FEDERAL COMPLIANCE GUIDE

Total Access Control (TAC) and FedRAMP

How TAC supports federal Authority to Operate (ATO) processes through NIST 800-53 control alignment, NIST 800-207 Zero Trust Architecture, and flexible deployment in agency-controlled environments — from on-premises to FedRAMP-authorised cloud regions.

Audience	Frameworks	Version
Federal CISOs, ISSOs, agency authorising officials, FedRAMP-track buyers	NIST SP 800-53 Rev. 5, NIST SP 800-207, FedRAMP program	v2.0 — 2026

TAC FedRAMP Status. TAC is **not currently FedRAMP authorised** and does not hold the FedRAMP Ready designation. TAC is architected to align with NIST SP 800-53 Rev. 5 controls at the Moderate and High baselines — the same control framework that underpins FedRAMP authorisation — and deploys in FedRAMP-authorised cloud environments (AWS GovCloud, Azure Government) as well as on-premises within agency facilities. Federal authorisation paths available for TAC are discussed in the Deployment Scenarios section.

Overview

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide programme that provides a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services used by federal agencies. Established in 2011 and codified by the FedRAMP Authorization Act of 2022, the programme is administered by the General Services Administration (GSA) with Office of Management and Budget (OMB) oversight.

FedRAMP evaluates cloud service providers (CSPs) against NIST SP 800-53 Rev. 5 security controls at three impact levels: Low, Moderate, and High. A FedRAMP Third Party Assessment Organisation (3PAO) conducts the security assessment, and authorisation is granted by either an individual sponsoring agency or the Joint Authorization Board (JAB).

Total Access Control (TAC) by PortSys is a single-tenant zero-trust access control platform that **implements the Policy Engine, Policy Administrator, and Policy Enforcement Point** defined in NIST SP 800-207, and aligns with NIST 800-53 Rev. 5 controls relevant to federal access control, authentication, audit, and boundary protection. TAC is deployable in any agency-controlled environment.

FEDRAMP SCOPE

What FedRAMP Covers (Per OMB M-24-15)

REQUIREMENT	HOW TAC DELIVERS
Cloud products and services offered to multiple federal agencies	FedRAMP applies to Infrastructure-, Platform-, and Software-as-a-Service offerings that process, store, or transmit federal information on behalf of multiple federal agencies. Per OMB Memorandum M-24-15, a cloud offering falls within FedRAMP scope when all four indicators are present: (1) handles sensitive federal information under 44 USC §3506; (2) requires agency-specific tenant configuration; (3) integrates into agency enterprise security services; (4) is available for use by multiple agencies.
What FedRAMP does NOT cover	FedRAMP does not apply to: (1) on-premises software deployed within an agency's own facility; (2) single-agency systems hosted on cloud infrastructure that are not offered as shared services (excluded by OMB M-24-15); (3) software installed and operated by the agency on their own cloud tenancy (e.g., an agency-managed VM in AWS GovCloud). These deployment models are governed by the agency's own ATO process under FISMA and the NIST Risk Management Framework (RMF), not by FedRAMP.

TAC Deployment Scenarios for Federal Agencies

TAC's single-tenant Secure Virtual Appliance (SVA) architecture provides federal agencies with deployment flexibility that multi-tenant SaaS access platforms cannot offer. Three primary scenarios apply.

SCENARIO 1

On-Premises / Agency Data Centre Deployment

REQUIREMENT	HOW TAC DELIVERS
Infrastructure	Agency-owned and operated data centre, classified facility, or secure enclave. TAC SVA installed on agency-controlled virtualisation infrastructure (VMware, Hyper-V, KVM) or bare metal.
FedRAMP required?	No. On-premises software deployed within an agency's facility is outside FedRAMP scope. OMB M-24-15 explicitly excludes this deployment model.
Authorisation path	Agency ATO under FISMA and the NIST Risk Management Framework (RMF). Agency authorising official issues the ATO based on the agency's own assessment of TAC against applicable NIST 800-53 controls.
Data sovereignty	Complete — all access policy data, audit logs, and configuration remain within agency-controlled infrastructure. No external data transmission to PortSys or any third party.

