# GovDataHosting Cloud Platform
# Cloud Tenant Portal (CTP)

## Secure Configuration Guide

**PUBLIC RELEASE VERSION**

FedRAMP Rev5 Compliance Document

| | |
|---|---|
| **Document Title** | GovDataHosting Cloud Platform<br>Cloud Tenant Portal (CTP) - Public Release |
| **Version** | 2.0 |
| **Date** | February 26, 2026 |
| **Classification** | PUBLIC |
| **Prepared By** | IT-CNP, Inc. |
| **FedRAMP Baseline** | Rev5 — Moderate / High |
| **Applicability** | All CTP environments and customer tenants |
| **Document Integrity** | SHA-256 checksum published at www.govdatahosting.com/SCG |

# Document Revision History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 2026-02-26 | IT-CNP, Inc. Office | Initial release — Internal version |
| | | | |

# Table of Contents

# 1. Introduction

The GovDataHosting Cloud Platform Cloud Testing Platform (CTP) is a multi-tenant, cloud-based infrastructure management portal designed for government agencies and enterprise organizations that require secure, compliant, and auditable cloud resource provisioning and management. CTP provides a centralized web interface through which authorized personnel can manage cloud infrastructure accounts, provision and monitor compute resources, configure network and security controls, manage billing and cost allocation, and oversee change management workflows - all within a framework that enforces the security and compliance requirements of federal information systems. GovDataHosting is a cloud hosting division of IT-CNP, Inc.

This Secure Configuration Guide (SCG) has been developed in accordance with the Federal Risk and Authorization Management Program (FedRAMP) Revision 5 requirements, specifically addressing the SCG-CSO-RSC, SCG-CSO-AUP, SCG-CSO-PUB, and SCG-CSO-SDF directives. The guide serves as a comprehensive reference for CTP administrators, customer organization administrators, and security personnel responsible for the secure configuration and ongoing operation of the platform.

The CTP platform operates within a shared responsibility model. CTP is responsible for the security of the platform itself — including the application layer, the underlying infrastructure, cryptographic protections, and the enforcement of access controls. Customer organizations are responsible for securely managing their own user accounts, configuring organizational policies within the boundaries provided by the platform, and ensuring that their use of CTP aligns with their own security policies and compliance requirements.

This public release version of the SCG provides configuration guidance using implementation-agnostic language to protect operational security while fully meeting FedRAMP transparency requirements. A restricted version containing full implementation details is available to authorized administrators and security assessors under appropriate access controls.

# 2. Purpose and Scope

## 2.1 Purpose

The purpose of this Secure Configuration Guide is to:

- Provide clear, actionable instructions for the secure initial configuration and ongoing operation of the CTP platform.
- Document all security-related settings available to administrators and explain their implications for the security posture of the system.
- Establish recommended secure defaults and explain the rationale behind each recommendation.
- Enable customer organizations to assess and verify the security configuration of their CTP tenant.
- Support continuous monitoring activities by defining the expected secure state of the platform.
- Satisfy FedRAMP Rev5 requirements for cloud service providers to maintain and publish secure configuration guidance.

## 2.2 Scope

This guide covers the following areas of the CTP platform:

- Administrative Account Lifecycle — Creation, configuration, privilege assignment, emergency access, monitoring, and decommissioning of all administrative account types.
- Authentication Configuration — Identity provider integration (OIDC), multi-factor authentication (MFA) enforcement, password policy configuration, CAC/PIV support, system use notification, and session management.
- Authorization and Access Control — Role-based access control (RBAC) configuration, permission assignments, just-in-time privileged access, privilege escalation prevention, and least-privilege enforcement.

- Network Security — Transport Layer Security (TLS) configuration, FIPS-validated cryptographic modules, DNSSEC, IP access restrictions, security group management, Web Application Firewall (WAF) rules, and egress filtering.
- Data Protection — Encryption at rest and in transit using FIPS validated modules, sensitive data handling, database security configuration, and secrets management.
- Audit and Monitoring — Audit log configuration, security event monitoring, alerting policies, and log retention.
- Change Management — Approval workflows, resource modification controls, and infrastructure change governance.
- Vulnerability Management — Scanning configuration, STIG compliance checking, and remediation workflows.
- Backup and Recovery — Backup policy configuration, disaster recovery settings, and data restoration procedures.
- Decommissioning — Secure removal of accounts, organizations, and associated data.

### 2.3 Exclusions

This guide does not cover:

- Physical security controls of the underlying data center infrastructure (managed by the hosting provider).
- Operating system hardening of the underlying container runtime (managed by the hosting provider).
- Configuration of external identity providers beyond the CTP integration points — these are documented separately by the identity provider administrator.
- Third-party tool configuration (e.g., SIEM, vulnerability scanners) beyond the CTP integration interfaces.
- Implementation-specific details (technology stack, internal architecture, exact security parameters) — these are documented in the Restricted version of this guide available to authorized personnel.

## 3. Intended Audience

| Audience | Relevant Sections |
|---|---|
| **CTP Platform Administrators (CTP Super Admin, CTP Admin)** | All sections — responsible for platform-wide security configuration |
| **Customer Organization Administrators (Org Admin)** | Sections 6–9, 12–14, 18–19 — responsible for tenant-level configuration |
| **Security Assessors and Auditors** | Sections 7, 10–12, 16, Appendices A–B — for compliance verification |
| **Information System Security Officers (ISSOs)** | All sections — for continuous monitoring and risk assessment |
| **FedRAMP Reviewers** | All sections — for authorization assessment |

## 4. How to Obtain and Use This Guide

### 4.1 Obtaining the Guide (SCG-CSO-AUP / SCG-CSO-PUB)

This Secure Configuration Guide is publicly available to support transparency and enable prospective customers to evaluate the security posture of the platform before onboarding. The guide can be obtained through the following channels:

1. CTP Public Documentation Site — The latest version of this guide is published at: [URL TO BE PROVIDED]. The page includes the document, its SHA-256 integrity checksum, and a change summary for each version.
2. FedRAMP Authorization Package — This guide is included as an artifact in the CTP FedRAMP authorization package, available to authorized agency reviewers through the FedRAMP Marketplace.
3. Direct Request — Organizations considering CTP may request a copy by contacting CTP support at the email address provided in their service agreement or through the public contact form on the CTP website.
4. CTP Documentation Portal (Authenticated) — Authenticated CTP users with an administrative role can access both this public version and the restricted version through the CTP documentation portal.

## 4.2 Document Integrity Verification (SCG-ENH Integrity)

Each release of this guide is accompanied by a SHA-256 checksum published at the same URL as the document. To verify document integrity:

1. Download the SCG document and the associated checksum file.
2. Compute the SHA-256 hash of the downloaded document using a trusted tool.
3. Compare the computed hash with the published checksum. If they match, the document has not been modified in transit.

*Version 2.0 SHA-256 Checksum: [TO BE COMPUTED UPON FINAL PUBLICATION]*

## 4.3 Customer Acknowledgment Process

Customer organizations are required to formally acknowledge receipt and review of this SCG at the following milestones:

- During initial onboarding — The designated Organization Administrator must confirm receipt and review of the current SCG version before the tenant is activated for production use.
- After each major version update — Organization Administrators are notified of SCG updates and must acknowledge review of the updated guide within 30 days of publication.

Acknowledgment records are maintained in the CTP platform and are available for audit purposes.

## 4.4 Using the Guide

This guide should be used in the following contexts:

- Initial Deployment — When a new CTP tenant is provisioned, the Organization Administrator should review this guide and verify that all security settings are configured in accordance with the recommendations.
- Ongoing Operations — Administrators should reference this guide when making changes to security-related settings.
- Security Assessments — Auditors and security assessors should use this guide as a baseline. The configuration checklist in Appendix A provides a structured format for assessment activities.
- Incident Response — This guide provides a reference for the expected secure state, enabling rapid identification of configuration deviations.
- Continuous Monitoring — This guide defines the expected configuration state against which continuous monitoring tools compare actual system state.

## 4.5 Document Maintenance

This guide is reviewed and updated:

- At least annually as part of the FedRAMP continuous monitoring program.
- Whenever significant changes are made to the CTP platform that affect security-related settings.

- When new FedRAMP requirements or guidance are published that necessitate updates.

Version history is maintained in Appendix D. Changes between versions are highlighted to enable administrators to identify and apply updated recommendations. Customers are notified of updates via the CTP notification system and email.

