connections. • The information system monitors and controls remote access methods. • The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. • The information system routes all remote accesses through managed remote access control points.	Teleport administrators create users with configurable roles that can be used to allow or deny access to system resources. Teleport Proxy uses SSH or HTTP/TLS to authenticate and encrypt and transfer data between clients and servers. Teleport encourages an architecture that requires all connections to go through the Teleport proxy.
AC-20 Use of External Information Systems The organization establishes terms and conditions consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. This allows authorized individuals to: 1. Access the information system from external information systems; and 2. Process, store, or transmit organization-controlled information using external information systems.	Teleport supports connecting multiple independent clusters using a feature called Trusted Clusters. After the establishment of a Trusted Cluster relationship between two clusters, one cluster “trusts” SSH and TLS certificates signed by the other and allows SSH connections from the other. When allowing access from one cluster to another, roles are mapped according to a pre-defined relationship based on the scope of access.

AU-03 Audit and Accountability The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. **AU-04 Audit Storage Capacity** The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	Teleport contains an Audit Log that records cluster-wide events such as: - Failed login attempts - The command that was executed (SSH “exec” commands) - Ports that were forwarded - File transfers that were initiated - Filesystem changes - Network activity that happened during an interactive user session - Recorded interactive user sessions Events typically include information such as the type, time of occurrence, user or node on which they occurred, and a human-readable audit message. Teleport supports sending audit events to external managed services like DynamoDB where storage concerns are handled by the cloud provider.
IA-03 Device Identification and Authentication The information system uniquely identifies and authenticates organization-defined specific types of devices before establishing a connection.	Teleport requires valid x509 or SSH certificates issued by a Teleport Certificate Authority (CA) to establish a network connection for device-to-device connection between Teleport components.

IA-04 Identifier Management The organization manages information system identifiers by: • Receiving authorization from organization-defined personnel to assign an individual, group, role, or device identifier; • Selecting an identifier that identifies an individual, group, role, or device; • Assigning the identifier to the intended individual, group, role, or device; • Preventing reuse of identifiers for the organization-defined time period; and • Disabling the identifier after an organization-defined time period of inactivity.	Teleport maintains several unique identifiers: • The local users are required to be unique (unique username). • Teleport roles have unique names tied to organization roles via SSO. • Teleport identifiers for devices are unique randomly generated IDs (UUID).
SC-10 Network Disconnection The information system terminates the network connection associated with a communications session at the end of the session or after the organization-defined time period of inactivity.	Teleport disconnects and releases all resources for non-active communications. In addition, session and idle timeouts are specified to terminate and release resources for inactive connections.

SC-12 Cryptographic Key Establish and Management The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction. The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant or NSA-approved key management technology and processes.	Teleport initializes cryptographic keys that act as a Certificate Authority (CA) to further issue x509 and SSH certificates. SSH and x509 user certificates that are issued are signed by the CA and are (by default) short-lived. SSH host certificates are also signed by the CA and rotated automatically (a manual force rotation can also be performed). Teleport Enterprise builds against a FIPS 140-2 compliant library (BoringCrypto). In addition, when Teleport Enterprise is in FedRAMP/FIPS 140-2 mode, Teleport will only start and use FIPS 140-2 compliant cryptography.
SC-17 Public Key Infrastructure Certificates The organization issues public-key certificates under an organization-defined certificate policy or obtains public-key certificates from an approved service provider.	Teleport initializes cryptographic keys that act as a Certificate Authority (CA) to further issue x509 and SSH certificates. SSH and x509 user certificates that are issued are signed by the CA and are (by default) short-lived. SSH host certificates are also signed by the CA and rotated automatically (a manual force rotation can also be performed).

SC-23 Session Authenticity The information system protects the authenticity of communications sessions. The information system invalidates session identifiers upon user logout or other session termination.	Teleport SSH and TLS sessions are protected with SSH user and x509 client certificates. For access to the Web UI, Teleport uses bearer token auth stored in a browser token to authenticate a session. Upon user logout, SSH and TLS certificates are deleted from disk, and cookies are removed from the browser.

Note that not all relevant NIST requirements are listed above. Contact us at https://goteleport.com/signup/enterprise/ to schedule a FedRAMP deep-dive with one of our deeply technical Solution Engineers.

Conclusion

Demonstrating compliance with FedRAMP can seem like a tall order. Yet when approached correctly, implementing the controls necessary to demonstrate FedRAMP compliance can improve not only the security of your SaaS offering, but developer productivity as well.

Teleport's design goal is to provide sensible choices by default. As a result, Teleport automatically enforces most of the best practices listed above without additional configuration.

Want to learn more about how Teleport can help your team pass a FedRAMP audit? Reach out to us at https://goteleport.com/signup/enterprise/ to schedule a FedRAMP deep-dive today.