REQUIREMENT	HOW TAC DELIVERS
Best for	Classified environments (SCIF, JWICS, SIPRNet), air-gapped networks, agencies requiring physical control of infrastructure, DoD components, intelligence community.

SCENARIO 2

Agency GovCloud Deployment

REQUIREMENT	HOW TAC DELIVERS
Infrastructure	TAC SVA deployed as a dedicated virtual machine in the agency's own government cloud tenancy — AWS GovCloud, Azure Government, or equivalent FedRAMP-authorised IaaS.
FedRAMP required for TAC?	Likely no. Per OMB M-24-15, single-agency systems hosted on cloud infrastructure that are not offered as shared services are excluded from FedRAMP scope. The underlying IaaS (AWS GovCloud, Azure Government) carries its own FedRAMP authorisation. TAC operates within the agency's existing authorisation boundary.
Authorisation path	Agency ATO under FISMA / NIST RMF. The agency or sponsor authorises TAC as part of their system boundary, leveraging the underlying IaaS FedRAMP authorisation. Final authorisation is the agency authorising official's decision.
Data sovereignty	Agency controls the cloud tenancy, encryption keys, network configuration, and the TAC instance itself. PortSys has no operational access to the deployment.
Best for	Agencies with existing GovCloud tenancies, hybrid cloud strategies, agencies seeking cloud elasticity while retaining full infrastructure control.

SCENARIO 3

Multi-Agency Shared Cloud Service (Not Currently Offered)

REQUIREMENT	HOW TAC DELIVERS
Hypothetical model	If PortSys were to offer TAC as a managed, multi-agency cloud service — where PortSys hosts and operates the infrastructure on behalf of multiple federal agencies — FedRAMP authorisation would be required.
FedRAMP required?	Yes. A cloud service offered to multiple federal agencies requires FedRAMP authorisation under OMB M-24-15.
Authorisation path	Formal FedRAMP authorisation through 3PAO assessment and agency or JAB sponsorship at the appropriate impact level.

REQUIREMENT	HOW TAC DELIVERS
Current status	**Not currently offered.** TAC is deployed within customer-controlled environments today. PortSys does not host or operate TAC on behalf of multiple agencies. This scenario is included for completeness; TAC's existing NIST 800-53 alignment would provide a strong foundation if this model is pursued in the future.

Why Single-Tenant Architecture Matters in Federal Environments

Most cloud-based access control platforms operate as multi-tenant Software-as-a-Service — federal agency data flows through shared infrastructure alongside commercial customers and other agencies. These platforms typically mitigate risk through logical separation, but the underlying infrastructure is shared. TAC takes a different architectural approach.

ARCHITECTURE

Single-Tenant SVA vs. Multi-Tenant SaaS

REQUIREMENT	HOW TAC DELIVERS
Infrastructure isolation	**TAC:** Dedicated, virtually isolated appliance per agency. No infrastructure shared with any other organisation. **Multi-tenant SaaS:** Logical separation within shared infrastructure. Multiple customers' data flows through the same underlying systems.
Data co-mingling risk	**TAC:** Architecturally not possible — no other organisation's data touches the infrastructure. **Multi-tenant SaaS:** Mitigated through controls; shared infrastructure creates theoretical exposure that must be addressed at the platform level.
Data sovereignty	**TAC:** Agency controls infrastructure, data residency, and encryption keys. **Multi-tenant SaaS:** Data resides in vendor-operated cloud; agency may not control data residency or have access to encryption keys.
Deployment location	**TAC:** Agency data centre, classified facility, GovCloud, air-gapped network, hybrid — wherever the mission requires. **Multi-tenant SaaS:** Limited to vendor's cloud regions; GovCloud options may be available but agency does not control underlying infrastructure.
Audit and inspection	**TAC:** Agency owns and can directly inspect the full deployment, including configuration, logs, and underlying VM. **Multi-tenant SaaS:** Agency cannot directly inspect vendor infrastructure; assurance comes from third-party attestations (e.g., FedRAMP authorisation, SOC 2 reports).
Noisy neighbour risk	**TAC:** Dedicated appliance; no resource contention with other customers. **Multi-tenant SaaS:** Shared infrastructure means one customer's load can theoretically impact others; mitigated through vendor capacity management.