# 5. CTP Platform Overview

## 5.1 System Description

The Cloud Testing Platform (CTP) is a web-based, multi-tenant Software-as-a-Service (SaaS) application that provides government agencies and enterprise organizations with a centralized portal for managing cloud infrastructure testing environments. CTP enables authorized users to:

- Manage Organizations and Accounts — Create, configure, and manage hierarchical customer organizations with multiple cloud accounts, each isolated within dedicated organizational units.
- Provision Cloud Infrastructure — Deploy and manage virtual private clouds, subnets, security groups, compute instances, load balancers, DNS records, and TLS certificates through a guided, policy-enforced workflow.
- Enforce Change Management — Submit, review, and approve infrastructure changes through a configurable approval workflow that ensures all modifications are authorized and documented.
- Monitor and Audit — Track all user actions, infrastructure changes, and security events through a comprehensive audit logging system.
- Manage Security Controls — Configure and monitor Web Application Firewall (WAF) rules, security group policies, egress filtering, and vulnerability scanning.
- Oversee Billing and Cost Allocation — Track cloud resource usage, generate invoices, and allocate costs across organizational units and projects.
- Ensure Compliance — Enforce security baselines, run STIG compliance checks, and maintain audit trails for regulatory compliance.

## 5.2 Architecture Overview

CTP employs a modern, multi-tier architecture with clear separation of concerns:

- Presentation Layer — A server-rendered web interface with responsive design, providing a consistent user experience across devices.
- Application Layer — A server-side web application framework handling business logic, authentication and authorization enforcement, input validation, and API routing.
- Data Layer — An enterprise relational database management system providing ACID-compliant data storage with encryption at rest using FIPS validated cryptographic modules and encrypted connections.
- Infrastructure Layer — Containerized deployment on a serverless compute platform with automatic scaling, health monitoring, and zero-downtime deployments.
- Integration Layer — Secure API integrations with identity providers (OIDC/OAuth 2.0), cloud infrastructure provisioning services, email services, and ticketing systems.

All components communicate using FIPS validated TLS implementations. Detailed architecture diagrams and technology-specific information are available in the Restricted version of this guide.

## 5.3 Deployment Environments

| Environment Type | Description | Use Case |
|---|---|---|
| **Cloud-Hosted** | Fully managed deployment on cloud infrastructure | Standard PaaS offering for production, development and testing |

Each deployment environment is fully isolated, with dedicated compute resources, databases, and network configurations. No data is shared between environments or tenants.

## 5.4 Shared Responsibility Model

### CTP Responsibilities

- Application security (code quality, vulnerability remediation, secure coding practices)
- Secure default configuration of all platform settings
- Encryption of data at rest and in transit using FIPS 3 validated cryptographic modules
- Authentication and authorization framework implementation
- Audit logging and security event generation
- Platform availability and incident response
- Regular security assessments and penetration testing
- Timely patching of application-level vulnerabilities
- Maintenance of FIPS 140 validation status for all cryptographic modules

### Customer Organization Responsibilities

- Managing user accounts and access within their organization
- Configuring organization-specific security policies (within platform capabilities)
- Reviewing audit logs for their organizational scope
- Reporting security concerns to CTP support
- Ensuring end-user devices meet organizational security requirements, including the use of approved privileged access workstations for administrative functions
- Managing their identity provider configuration (when using customer-managed IdP), including CAC/PIV integration
- Approving or denying change requests within their organization
- Acknowledging receipt and review of SCG updates

### Hosting Provider Responsibilities

- Physical security of data centers
- Hypervisor and host operating system security
- Network infrastructure security
- Hardware maintenance and replacement
- Environmental controls (power, cooling, fire suppression)
- FIPS 140 validation of underlying cryptographic services

# 6. Administrative Account Management

This section provides instructions on how to securely access, configure, operate, and decommission top-level administrative accounts within the CTP platform, as required by FedRAMP SCG-CSO-RSC.

## 6.1 Administrative Account Types

CTP implements a hierarchical administrative customer account structure with distinct privilege levels:

| Account Type | Role Level | Scope | Description |
|---|---|---|---|
| **Organization Admin** | Organization | Single Organization | Full administrative control within a single customer organization, including user management, account configuration, and policy settings. |
| **Project Admin** | Functional | Assigned Projects | Administrative access to specific projects within an organization, including infrastructure provisioning and change management. |
| **Security Admin** | Functional | Assigned Accounts | Administrative access to security features including WAF management, threat detection findings, and compliance scanning. |
| **Finance Admin** | Functional | Assigned Accounts | Administrative access to billing, invoicing, and cost allocation features. |
| **Technical Admin** | Functional | Assigned Accounts | Administrative access to infrastructure provisioning, networking, and compute management. |

## 6.2 Initial Administrative Account Provisioning

### 6.2.1 CTP Platform Administrator Accounts

CTP platform administrator accounts are provisioned through a controlled, auditable process:

1. A request for a new CTP platform administrator account is submitted through the CTP change management system, including the justification for access, the specific role required, and the duration of access (if temporary).
2. The request must be approved by an existing CTP Super Admin and must comply with the principle of least privilege.
3. The identity of the new administrator is verified through the organization's identity management process.
4. The account is created in the identity provider (IdP) with the appropriate role assignment. The initial password is generated according to the platform's password policy and must be changed on first login.
5. Multi-factor authentication enrollment is mandatory for all CTP platform administrator accounts. The new administrator must enroll an MFA device before the account becomes fully active.
6. The account creation event is recorded in the audit log, including the approver, creation timestamp, and assigned role.

**Security Recommendation:** Limit the number of CTP Super Admin accounts to the minimum required for operational continuity. All CTP Super Admin actions should be reviewed by a second administrator on a regular basis.

### 6.2.2 Customer Organization Administrator Accounts

Customer organization administrator accounts are provisioned as part of the customer onboarding process:

1. During customer onboarding, the customer designates one or more individuals to serve as Organization Administrators.
2. A CTP Admin sends an invitation through the CTP user invitation system. Invitations include a unique, time-limited registration link.
3. The invited individual completes registration through the identity provider, creating their account with a compliant password.
4. Multi-factor authentication enrollment is required during the initial registration process.
5. The CTP Admin assigns the Organization Admin role to the newly registered account.
6. The customer organization verifies that the correct individuals have been granted administrative access.

**Security Recommendation:** Each customer organization should have at least two Organization Administrators to ensure continuity of operations. Organization Administrators should review their organization's user roster at least quarterly.

### 6.2.3 Functional Administrator Accounts

Functional administrator accounts (Project Admin, Security Admin, Finance Admin, Technical Admin) are created by Organization Administrators within their organizational scope following the same invitation, registration, and MFA enrollment process described above. Functional roles should be assigned based on job responsibilities, following the principle of least privilege. Avoid assigning Organization Admin roles when a functional role would suffice.

## 6.3 Secure Access to Administrative Accounts

### 6.3.1 Authentication Requirements

All administrative access to CTP requires:

- HTTPS Connection — All access to CTP must occur over HTTPS using FIPS validated TLS implementations. Unencrypted connections are automatically redirected to HTTPS.
- Identity Provider Authentication — Users authenticate through the configured OIDC-compliant identity provider. Direct database authentication is not supported.
- Multi-Factor Authentication — MFA is required for all administrative accounts. Supported MFA methods include hardware security keys and CAC/PIV HSPD-12 smart cards.
- System Use Notification — All users must acknowledge the system use notification banner before accessing the platform (see Section 8.4).

### 6.3.2 Privileged Access Workstation Requirements

Administrative access to CTP must be performed from approved devices that meet the following minimum requirements:

- The device must be managed by the organization and enrolled in the organization's endpoint management system.
- The device must have current operating system patches and endpoint protection software.
- Full disk encryption must be enabled.
- Screen lock must be configured with an inactivity timeout no greater than 15 minutes.
- The device must not be a shared or public-use workstation.
- For CTP Super Admin and CTP Admin accounts, a dedicated privileged access workstation (PAW) or equivalent hardened endpoint is strongly recommended.

**Security Recommendation:** Organizations should maintain an inventory of approved devices for administrative access and review this inventory quarterly. Access from unapproved devices should be blocked through conditional access policies at the identity provider level.

### 6.3.3 Administrator Credential Storage

Administrative credentials must be managed securely:

- Passwords must be stored in an enterprise-grade password manager approved by the organization. Plaintext credential storage (including sticky notes, spreadsheets, text files, or email) is prohibited.
- Hardware security keys must be physically secured when not in use and must not be shared between individuals.
- Recovery codes generated during MFA enrollment must be stored in a separate secure location from the primary credentials (e.g., a sealed envelope in a physical safe, or a separate compartment in the password manager).

### 6.3.4 Access Procedures

To securely access a CTP administrative account:

1. Navigate to the CTP login page using a current, supported web browser over HTTPS from an approved device.
2. Read and acknowledge the system use notification banner.
3. Click 'Sign In' to be redirected to the identity provider login page.
4. Enter your registered email address and password.
5. Complete the MFA challenge using your enrolled MFA device.
6. Upon successful authentication, you will be redirected to the CTP dashboard with access corresponding to your assigned role.

