

SECTION	WHAT FEDRAMP REQUIRES	WHAT POMERIUM PROVIDES
Access Control (AC)		
AC-2	Account Management <i>“The organization manages information system accounts, including establishing, activating, modifying, disabling, and removing accounts as needed.”</i>	Pomerium provides real-time integrations with your identity providers (IdPs) to manage user accounts and enforce role-based access control (RBAC). With Pomerium, administrators can also implement fine-grained policy controls.
AC-17	Remote Access <i>“The information system uses cryptographic methods to protect the confidentiality and integrity of remote access sessions.”</i>	Unlike nearly every other solution available, Pomerium provides clientless remote access that incorporates user context, device context, and any other context you want to provide, with every single request being verified and logged, providing you with insights across the entire lifecycle of the user's sessions. We also enforce TLS encryptions on all connections which you can read more about here .
AC-19	Access Control for Mobile Devices <i>“The organization establishes usage restrictions and implementation guidance for mobile devices to reduce associated risks.”</i>	Policies in Pomerium can restrict access based on the device from which the user is requesting access, as well as on device posture, adding enforcement mechanisms to the policies set by your MDM solutions.
Audit and Accountability (AU)		
AU-2	Auditable Events <i>“The organization determines that the information system must generate audit records for the events that are relevant to the security of the system.”</i>	Pomerium creates an audit trail and log for every single request giving you full visibility into exactly what the user is trying to access, and whether they are in compliance with your policies when attempting each request.
AU-12	Audit Generation <i>“The information system provides audit record generation capability for the organization-defined auditable events.”</i>	Pomerium logs provide a full chain of custody that capture the entire lifecycle of a user's requests giving you full context into what users are doing

Identification and Authentication (IA)

IA-2	User Identification and Authentication <i>“The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).”</i>	Pomerium integrates directly with and serves as a centralization point for your IdP(s), HRIS, and any other source of context, letting you limit access based on a number of factors, for example, removing access if a user is supposed to be on vacation.
IA-5	Authenticator Management <i>“The organization manages information system authenticators by ensuring authenticator quality, changing default authenticators, and protecting authenticators from unauthorized use.”</i>	Using your IdP plus Pomerium policies ensures that you can enforce SSO and MFA compliance in order for users to successfully access protected resources.

System and Communications Protection (SC)

SC-12	Cryptographic Key Establishment and Management <i>“The organization establishes and manages cryptographic keys for required cryptography employed within the information system.”</i>	Pomerium uses cryptography to secure data in transit, at rest, and to provide guarantees around confidentiality, authenticity, and integrity between its services and upstream servers for which it manages access. The following docs links provide more information on Pomerium's cryptography and security practices.
SC-28	Protection of Information at Rest <i>“The information system protects the confidentiality and integrity of information at rest.”</i>	Whether in transit or at rest, Pomerium encrypts all sensitive data. This applies to all data in the databroker, including: • Session, user, and directory data; as well as any other identity or contextual data. • Service secrets (TLS certificates or identity provider credentials). Learn more about our cryptography and security practices.

System and Information Integrity (SI)

SI-4	Information System Monitoring <i>“The organization monitors the information system to detect unauthorized access and facilitate system protection.”</i>	Pomerium's access logs can be integrated with monitoring solutions to detect anomalies or breaches.
------	---	---