For agencies handling CUI, classified information, or operating under ITAR restrictions, TAC's single-tenant model provides a level of data isolation that multi-tenant SaaS platforms cannot architecturally match.

NIST SP 800-53 Rev. 5 Control Family Alignment

FedRAMP authorisation is built on NIST SP 800-53 Rev. 5 controls. TAC addresses specific controls within the families most relevant to access control and zero-trust enforcement. Coverage levels below reflect what TAC addresses for the applications and systems it fronts; broader 800-53 requirements (physical, personnel, risk assessment, contingency planning) require complementary controls in the agency environment.

AC FAMILY

Access Control

REQUIREMENT	HOW TAC DELIVERS
AC-2 — Account management	Multi-directory identity federation (Active Directory, LDAP, SAML, RADIUS, OIDC, SQL, custom) connects simultaneously to all agency directory sources. Centralised policy engine enables account provisioning, modification, and revocation from a single console. Real-time access revocation when user status changes upstream.
AC-3 — Access enforcement	Reverse-proxy architecture enforces access decisions at the application layer. Every request passes through identity verification, MFA, device posture validation, and policy evaluation before reaching the target federal application. Applications behind TAC are not directly addressable.
AC-7 — Unsuccessful logon attempts	Configurable lockout policies and MFA step-up requirements after failed authentication attempts. All failed attempts logged with full context: identity, source, device, timestamp.
AC-12 — Session termination	Session timeout policies enforced at the proxy layer. Idle sessions terminate automatically. Policy changes take effect mid-session — access can be revoked immediately when device compliance lapses or user status changes.
AC-17 — Remote access	TAC reverse proxy provides authenticated, policy-governed remote access to federal applications without exposing network ports. All remote access passes through identity, MFA, and device posture validation through a single encrypted channel (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules). Can replace traditional VPN for application access.
AC-20 — Use of external systems	Continuous device posture validation ensures only compliant, known devices can access federal systems — including from external networks, contractor devices, or BYOD. Checks include OS version, patches, antivirus, disk encryption, firewall status, and domain join.

IA FAMILY

Identification and Authentication

REQUIREMENT	HOW TAC DELIVERS
IA-2 — Identification and authentication (organisational users)	Every user uniquely identified and authenticated against agency identity sources before any access to federal systems is granted. Service accounts and AI agents identified and authenticated under the same policy framework.
IA-2(1) — MFA for privileged accounts	MFA mandatory for all privileged access. FIDO2 / WebAuthn phishing-resistant authentication available — meeting OMB M-22-09 requirements for phishing-resistant MFA for federal employees and contractors.
IA-2(2) — MFA for non-privileged accounts	MFA enforced on all user access regardless of privilege level. Built-in methods include FIDO2 / WebAuthn, SafeLogin (proprietary), TOTP, push notifications, SMS, OTP, and hardware tokens. Third-party MFA integration with Duo, RSA, Swivel, biometric solutions, and others. All MFA methods included in base licence.
IA-3 — Device identification and authentication	Continuous device posture validation identifies and authenticates every device on every access request — OS version, patch level, certificate validity, domain join, and endpoint security state.
IA-5 — Authenticator management	Multi-directory federation manages authenticators across all connected identity sources. Credential lifecycle integrated with existing agency identity infrastructure. MFA enrolment, modification, and revocation events logged.
IA-8 — Identification and authentication (non-organisational users)	Contractor, partner, and third-party access governed by the same policy engine as agency users. No separate authentication path; no governance gaps. Service accounts and AI agents are first-class identities.

AU FAMILY

Audit and Accountability

REQUIREMENT	HOW TAC DELIVERS
AU-2 — Event logging	Every access event logged with full attribution: user identity, authentication method, device posture, source IP, geolocation, timestamp, application accessed, and policy decision. Logging is automatic and cannot be disabled for protected applications.
AU-3 — Content of audit records	Audit records include: who (user/service account/AI agent identity), what (application and action), when (timestamp), where (source IP, geolocation), how (authentication method, device posture), and outcome (policy decision, allow/deny/step-up).
AU-6 — Audit record review	TAC provides native real-time monitoring and alerting on access events and platform health. Centralised audit data exportable via syslog or API to your SIEM for downstream correlation, review, and forensic analysis.