### 6.3.5 Session Security

Once authenticated, the following session security controls are enforced:

- Session Timeout — Administrative sessions expire after a configured period of inactivity. Upon timeout, the user must re-authenticate.
- Maximum Session Duration — Sessions have an absolute maximum lifetime regardless of activity, after which re-authentication is required.
- Session Regeneration — Session identifiers are regenerated upon successful authentication to prevent session fixation attacks.
- Single Active Session — By default, only one active session per user account is permitted. A new login invalidates any existing sessions.
- Secure Cookie Configuration — Session cookies are configured with industry-standard security attributes to prevent interception and cross-site attacks.

## 6.4 Configuring Administrative Accounts

### 6.4.1 Profile Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Display Name** | Use the administrator's official name as registered in the organization's identity management system | Ensures accurate attribution in audit logs and supports accountability. |
| **Email Address** | Use an organizational email address; personal email addresses should not be used for administrative accounts | Ensures notifications reach the organization and supports account recovery through organizational processes. |
| **MFA Devices** | Enroll at least one MFA device to prevent lockout; one hardware key and one authenticator application is recommended | Multiple enrolled devices provide resilience against device loss while maintaining strong authentication. |

### 6.4.2 Notification Preferences

Administrators can configure notifications for security-relevant events including: infrastructure change requests requiring approval, new user registrations, security alerts (WAF triggers, threat detection findings, compliance scan results), billing alerts, and system maintenance notifications.

**Security Recommendation:** Administrative accounts should have notifications enabled for all security-relevant events. Disabling security notifications is not recommended and may impact the organization's ability to respond to security incidents in a timely manner.

## 6.5 Operating Administrative Accounts

### 6.5.1 Principle of Least Privilege

- Use the lowest privilege role that is sufficient for the task being performed.
- Do not share administrative credentials between individuals.
- Do not use administrative accounts for routine, non-administrative tasks.
- Review and remove unnecessary privilege assignments on a regular basis (at least quarterly).

### 6.5.2 Just-in-Time (JIT) Privileged Access

CTP supports a just-in-time privileged access model for temporary elevation of access rights:

1. A user submits a request for temporary elevated access through the CTP access request interface, specifying the role needed, the justification, and the duration required.
2. An authorized approver (Organization Admin or higher) reviews and approves or denies the request. Self-approval is not permitted.
3. Upon approval, the elevated role is assigned with an automatic expiration timestamp.
4. The user performs the required administrative tasks within the approved time window.
5. At expiration, the elevated role is automatically revoked. Manual early revocation is also available.
6. The complete lifecycle of the elevation (request, approval, activation, actions performed, expiration/revocation) is recorded in the audit log.

**Security Recommendation:** JIT access should be the preferred method for performing infrequent administrative tasks. Standing elevated access should be reserved for roles that require continuous administrative capability.

### 6.5.3 Administrative Actions Subject to Audit

All administrative actions are recorded in the CTP audit log. The following categories of actions generate audit events:

| Action Category | Examples | Audit Detail Level |
|---|---|---|
| **Account Management** | User creation, role changes, account deactivation, JIT access requests | Full — includes before/after state |
| **Organization Management** | Organization creation, configuration changes, account provisioning | Full — includes all modified fields |
| **Infrastructure Changes** | VPC creation, security group modification, instance provisioning | Full — includes resource details and provisioning information |
| **Security Configuration** | WAF rule changes, security group modifications, compliance scan initiation | Full — includes before/after configuration state |
| **Authentication Events** | Login success, login failure, MFA challenge, session timeout, banner acknowledgment | Full — includes source IP, user agent, and outcome |
| **Approval Workflows** | Change request submission, approval, denial, escalation | Full — includes all decision details and comments |

### 6.5.4 Regular Administrative Reviews

| Review Activity | Frequency | Responsible Role |
|---|---|---|
| User access review (active accounts, role assignments) | Quarterly | Organization Admin |
| Privileged account activity review | Monthly | CTP Admin |
| Audit log review for anomalous activity | Weekly | Security Admin or ISSO |
| Security configuration baseline verification | Monthly | CTP Admin |
| MFA enrollment verification | Quarterly | Organization Admin |
| Dormant account identification and remediation | Quarterly | Organization Admin |
| JIT access usage review | Monthly | Organization Admin |
| Privileged access workstation inventory review | Quarterly | Organization Admin |

## 6.6 Emergency Access (Break-Glass) Procedures

In the event that all active CTP platform administrators are unavailable (e.g., simultaneous incapacitation, natural disaster, or compromised credentials requiring mass revocation), CTP maintains emergency access procedures:

1. Emergency Access Credentials — A dedicated emergency access account is maintained with sealed credentials stored under dual-custody controls (two authorized personnel are required to retrieve the credentials). The sealed credentials are stored in a physical safe or equivalent high-security storage at a location documented in the organization's contingency plan.
2. Activation — Emergency access may only be activated when normal administrative access is unavailable. Activation requires authorization from the CTP Information System Security Officer (ISSO) or their designated alternate, plus one member of organizational leadership.
3. Scope — The emergency access account provides the minimum privileges necessary to restore normal administrative access (e.g., resetting MFA for an existing administrator, creating a new administrator account). It does not provide unrestricted platform access.
4. Time Limitation — Emergency access sessions are limited to a maximum of 4 hours. The account is automatically disabled after this period.
5. Mandatory Audit Review — All actions performed during an emergency access session are recorded in the audit log. A complete review of all emergency session actions must be conducted by the ISSO within 24 hours of the session.
6. Post-Incident Report — A written report documenting the circumstances requiring emergency access, all actions taken, and any follow-up actions required must be completed within 72 hours and retained for audit purposes.
7. Credential Rotation — After any use of emergency access credentials, the sealed credentials must be rotated and resealed under dual-custody controls within 24 hours.

**Security Recommendation:** Emergency access credentials should be tested at least annually to verify they function correctly. Testing should follow the full activation procedure and be documented as a planned test in the audit log.

## 6.7 Decommissioning Administrative Accounts

When an administrative account is no longer needed, it must be decommissioned through a controlled process:

1. A decommissioning request is submitted, specifying the account to be decommissioned and the reason.

2. If the account is the sole administrator for any resources or organizations, administrative responsibilities must be transferred to another authorized individual before decommissioning.
3. The account's role assignments are removed in CTP, and the account is deactivated in the identity provider.
4. Any active sessions for the account are immediately terminated.
5. MFA devices associated with the account are de-enrolled.
6. The decommissioning event is recorded in the audit log, including the reason for decommissioning and the authorizing administrator.
7. A second administrator verifies that the account can no longer access the system.

**Security Recommendation:** Accounts should be decommissioned within 24 hours of the triggering event (e.g., employee departure, role change). Decommissioned accounts are retained in a deactivated state for audit trail purposes but cannot be used to authenticate.

# 7. Security-Related Settings and Their Implications

This section documents all security-related settings that can be operated by administrative accounts, along with their recommended values and the security implications of each setting. This fulfills FedRAMP requirement SCG-CSO-RSC. For each setting, a verification method is provided to enable independent confirmation that the setting is correctly configured.

## 7.1 Platform-Level Settings (CTP Admin and Above)

### 7.1.1 Session Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Session Timeout (Idle)** | Configured per role tier (see Section 13.3) | Shorter timeouts limit the window for session hijacking on unattended workstations. Longer timeouts improve usability but increase risk. |
| **Maximum Session Duration** | Configured per role tier (see Section 13.3) | Absolute maximum session lifetime regardless of activity. After this period, re-authentication is required. |
| **Concurrent Session Limit** | One active session per user | Restricting users to a single active session prevents credential sharing and reduces the attack surface. |
| **Session Cookie Security** | All industry-standard security attributes enabled | Session cookies are protected against interception and cross-site attacks. These settings must remain enabled. |

**Verification:** Navigate to Platform Settings > Session Configuration to view current values. Verify cookie attributes using browser developer tools (Application > Cookies) on any CTP page.

### 7.1.2 Password Policy

The following password policy settings are configured at the identity provider level and enforced for all CTP users:

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Minimum Password Length** | 14 characters or greater | Longer passwords are significantly more resistant to brute-force and dictionary attacks. Aligns with NIST SP 800-63B and FedRAMP Moderate/High baselines. |
| **Complexity Requirements** | At least 3 of 4 character types (uppercase, lowercase, digits, special characters) | Character diversity increases the search space for password-guessing attacks. Overly strict requirements can lead to predictable patterns. |
| **Password History** | Remember previous passwords per organizational policy | Prevents users from cycling through a small set of passwords. |
| **Maximum Password Age** | 365 days (or event-driven change on suspected compromise) | Aligns with NIST SP 800-63B guidance against arbitrary rotation. The maximum age serves as a safety net. |
| **Account Lockout** | Configured with industry-standard thresholds | Limits brute-force attack effectiveness. After the configured number of failed attempts, the account is temporarily locked. |

| | | |
|---|---|---|
| **Prohibited Passwords** | Common passwords, dictionary words, and passwords from known breach databases are blocked | Prevents use of easily guessable passwords. |

**Verification:** Password policy settings are configured and verified at the identity provider. Organization Administrators can view the effective policy in Organization Settings > Authentication Policy.

### 7.1.3 Multi-Factor Authentication (MFA)

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **MFA Enforcement** | Required for all users | MFA significantly reduces the risk of account compromise from stolen credentials. Disabling MFA is strongly discouraged and may violate FedRAMP requirements. |
| **Allowed MFA Methods** | Hardware MFA token issued by GovDataHosting or Government. | Hardware security keys or CAC/PIV provide the strongest phishing-resistant protection. |
| **MFA Re-authentication** | Every login session | MFA is required at the start of each new session. |
| **Recovery Codes** | Generated at MFA enrollment | Recovery codes provide a fallback if the MFA device is lost. Must be stored securely per Section 6.3.3. |

**Verification:** Navigate to Platform Settings > Authentication to confirm MFA enforcement status. Verify individual enrollment via User Management > [User] > MFA Status.

### 7.1.4 TLS Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Minimum TLS Version** | TLS 1.2 | TLS 1.0 and 1.1 contain known vulnerabilities and are deprecated. CTP enforces TLS 1.2 as the minimum. All TLS implementations use FIPS validated cryptographic modules. |
| **Preferred TLS Version** | TLS 1.3 | TLS 1.3 provides improved security through simplified handshake, forward secrecy by default, and removal of legacy cipher suites. |
| **Cipher Suites** | FIPS-approved algorithms | Only FIPS-approved algorithms are permitted. Legacy cipher suites are disabled. |
| **HTTP Strict Transport Security (HSTS)** | Enabled with long-duration max-age and includeSubDomains | HSTS instructs browsers to only connect via HTTPS, preventing protocol downgrade attacks. |
| **HTTP to HTTPS Redirect** | Enabled | All unencrypted requests are automatically redirected to HTTPS. This setting must remain enabled. |

**Verification:** TLS configuration can be verified using external TLS testing tools (e.g., SSL Labs). HSTS headers can be verified in browser developer tools (Network > Response Headers).

### 7.1.5 Security Headers

CTP configures security response headers to mitigate common web application attack vectors:

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Content-Security-Policy** | Restrictive policy limiting content sources | Mitigates XSS and data injection attacks by restricting sources from which content can be loaded. Prevents the application from being embedded in frames (clickjacking protection). |
| **X-Frame-Options** | DENY | Prevents the application from being embedded in frames or iframes, mitigating clickjacking attacks. |
| **X-Content-Type-Options** | nosniff | Prevents browsers from MIME-type sniffing, which can lead to XSS through content type confusion. |
| **Referrer-Policy** | Restrictive policy balancing functionality and privacy | Controls referrer information included with requests, balancing functionality and privacy. |
| **Permissions-Policy** | Restrictive policy disabling unnecessary browser features | Restricts access to browser features not needed by the application, reducing the attack surface. |

**Verification:** Security headers can be verified using browser developer tools (Network > Response Headers) or external header testing tools on any CTP page.

## 7.2 Organization-Level Settings (Organization Admin and Above)

### 7.2.1 User Invitation Settings

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Invitation Expiration Period** | Configured per organizational policy (recommended: 72 hours or less) | Limits the window during which an intercepted invitation link could be used. |
| **Auto-Approval of User Registration** | Disabled | When disabled, new user registrations require explicit approval from an Organization Admin, preventing unauthorized access through compromised invitation links. |

**Verification:** Navigate to Organization Settings > User Management to view invitation policy configuration.

### 7.2.2 Change Management Settings

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Change Request Approval Required** | Enabled | All infrastructure changes must be submitted as change requests and approved before execution. Disabling is not recommended for production environments. |
| **Minimum Approvers** | 1 or more (configurable) | Higher values provide stronger governance. For FedRAMP environments, at least one approver is required. |
| **Self-Approval** | Disabled | Prevents users from approving their own changes, enforcing separation of duties. |

| | | |
|---|---|---|
| **Auto-Approve Threshold** | Disabled | Not recommended for FedRAMP environments where all infrastructure changes should be reviewed. |
| **Change Request Expiration** | Configured per organizational policy (recommended: 30 days) | Prevents stale change requests from being approved after context has changed. |

**Verification:** Navigate to Organization Settings > Change Management to view approval workflow configuration.

### 7.2.3 Notification and Alerting Settings

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Security Alert Notifications** | Enabled for all Organization Admins | Ensures prompt notification of security-relevant events for timely incident response. |
| **Failed Login Notifications** | Enabled with configured threshold | Enables early detection of brute-force attacks against accounts within the organization. |
| **Infrastructure Change Notifications** | Enabled for all Admins | Ensures awareness of all infrastructure modifications, supporting change management governance. |
| **Billing Alert Thresholds** | Configured per organizational policy | Cost anomalies can indicate unauthorized resource provisioning. |

**Verification:** Navigate to Organization Settings > Notifications to view alerting configuration.

## 7.3 Account-Level Settings

### 7.3.1 Security Group Defaults

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Default Inbound Rule** | Deny All | No inbound traffic is permitted to newly created resources. Administrators must explicitly allow required traffic. |
| **Default Outbound Rule** | Deny All (with exceptions for required services) | Restricting outbound traffic prevents compromised resources from communicating with unauthorized external systems. |
| **Security Group Rule Justification Required** | Enabled | Administrators must provide a justification for each security group rule, supporting audit and compliance activities. |

**Verification:** Create a new security group and verify that no inbound rules exist by default. Navigate to Account Settings > Security to verify justification requirements.

### 7.3.2 Instance Provisioning Defaults

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Allowed Instance Types** | Configured per organizational policy | Restricting instance types prevents provisioning of unnecessarily large resources. |

| | | |
|---|---|---|
| **Required Tags** | Owner, Purpose, Environment, Expiration | Mandatory tagging ensures all resources are identifiable, attributable, and subject to lifecycle management. |
| **Auto-Termination Policy** | Enabled with configurable threshold | Resources exceeding their intended lifecycle are flagged for review or termination. |

**Verification:** Navigate to Account Settings > Provisioning Policy to view instance restrictions and tagging requirements.

### 7.3.3 WAF Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Managed Rule Groups** | Core protection rule sets enabled (OWASP Top 10, known bad inputs, injection protection, XSS protection) | Managed rules provide regularly updated protection against common web application attack vectors. Disabling exposes the application to known attack patterns. |
| **Rate Limiting** | Enabled with configurable thresholds | Prevents denial-of-service attacks and brute-force attempts. |
| **Geo-Blocking** | Configured per organizational policy | Restricting access by geographic region reduces the attack surface. |
| **Custom Rule Override** | Requires Security Admin or higher | Custom overrides should be carefully reviewed and documented. See Section 15.3 for guidance. |

**Verification:** Navigate to Security > WAF Configuration to view enabled rule groups, rate limiting settings, and any active overrides.

# 8. Authentication and Identity Management

## 8.1 Identity Provider Integration

CTP uses OpenID Connect (OIDC) for authentication, integrating with enterprise-grade identity providers. The platform supports the following configurations:

| Configuration | Description | Recommended For |
|---|---|---|
| **Managed IdP** | CTP-managed identity provider for non-production environments | Non-production environments, initial onboarding |
| **Customer-Managed IdP** | Customer-operated identity provider integrated through OIDC | Production environments, organizations with existing IdP infrastructure |
| **Federated IdP** | Customer's existing IdP federated through a broker | Large enterprises with established identity management programs |

### 8.1.1 OIDC Configuration Parameters

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Discovery URL** | OIDC provider's well-known configuration endpoint | Must use HTTPS. Provides all endpoints and public keys needed for token validation. |
| **Client ID** | Unique identifier for the CTP application registered with the IdP | Not considered secret but should not be publicly disclosed unnecessarily. |
| **Client Secret** | Confidential key for server-to-server communication | Must be stored securely (encrypted at rest) and never exposed in client-side code or logs. |
| **Redirect URI** | CTP endpoint for post-authentication redirect | Must exactly match the registered URI to prevent authorization code interception attacks. |
| **Scopes** | OIDC scopes requested during authentication | CTP requests standard identity scopes. Additional scopes should only be requested if needed. |

## 8.2 Multi-Factor Authentication (MFA)

### 8.2.1 MFA Policy

- MFA is mandatory for all CTP users, regardless of role.
- MFA enrollment must be completed during the initial account registration process.
- Users who have not enrolled in MFA cannot access any CTP functionality.
- MFA bypass is not configurable through the CTP interface — it must be managed through the identity provider for emergency access scenarios only (see Section 6.6).