REQUIREMENT	HOW TAC DELIVERS
AU-9 — Protection of audit information	Tamper-evident, centralised logging. Audit data cannot be modified through the TAC console. Administrative actions on the audit logging functionality are themselves logged.
AU-12 — Audit record generation	Audit records generated automatically for every access event — both successful and denied. No configuration required to capture baseline events. Service accounts and AI agents are uniquely logged.

SC FAMILY

System and Communications Protection

Scope note. TAC addresses boundary protection and cryptographic protection in transit. TAC does *not* address protection of federal data at rest (SC-28(1) cryptographic protection at rest), denial-of-service protection beyond reducing attack surface, or platform-level cryptographic key management for the agency environment broadly.

REQUIREMENT	HOW TAC DELIVERS
SC-5 — Denial-of-service protection (partial)	Federal applications are never directly exposed to the internet. TAC reverse proxy absorbs and filters all inbound traffic before it reaches protected systems. (Note: TAC does not replace dedicated DDoS protection infrastructure for the agency boundary.)
SC-7 — Boundary protection	Single encrypted-port architecture closes all inbound firewall ports except one TLS 1.2 or TLS 1.3 channel with FIPS 140-2 compliant cryptographic modules. Network boundary is clearly defined and minimised for the applications TAC fronts.
SC-8 — Transmission confidentiality and integrity	All traffic to and from protected applications encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. End-to-end encryption between the user's device and TAC, and between TAC and the backend application. Single encrypted channel for all access.
SC-28 — Protection of information at rest (partial)	Single-tenant SVA architecture ensures federal data processed through TAC is never co-mingled with other organisations' data. Dedicated infrastructure per agency deployment. (Note: TAC does not encrypt application data at rest; SC-28(1) requires complementary at-rest encryption controls.)

NIST SP 800-207 Zero Trust Architecture Alignment

Executive Order 14028 and OMB M-22-09 require federal agencies to adopt zero trust architecture. NIST SP 800-207 defines Zero Trust Architecture through three logical components: the **Policy Engine** (makes access decisions), the **Policy Administrator** (communicates decisions and manages sessions), and the **Policy Enforcement Point** (enforces decisions at the point of access). TAC implements all three components in a single platform, eliminating the integration complexity of multi-vendor zero trust architectures.

TAC aligns with the resource-portal deployment model described in 800-207 Section 3.2.1: a gateway-based reverse proxy that mediates access between subjects and enterprise resources. Applications behind TAC are never

directly addressable from any network. See the *TAC NIST Compliance Alignment Guide* for the complete 800-207 tenet mapping.

Federal Frameworks TAC Aligns With

TAC's NIST 800-53 and 800-207 foundation produces alignment with multiple federal frameworks and policy directives. Alignment below reflects technical capability fit; formal compliance with each framework requires the agency or contractor's complete control environment.

FRAMEWORK

Federal Compliance Alignment

REQUIREMENT	HOW TAC DELIVERS
NIST SP 800-53 Rev. 5	Aligned with controls across AC, IA, AU, SC families relevant to access control and zero-trust enforcement; partial alignment with CM and SI for the systems TAC fronts.
NIST SP 800-207	Implements Policy Engine, Policy Administrator, and Policy Enforcement Point in one platform. Aligns with the resource-portal gateway model (Section 3.2.1).
NIST SP 800-171 Rev. 2	Supports CUI protection requirements for defense contractors and non-federal organisations handling controlled information. See *TAC NIST Compliance Alignment Guide* for control mapping.
CMMC 2.0	Architecture supports Level 2 and Level 3 access control, identification and authentication, and audit practices for defense industrial base contractors.
CJIS Security Policy 5.9	Addresses access control, authentication, and audit requirements for criminal justice information. Complete CJIS compliance requires the agency's full security programme.
ITAR	Single-tenant on-premises and agency-cloud deployment supports International Traffic in Arms Regulations data sovereignty requirements. TAC does not itself handle ITAR-controlled data flow; it controls access to systems that do.
Executive Order 14028	Zero trust architecture mandate for federal agencies — TAC is a native ZTA implementation per NIST 800-207.
OMB M-22-09	Federal zero trust strategy implementation — TAC addresses identity (phishing-resistant MFA), device (continuous posture), network (boundary), and access (per-request policy) pillars.