### 8.2.2 Supported MFA Methods

| Method | Strength | Recommendation |
|---|---|---|
| **Hardware Security Key** | Highest | Strongly recommended for all administrative accounts. Phishing-resistant. |

| | | |
|---|---|---|
| **CAC/PIV Smart Card (via IdP)** | Highest | Strongly recommended for federal agency users. Phishing-resistant. Requires customer IdP configuration for certificate-based authentication. |

### 8.2.3 CAC/PIV Authentication

CTP supports CAC/PIV (Common Access Card / Personal Identity Verification) authentication through the integrated identity provider:

- The customer-managed identity provider must be configured to accept certificate-based authentication from CAC/PIV smart cards.
- The IdP validates the certificate chain against the Federal PKI trust anchor.
- Certificate revocation checking (CRL or OCSP) must be enabled at the IdP level.
- CTP receives the authenticated identity through standard OIDC claims after the IdP has completed certificate validation.
- CAC/PIV authentication satisfies the MFA requirement as the smart card provides both the possession factor (the card) and the knowledge factor (the PIN).

**Security Recommendation:** Federal agency customers should configure their IdP for CAC/PIV as the primary authentication method. CTP support can provide integration guidance for common identity provider configurations.

### 8.2.4 MFA Recovery

In the event that an administrator loses access to their MFA device:

1. The administrator contacts their Organization Admin (or CTP Admin for platform administrators).
2. The administrator's identity is verified through an out-of-band process (e.g., phone call to a verified number, in-person verification).
3. The identity provider administrator temporarily disables MFA for the account.
4. The administrator logs in and immediately enrolls a new MFA device.
5. The temporary MFA bypass is removed.
6. The recovery event is recorded in the audit log.

## 8.3 Account Lockout and Brute-Force Protection

CTP implements layered protection against brute-force authentication attacks:

- Account Lockout — After a configured number of consecutive failed authentication attempts, the account is temporarily locked. The lockout counter resets after a configured period of no failed attempts.
- Rate Limiting — The authentication endpoint is rate-limited to prevent high-volume credential stuffing attacks.
- WAF Protection — Web Application Firewall rules provide an additional layer of protection against automated authentication attacks at the network level.
- Monitoring and Alerting — Failed authentication attempts are logged and, when thresholds are exceeded, generate alerts to administrative personnel.

## 8.4 System Use Notification (AC-8)

CTP displays a system use notification banner on the login page that all users must acknowledge before accessing the platform. The default banner text is:

> *You are accessing a U.S. Government information system, which includes this computer, this network, all computers connected to this network, and all devices and storage media attached to or connected to this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of or access to this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications or data transiting,*

*stored on, or traveling to or from this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose. Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding the use of this system, whether oral or written, by your supervisor or any other official. Your consent to monitoring includes the proactive searching of your activities, contents, and metadata.*

**Configuration:** The banner text can be customized by CTP platform administrators to meet agency-specific requirements. Changes to the banner text are recorded in the audit log.

**Verification:** Navigate to the CTP login page and confirm the system use notification is displayed. Verify the banner text matches the approved version in Platform Settings > System Use Notification.

**Default State:** Enabled. The system use notification cannot be disabled.

# 9. Role-Based Access Control (RBAC)

## 9.1 RBAC Architecture

CTP implements a hierarchical role-based access control system that governs access to all platform functionality. The RBAC system is designed around the following principles:

- Least Privilege — Users are granted only the permissions necessary to perform their assigned duties.
- Separation of Duties — Administrative functions are divided into distinct roles (security, finance, technical, project) to prevent any single user from having unrestricted access.
- Hierarchical Inheritance — Higher-level roles inherit the permissions of lower-level roles within their scope.
- Scope-Based Isolation — Permissions are enforced within organizational and account boundaries, preventing cross-tenant access.

## 9.2 Permission Structure

CTP organizes permissions into a hierarchical structure aligned with the administrative account types described in Section 6.1. At the highest level, platform-wide permissions govern CTP system administration. Below that, organization-level permissions control tenant management. At the functional level, permissions are divided into security, finance, technical, and project domains. All users have a base permission set that includes read-only dashboard access and the ability to submit change requests.

The permission hierarchy ensures that each role level can only access and modify resources within its designated scope. Cross-tenant access is architecturally prevented through scope-based data isolation.

Detailed permission definitions and the complete permission mapping are available in the Restricted version of this guide for authorized administrators.

## 9.3 Role Assignment Best Practices

| Principle | Guidance |
|---|---|
| **Assign the most specific role possible** | If a user only needs to manage billing, assign the Finance Admin role rather than Organization Admin. |
| **Avoid shared accounts** | Each user must have an individual account. Shared accounts undermine accountability and audit integrity. |
| **Review assignments regularly** | Conduct quarterly access reviews to identify and remove unnecessary role assignments. |
| **Document justification** | Maintain records of why each user was assigned their role(s) to support audit activities. |
| **Use just-in-time elevation** | When temporary elevated access is needed, use the JIT access model (Section 6.5.2) with automatic expiration. |

## 9.4 Permission Enforcement

Permissions are enforced at multiple layers within CTP:

- Route-Level Enforcement — Each application route verifies the user's role before allowing access.
- Data-Level Enforcement — Database queries are scoped to the user's organizational and account context, preventing access to data outside their authorized scope.
- UI-Level Enforcement — Interface elements are conditionally rendered based on the user's permissions.
- API-Level Enforcement — All API endpoints validate the requesting user's permissions before processing.

# 10. Network Security Configuration

## 10.1 Transport Layer Security (TLS)

All communication with the CTP platform is encrypted using FIPS validated TLS implementations:

- Minimum TLS Version: 1.2
- Preferred TLS Version: 1.3
- Certificate Authority: Certificates are issued by trusted certificate authorities with automated renewal before expiration.
- HSTS: HTTP Strict Transport Security is enabled with a long-duration max-age and includeSubDomains directive.
- All cipher suites use FIPS-approved algorithms. Legacy cipher suites (CBC mode, RC4, 3DES) are disabled.

**Verification:** Use external TLS testing services to verify the TLS configuration of CTP endpoints. Verify that only TLS 1.2 and 1.3 are accepted and that all cipher suites are FIPS-approved.

## 10.2 FIPS 140 Cryptographic Validation

All cryptographic operations within the CTP platform use FIPS validated cryptographic modules. This includes:

- TLS termination and encryption in transit — The TLS libraries used for all HTTPS communications are FIPS validated.
- Encryption at rest — Database encryption and object storage encryption use validated modules provided by the hosting platform's key management service.
- Key management — Cryptographic key generation, storage, and rotation are performed by validated key management services.
- Hashing and digital signatures — All cryptographic hashing (e.g., for integrity verification, password storage) uses FIPS-approved algorithms within validated modules.
- Random number generation — Cryptographic random number generation uses FIPS-approved deterministic random bit generators (DRBGs) within validated modules.

CTP operates in a FIPS-compliant mode at all times. Non-FIPS cryptographic algorithms and modules are not available for use within the platform. Specific FIPS 140 certificate references for each component are available in the Restricted version of this guide and upon request from CTP support.

**Verification:** Contact CTP support to request the current list of FIPS certificate numbers for all cryptographic modules in use. Verify TLS cipher suites using external testing tools.

## 10.3 IP Access Restrictions

CTP supports IP-based access restrictions at multiple levels:

- Load Balancer / WAF Level — IP allowlists restrict which addresses can reach the CTP application.
- Network Security Group Level — Network-level rules restrict which addresses can communicate with the application infrastructure.
- Database Level — Database security groups restrict access to the application tier only — no direct database access from the internet.

**Security Recommendation:** IP whitelisting should be as restrictive as possible. In environments where users connect from known, static IP addresses (e.g., organizational VPN exit points), the allowlist should include only those addresses. For environments with dynamic IP addresses, consider using a VPN or zero-trust network access (ZTNA) solution as an intermediary.

**Verification:** Navigate to Security > Network Access to view current IP allowlist configuration. Verify database isolation through Account Settings > Infrastructure.

## 10.4 Security Group Management

- Default Deny — Newly created security groups have no inbound rules (deny all) and restricted outbound rules.
- Rule Documentation — Each security group rule should include a description explaining its purpose.
- Change Tracking — All security group modifications are recorded in the audit log and may require change request approval.
- Periodic Review — Security group rules should be reviewed quarterly to identify and remove unnecessary rules.

## 10.5 Egress Filtering

- Domain-Based Filtering — Outbound traffic can be restricted to a configurable allowlist of domains.
- Protocol-Based Filtering — Outbound traffic can be restricted by protocol (e.g., HTTPS only).
- Default Policy — The recommended default egress policy is to deny all outbound traffic except to explicitly allowlisted destinations.

## 10.6 DNSSEC Configuration

CTP supports DNS Security Extensions (DNSSEC) for DNS zones managed through the platform:

- DNSSEC Signing — DNS zones managed by CTP can be configured with DNSSEC signing to provide authentication and integrity for DNS responses. DNSSEC signing uses FIPS-approved algorithms
- Key Management — DNSSEC key signing keys (KSK) and zone signing keys (ZSK) are managed by the platform's key management service. Key rotation occurs automatically per industry best practices (KSK rotation annually, ZSK rotation quarterly).
- DS Record Delegation — When DNSSEC is enabled, CTP provides the Delegation Signer (DS) records that must be registered with the parent zone's registrar to complete the chain of trust.
- DNSSEC Validation — CTP's DNS resolvers perform DNSSEC validation on recursive queries, ensuring that responses from external DNS zones are authenticated when DNSSEC is available.