Supporting Your Agency ATO

TAC is not currently FedRAMP authorised. For agencies pursuing an Authority to Operate for TAC under FISMA / NIST RMF, PortSys provides documentation and engineering support to assist with the assessment process.

ATO SUPPORT

Documentation and Engineering Support

REQUIREMENT	HOW TAC DELIVERS
NIST 800-53 control mapping documentation	Detailed control-by-control mapping at Moderate and High baselines, including implementation narratives and inheritance considerations.
NIST 800-207 ZTA alignment documentation	Mapping to all seven 800-207 tenets and the resource-portal deployment model.
System Security Plan (SSP) contribution materials	Reference architecture, control narratives, and component descriptions suitable for inclusion in the agency's SSP. Agency ISSO finalises the SSP based on the deployment context.
Architecture and integration documentation	Reference diagrams showing TAC integration with agency directory services, SIEM, ITSM, and network infrastructure. Deployment guides for on-premises, AWS GovCloud, Azure Government, and hybrid environments.
Audit log and SIEM integration specifications	Field-level documentation of audit log content, syslog and API export specifications, and sample SIEM correlation rules.
Continuous monitoring support	Documentation supporting the continuous monitoring requirements of the agency ATO, including configuration drift detection and policy change logging.
Direct engineering support	PortSys engineering resources engage directly with agency ISSOs and 3PAOs during assessment, responding to control implementation questions, providing evidence packages, and supporting POA&M activities.

Why TAC Is Strong for Federal Environments

Unified PE + PA + PEP — One Platform. NIST 800-207 defines three logical zero trust components: Policy Engine, Policy Administrator, and Policy Enforcement Point. TAC implements all three in a single integrated platform. No multi-vendor integration. No policy synchronisation drift. Decisions, communication, and enforcement happen in the same engine.

Single-Tenant by Design. Every TAC deployment is a dedicated, virtually isolated Secure Virtual Appliance. There is no shared infrastructure across agencies or customers. Federal assessors and agency ISSOs can verify data isolation directly — it is architectural, not contractual.

Phishing-Resistant MFA Included. TAC includes FIDO2 / WebAuthn authentication — satisfying OMB M-22-09 requirements for phishing-resistant MFA for federal employees and contractors. No additional identity provider purchase required. All MFA methods included in the base licence.

Legacy Federal Application Protection. Federal agencies operate some of the oldest application portfolios in existence. TAC injects MFA, device posture, and continuous validation in front of any application — including mainframe systems, thick-client applications, and forms-based logins — without any code changes.

Deploy Anywhere the Mission Requires. TAC deploys on-premises in agency facilities, in FedRAMP-authorised cloud regions (AWS GovCloud, Azure Government), in hybrid configurations, or in air-gapped environments. The customer controls the infrastructure; TAC adapts to the deployment model.

Federal Compliance Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
NIST SP 800-53 Rev. 5	AC, IA, AU, SC, CM, SI (selected controls)	AC-2/3/7/12/17/20, IA-2/3/5/8, AU-2/3/6/9/12, SC-5/7/8/28; partial CM and SI
NIST SP 800-207	Zero Trust Architecture (PE / PA / PEP)	All three logical ZTA components in one platform; resource-portal model
FedRAMP Program	NIST 800-53 alignment	Architected to NIST 800-53 Moderate and High baselines; NOT FedRAMP authorised
EO 14028 / OMB M-22-09	Federal zero trust strategy	Identity, device, network boundary, and access pillars addressed
OMB M-24-15	FedRAMP scope determination	On-premises and agency-tenancy deployments outside FedRAMP scope
CMMC 2.0 / 800-171	DIB contractor CUI protection	Supports Level 2/3 access control, IA, audit practices (see NIST guide)

Next Steps

Identify the deployment scenario. Determine which of the three deployment scenarios fits your agency's mission — on-premises, agency GovCloud, or future shared service. Each has different authorisation paths. **Request a federal walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your specific environment, identify the right authorisation path, and provide the documentation package to support your agency ATO process.