**Security Recommendation:** Enable DNSSEC signing for all DNS zones managed through CTP. Verify that DS records are properly registered with the parent zone registrar after enabling DNSSEC.

**Verification:** Navigate to DNS Management > [Zone] > DNSSEC to view signing status. Use external DNSSEC validation tools to verify the complete chain of trust.

# 11. Data Protection and Encryption

## 11.1 Encryption at Rest

All data stored by the CTP platform is encrypted at rest using FIPS validated cryptographic modules:

| Data Store | Encryption Method | Key Management |
|---|---|---|
| **Primary Database** | Transparent Data Encryption (TDE) with AES- using FIPS validated modules | Encryption keys managed by the hosting platform's key management service with configurable rotation |
| **Object Storage** | Server-Side Encryption with FIPS validated key management | Keys managed by the key management service with configurable rotation |
| **Container File System** | Ephemeral (no persistent local storage) | N/A — containers use ephemeral storage destroyed when the container stops |
| **Backup Snapshots** | Encrypted using the same key as the source database, FIPS validated | Key rotation does not affect existing snapshots |

**Verification:** Navigate to Account Settings > Encryption to confirm encryption-at-rest status. Database encryption status is also visible in the compliance dashboard.

## 11.2 Encryption in Transit

All data transmitted to, from, and within the CTP platform is encrypted in transit using FIPS validated TLS implementations:

| Communication Path | Encryption | Protocol |
|---|---|---|
| Client ↔ Load Balancer | TLS 1.2/1.3 (FIPS validated) | HTTPS |
| Load Balancer ↔ Application | TLS 1.2/1.3 or internal network encryption | HTTPS or internal |
| Application ↔ Database | TLS 1.2/1.3 (FIPS validated) | Encrypted database connection |
| Application ↔ Identity Provider | TLS 1.2/1.3 (FIPS validated) | HTTPS (OIDC API calls) |
| Application ↔ Cloud APIs | TLS 1.2/1.3 (FIPS validated) | HTTPS (SDK calls) |

## 11.3 Sensitive Data Handling

| Classification | Examples | Handling Requirements |
|---|---|---|
| **Confidential** | Authentication credentials, encryption keys, API secrets | Stored in secrets management systems; never logged or displayed in UI; masked in audit records |
| **Sensitive** | PII, billing information, account details | Encrypted at rest and in transit; access restricted by RBAC; logged with appropriate detail |
| **Internal** | Infrastructure configuration, change request details, audit logs | Protected by access controls; available to authorized administrative users |
| **Public** | System documentation, general platform information | No special handling required beyond integrity protection |

## 11.4 Secrets Management

- Environment Variables — Application secrets are injected as environment variables at container startup, not stored in application code or configuration files.
- Secrets Volumes — Complex secrets (e.g., TLS certificates, signing keys) use dedicated secrets volumes mounted at runtime.
- No Hardcoded Secrets — Application code does not contain hardcoded credentials. All secrets are externalized.
- Secret Rotation — Secrets should be rotated at least annually, or immediately upon suspected compromise.

# 12. Logging, Auditing, and Monitoring

## 12.1 Audit Log Architecture

CTP maintains a comprehensive audit log that records all security-relevant events, supporting compliance requirements, incident investigation, and continuous monitoring.

### 12.1.1 Audit Log Fields

Each audit log entry contains: UTC timestamp with millisecond precision, unique user identifier, display name, user role, specific action performed, resource type and ID, structured before/after state details for configuration changes, source IP address, client information, outcome (success/failure), and error message for failed actions.

### 12.1.2 Audited Events

- Authentication Events — Login success/failure, MFA challenges, session lifecycle, banner acknowledgment
- Authorization Events — Permission checks, access denials, role escalation attempts, JIT access lifecycle
- User Management Events — User creation, modification, role assignment, deactivation, invitation
- Organization Management Events — Organization creation, configuration changes, account provisioning/decommissioning
- Infrastructure Events — Resource creation, modification, deletion (VPCs, subnets, security groups, instances, load balancers, DNS records)
- Security Events — WAF rule changes, security group modifications, compliance scans, threat detection findings
- Change Management Events — Change request submission, approval, denial, execution, cancellation
- System Events — Configuration changes, system health events, scheduled task execution, emergency access activation

## 12.2 Log Protection

- Write-Once Storage — Audit log entries, once written, cannot be modified or deleted through the application interface.
- Access Control — Audit log viewing is restricted to users with appropriate administrative roles. Organization-scoped logs are only visible to administrators within that organization.
- Integrity Verification — Log entries include integrity verification mechanisms to detect tampering.
- Retention — Audit logs are retained for a minimum of one year (or longer as required by organizational policy or regulatory requirements).

## 12.3 Log Forwarding and Integration

- Cloud-native log aggregation services for centralized monitoring in cloud-hosted environments.
- Syslog/SIEM Integration — Logs can be exported for ingestion by enterprise SIEM platforms.
- Structured Format — Logs are generated in structured formats (JSON) to facilitate automated parsing and analysis.

## 12.4 Monitoring and Alerting

| Monitoring Area | Mechanism | Alert Conditions |
|---|---|---|
| **Application Health** | Automated health check monitoring | Service unavailability, degraded performance |
| **Authentication Anomalies** | Audit log analysis | Excessive failed logins, login from unusual locations, concurrent sessions |

| | | |
|---|---|---|
| **Configuration Changes** | Audit log events | Unauthorized or unexpected security configuration changes |
| **Resource Utilization** | Infrastructure monitoring metrics | Resource threshold exceeded, scaling events |
| **Security Findings** | Threat detection, WAF, compliance scans | New findings, severity escalation, unresolved findings aging |
| **Cost Anomalies** | Billing monitoring | Unexpected cost increases, budget threshold exceeded |

# 13. Session Management

## 13.1 Session Lifecycle

1. Creation — A session is created upon successful authentication (including MFA verification). A unique session identifier is generated using a cryptographically secure random number generator within a FIPS validated module.
2. Validation — The session is validated on each request by verifying the session identifier, checking expiration status, and confirming account activity.
3. Renewal — The session's idle timeout counter is reset on each valid request, extending the session for active users.
4. Expiration — Sessions expire after the configured idle timeout or after the maximum session duration, whichever comes first.
5. Termination — Sessions can be explicitly terminated by the user (logout) or by an administrator (forced logout). Terminated session identifiers are invalidated and cannot be reused.

## 13.2 Session Security Controls

- Cryptographically Secure Session IDs — Session identifiers are generated with sufficient entropy using FIPS-validated random number generators to prevent prediction and brute-force attacks.
- Session Fixation Prevention — Session IDs are regenerated after successful authentication to prevent attackers from fixing a known session ID.
- Secure Cookie Configuration — Session cookies are protected with industry-standard security attributes to prevent hijacking through cookie theft.
- Server-Side Session Storage — Sessions are stored server-side, preventing session data tampering by the client.
- Concurrent Session Control — Single active session per user by default, preventing credential sharing and limiting the impact of compromised credentials.

## 13.3 Session Timeout Recommendations

| User Type | Idle Timeout | Maximum Duration | Rationale |
|---|---|---|---|
| **CTP Super Admin / CTP Admin** | Shortest tier | Shortest tier | Highest-privilege accounts require shorter timeouts to limit exposure |
| **Organization Admin** | Standard tier | Standard tier | Standard administrative timeout |
| **Functional Admins** | Standard tier | Standard tier | Standard administrative timeout |
| **Standard Users (Viewer)** | Extended tier | Standard tier | Lower-privilege accounts can have longer idle timeouts for usability |

Specific timeout values are configured at the platform level. Administrators can view current values in Platform Settings > Session Configuration. All timeout values comply with NIST AC-11 and AC-12 requirements.

# 14. Change Management and Approval Workflows

## 14.1 Change Management Overview

CTP implements a formal change management process for all infrastructure modifications, ensuring all changes are authorized, documented, auditable, and reversible where possible.

## 14.2 Change Request Workflow

1. Submission — A user submits a change request through the CTP interface, specifying the resources to be modified and the requested changes.
2. Review — The change request is reviewed by one or more authorized approvers. Reviewers can add comments, request modifications, or escalate.
3. Approval / Denial — Approved changes are queued for execution. Denied changes include a reason for denial.
4. Execution — Approved changes are executed through the CTP platform's infrastructure provisioning layer.
5. Verification — After execution, the change is verified to confirm correct application with no unintended side effects.
6. Closure — The change request is closed with a final status and verification notes.

## 14.3 Change Request Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Approval Required** | Yes (all changes) | Ensures all infrastructure modifications are reviewed and authorized. |
| **Self-Approval** | Disabled | Prevents users from approving their own changes, enforcing separation of duties. |
| **Minimum Approvers** | 1 or more (configurable) | Higher values provide stronger governance but may slow operations. |
| **Emergency Change Process** | Available with mandatory post-hoc review | Enables critical changes outside the standard process, with mandatory retroactive review within 24 hours. |
| **Change Window** | Configurable per organization | Organizations can define maintenance windows during which changes are permitted. |

**Verification:** Navigate to Organization Settings > Change Management to view current approval workflow configuration. Verify that self-approval is disabled.

# 15. Web Application Firewall (WAF) Configuration

## 15.1 WAF Architecture

- Platform WAF — Protects the CTP application itself. Managed by CTP platform administrators.
- Customer WAF — Enables customer organizations to configure WAF protections for their cloud resources. Managed by Security Administrators.

## 15.2 Managed Rule Groups

| Rule Group | Purpose | Recommendation |
|---|---|---|
| **Core Rule Set (CRS)** | Protection against common web vulnerabilities including OWASP Top 10 | Enabled (required) |
| **Known Bad Inputs** | Protection against known exploit patterns | Enabled (required) |
| **SQL Injection** | Protection against SQL injection attacks | Enabled (required) |
| **Cross-Site Scripting (XSS)** | Protection against XSS attacks | Enabled (required) |
| **OS-Specific Rules** | Protection against OS-specific exploits | Enabled (if applicable) |
| **IP Reputation** | Blocks requests from known malicious IPs | Enabled (recommended) |
| **Anonymous IP** | Blocks requests from known VPN, proxy, and Tor exit nodes | Configurable per organizational policy |
| **Bot Control** | Detection and mitigation of automated bot traffic | Enabled (recommended) |

## 15.3 Custom WAF Rules

Security Administrators can create custom WAF rules for organization-specific requirements: IP/geo-based filtering, endpoint rate-limiting, header/parameter filtering, and managed rule overrides for verified false positives.

**Security Recommendation:** Custom rule overrides should be used sparingly and only for verified false positives. Each override must be documented with a justification and reviewed at least quarterly.

## 15.4 WAF Logging and Monitoring

All WAF actions (allow, block, count) are logged and available to Security Administrators, including request metadata, matched rules, actions taken, and aggregate metrics for trend analysis.

**Verification:** Navigate to Security > WAF > Dashboard to view enabled rules, recent activity, and any active overrides.

# 16. Vulnerability and Compliance Scanning

## 16.1 Scanning Capabilities

| Scan Type | Description | Frequency |
|---|---|---|
| **Vulnerability Scanning** | Identifies known vulnerabilities based on CVE databases | On-demand and scheduled (recommended: weekly) |
| **STIG Compliance Checking** | Verifies configurations against applicable STIGs | On-demand and scheduled (recommended: monthly) |
| **Configuration Assessment** | Evaluates configurations against CIS Benchmarks and organizational baselines | On-demand and scheduled (recommended: weekly) |

## 16.2 Scan Policy Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Scan Scope** | Include all managed resources | Comprehensive coverage ensures no resources are excluded from security assessment. |
| **Scan Frequency** | Weekly (vulnerability), Monthly (STIG) | Regular scanning enables timely detection of new vulnerabilities and configuration drift. |
| **Severity Threshold** | Notify on all findings | All severity levels should be tracked; Critical and High require expedited remediation. |
| **Auto-Remediation** | Disabled by default | Enable only for well-understood, low-risk remediations to prevent unintended changes. |
| **Report Distribution** | Security Admin, Organization Admin | Ensures appropriate personnel are informed of findings. |

## 16.3 Finding Management

1. Detection — Finding identified, recorded with severity, affected resource, and remediation guidance.
2. Triage — Security Administrator reviews validity and assesses contextual risk.
3. Remediation Planning — Remediation plan developed, may include a change request.
4. Remediation — Implemented through the change management process.
5. Verification — Follow-up scan verifies the finding has been resolved.
6. Closure — Finding closed with remediation documentation.

**Remediation Timelines:** Critical findings: 30 days. High: 90 days. Medium: 180 days. Low: per organizational policy.

# 17. Backup, Recovery, and Disaster Recovery

## 17.1 Backup Configuration

| Setting | Recommended Value | Security Implication |
|---|---|---|
| **Backup Frequency** | Daily (minimum) | More frequent backups reduce potential data loss. |
| **Backup Retention** | 30 days (minimum) | Longer retention enables recovery from incidents not immediately detected. |
| **Backup Encryption** | Enabled (AES-256, FIPS validated) | Ensures backup data is protected at rest. |
| **Cross-Region Backup** | Enabled (where regulatory requirements permit) | Protects against region-level failures. |
| **Backup Verification** | Monthly test restore | Regular verification ensures backups are usable when needed. |

**Verification:** Navigate to Account Settings > Backup Configuration to view current settings. Review backup job history and last successful verification date.

## 17.2 Recovery Procedures

| Scenario | RTO | RPO | Procedure |
|---|---|---|---|
| **Application Failure** | < 5 minutes | Zero | Automatic container restart and health check recovery |
| **Database Failure** | < 1 hour | < 5 minutes | Failover to database replica or restore from point-in-time backup |
| **Region Failure** | < 4 hours | < 1 hour | Deploy to alternate region from cross-region backups |
| **Data Corruption** | < 2 hours | Detection-dependent | Restore from backup snapshot predating the corruption event |

## 17.3 Disaster Recovery Configuration

- Multi-AZ Deployment — Resources distributed across multiple availability zones for high availability.
- Cross-Region Replication — Critical data replicated to a secondary region for disaster recovery.
- Infrastructure as Code — All infrastructure defined as code, enabling rapid environment recreation.
- Recovery Testing — Disaster recovery procedures tested at least annually.

# 18. Secure Defaults

In accordance with FedRAMP requirement SCG-CSO-SDF, CTP is configured with recommended secure defaults upon initial provisioning. The following table summarizes the complete default security configuration with verification methods for each setting.

| Category | Setting | Default Value | Secure? | Verification Method |
|---|---|---|---|---|
| Authentication | **MFA Required** | Yes | Yes | Platform Settings > Authentication |
| Authentication | **Account Lockout** | Configured per policy | Yes | Identity Provider > Lockout Settings |
| Authentication | **System Use Notification** | Enabled | Yes | Login page visual inspection |
| Authentication | **CAC/PIV Support** | Available (via IdP) | Yes | IdP configuration documentation |
| Sessions | **Idle Timeout** | Per role tier | Yes | Platform Settings > Session Configuration |
| Sessions | **Secure Cookie Attributes** | All enabled | Yes | Browser developer tools > Cookies |
| Sessions | **Concurrent Sessions** | 1 per user | Yes | Platform Settings > Session Configuration |
| Network | **TLS Minimum Version** | 1.2 | Yes | External TLS testing tools |
| Network | **FIPS 140 Mode** | Enabled | Yes | CTP support / compliance documentation |
| Network | **HSTS** | Enabled | Yes | Browser developer tools > Response Headers |
| Network | **HTTP to HTTPS Redirect** | Enabled | Yes | Navigate to HTTP URL, confirm redirect |
| Network | **Default Inbound Rule** | Deny All | Yes | Create new security group, inspect rules |
| Network | **Default Outbound Rule** | Deny All | Yes | Create new security group, inspect rules |
| Network | **DNSSEC Support** | Available | Yes | DNS Management > DNSSEC |
| Headers | **Content-Security-Policy** | Restrictive | Yes | Browser developer tools > Response Headers |
| Headers | **X-Frame-Options** | DENY | Yes | Browser developer tools > Response Headers |
| Headers | **X-Content-Type-Options** | nosniff | Yes | Browser developer tools > Response Headers |
| Headers | **Referrer-Policy** | Restrictive | Yes | Browser developer tools > Response Headers |
| Data | **Encryption at Rest** | Enabled FIPS validated | Yes | Account Settings > Encryption |
| Data | **Encryption in Transit** | Enabled FIPS validated | Yes | External TLS testing tools |

| | | | | |
|---|---|---|---|---|
| Logging | **Audit Logging** | Enabled | Yes | Audit Logs > verify recent entries exist |
| Logging | **Auth Event Logging** | Enabled | Yes | Audit Logs > filter by Authentication events |
| Change Mgmt | **Approval Required** | Yes | Yes | Org Settings > Change Management |
| Change Mgmt | **Self-Approval** | Disabled | Yes | Org Settings > Change Management |
| WAF | **Core Rule Set** | Enabled | Yes | Security > WAF Configuration |
| WAF | **SQL Injection Protection** | Enabled | Yes | Security > WAF Configuration |
| WAF | **XSS Protection** | Enabled | Yes | Security > WAF Configuration |
| Scanning | **Vulnerability Scanning** | Enabled (weekly) | Yes | Security > Scan Policies |
| Invitations | **Expiration Period** | 72 hours | Yes | Org Settings > User Management |
| Backup | **Frequency** | Daily | Yes | Account Settings > Backup Configuration |
| Backup | **Retention** | 30 days | Yes | Account Settings > Backup Configuration |
| Backup | **Encryption** | Enabled (FIPS validated) | Yes | Account Settings > Backup Configuration |

**Note:** All default settings are configured to recommended secure values. Administrators who wish to deviate from these defaults must follow the deviation request process documented in Appendix E.

# 19. Decommissioning and Account Removal

## 19.1 User Account Decommissioning

1. Remove all role assignments from the user account in CTP.
2. Deactivate the user's account in the identity provider, preventing authentication.
3. Terminate any active sessions immediately.
4. Transfer ownership of any resources or pending change requests to another authorized user.
5. Verify the decommissioning event is recorded in the audit log.
6. Confirm that the decommissioned user cannot access any CTP functionality.

## 19.2 Organization Decommissioning

1. Provide the customer with an export of their organizational data in a standard format.
2. Compile a complete inventory of all cloud resources associated with the organization.
3. Decommission all cloud resources per customer instructions.
4. Close all sub-accounts associated with the organization.
5. Deactivate all user accounts following the process in Section 19.1.
6. Retain audit logs and configuration records per the required retention period (minimum one year).
7. After the retention period, securely delete all remaining organizational data.
8. Provide written confirmation of decommissioning and data deletion to the customer.

## 19.3 Cloud Account Decommissioning

When decommissioning a cloud account managed through CTP: terminate all running resources, delete all stored data, remove all security configurations and IAM policies, remove DNS records, verify no recurring charges remain, submit account closure, and record the complete decommissioning in the audit log.

# Appendix A — Security Configuration Checklist

This checklist provides a structured format for verifying the security configuration of a CTP deployment.

## A.1 Authentication and Access Control

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **A-1** | MFA is required for all users | Enabled | | |
| **A-2** | Password policy meets minimum requirements (14 char, complexity, history) | Configured | | |
| **A-3** | Account lockout is configured | Configured | | |
| **A-4** | Concurrent session limit is set to 1 | Configured | | |
| **A-5** | Session idle timeout is configured per role tier | Configured | | |
| **A-6** | Session cookies have industry-standard security attributes | Enabled | | |
| **A-7** | CTP Super Admin accounts are limited to minimum required | Verified | | |
| **A-8** | All users have individual accounts (no shared accounts) | Verified | | |
| **A-9** | Role assignments follow least privilege | Verified | | |
| **A-10** | Dormant accounts (>90 days inactive) have been reviewed | Completed | | |
| **A-11** | System use notification banner is enabled and displays approved text | Enabled | | |
| **A-12** | CAC/PIV support is configured (if applicable) | Configured | | |
| **A-13** | Emergency access (break-glass) credentials are sealed and tested | Verified | | |
| **A-14** | JIT access model is documented and operational | Verified | | |
| **A-15** | Privileged access workstation requirements are documented | Verified | | |

## A.2 Network Security

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **B-1** | TLS 1.2 is the minimum supported version | Configured | | |
| **B-2** | All cryptographic modules are validated | Verified | | |
| **B-3** | HSTS is enabled with appropriate max-age | Enabled | | |
| **B-4** | HTTP to HTTPS redirect is enabled | Enabled | | |
| **B-5** | IP access restrictions are configured | Configured | | |

| | | | | |
|---|---|---|---|---|
| **B-6** | Default security groups deny all inbound traffic | Configured | | |
| **B-7** | Database is not publicly accessible | Verified | | |
| **B-8** | WAF Core Rule Set is enabled | Enabled | | |
| **B-9** | WAF SQL Injection and XSS rules are enabled | Enabled | | |
| **B-10** | DNSSEC is enabled for managed DNS zones (if applicable) | Configured | | |

## A.3 Data Protection

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **C-1** | Database encryption at rest is enabled (FIPS validated) | Enabled | | |
| **C-2** | Database connections use TLS (FIPS validated) | Enabled | | |
| **C-3** | Application secrets are externalized (not in code) | Verified | | |
| **C-4** | Backup encryption is enabled (FIPS validated) | Enabled | | |
| **C-5** | Backup retention meets minimum requirements (30 days) | Configured | | |

## A.4 Logging and Monitoring

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **D-1** | Audit logging is enabled for all event categories | Enabled | | |
| **D-2** | Audit logs are protected from modification | Verified | | |
| **D-3** | Log retention meets minimum requirements (1 year) | Configured | | |
| **D-4** | Security alert notifications are configured | Configured | | |
| **D-5** | Failed login notifications are enabled | Enabled | | |
| **D-6** | Log forwarding to SIEM is configured (if applicable) | Configured | | |

## A.5 Change Management

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **E-1** | Change request approval is required for all changes | Enabled | | |
| **E-2** | Self-approval is disabled | Disabled | | |
| **E-3** | Emergency change process is documented and approved | Documented | | |

## A.6 Vulnerability Management

| # | Check | Expected State | Verified | Notes |
|---|---|---|---|---|
| **F-1** | Vulnerability scanning is enabled and scheduled | Configured | | |
| **F-2** | STIG compliance checking is enabled | Configured | | |
| **F-3** | Critical/High findings are tracked with remediation timelines | Verified | | |

# Appendix B — NIST SP 800-53 Rev5 Control Mapping

| Control | Control Name | CTP Implementation | SCG Section |
|---|---|---|---|
| **AC-2** | Account Management | Administrative account lifecycle, role assignment, periodic review, JIT access, break-glass procedures | 6 |
| **AC-3** | Access Enforcement | RBAC permission enforcement at route, data, UI, and API levels | 9 |
| **AC-5** | Separation of Duties | Distinct administrative roles (Security, Finance, Technical, Project) | 9.1 |
| **AC-6** | Least Privilege | Hierarchical role structure, scope-based access, JIT privileged access | 9.1, 9.3, 6.5.2 |
| **AC-7** | Unsuccessful Logon Attempts | Account lockout, rate limiting, WAF protection | 8.3 |
| **AC-8** | System Use Notification | Login page banner with acknowledgment requirement | 8.4 |
| **AC-11** | Session Lock | Automatic session timeout per role tier | 13 |
| **AC-12** | Session Termination | Explicit logout, forced termination, session expiration | 13.1 |
| **AC-17** | Remote Access | HTTPS-only, MFA required, IP restrictions, PAW requirements | 6.3, 10 |
| **AU-2** | Event Logging | Comprehensive audit logging of all security-relevant events | 12 |
| **AU-3** | Content of Audit Records | Structured audit records with user, action, resource, timestamp, outcome | 12.1.1 |
| **AU-6** | Audit Record Review | Administrative review capabilities, SIEM integration | 12.3, 12.4 |
| **AU-9** | Protection of Audit Information | Write-once audit storage, access-controlled viewing | 12.2 |
| **AU-11** | Audit Record Retention | Minimum one-year retention | 12.2 |
| **CA-7** | Continuous Monitoring | Security scanning, configuration monitoring, alerting | 16, 12.4 |
| **CM-6** | Configuration Settings | Secure defaults, configuration guidance, baseline documentation, deviation tracking | 7, 18, App E |
| **CM-7** | Least Functionality | Restrictive Permissions-Policy, disabled unnecessary features | 7.1.5 |
| **CP-9** | System Backup | Backup configuration, FIPS-validated encryption, cross-region replication | 17.1 |
| **CP-10** | System Recovery | Documented recovery procedures with RTO/RPO targets | 17.2 |
| **IA-2** | Identification and Authentication | OIDC authentication with MFA, CAC/PIV support | 8 |
| **IA-5** | Authenticator Management | Password policy, MFA enrollment, secret management, credential storage guidance | 8.2, 7.1.2, 11.4, 6.3.3 |

| | | | |
|---|---|---|---|
| **IA-8** | Non-Org User Authentication | OIDC federation support, CAC/PIV via IdP | 8.1, 8.2.3 |
| **IR-4** | Incident Handling | Audit logs, monitoring alerts, emergency access procedures | 12, 6.6 |
| **RA-5** | Vulnerability Scanning | Integrated vulnerability and STIG compliance scanning | 16 |
| **SC-8** | Transmission Confidentiality | FIPS-validated TLS 1.2+ for all communications | 10.1, 11.2 |
| **SC-12** | Key Management | FIPS-validated key management, secret rotation | 10.2, 11.1, 11.4 |
| **SC-13** | Cryptographic Protection | FIPS validated AES at rest, TLS in transit | 10.2, 11 |
| **SC-20** | Secure Name Resolution | DNSSEC signing and validation for managed DNS zones | 10.6 |
| **SC-23** | Session Authenticity | Secure session management, CSRF protection, session regeneration | 13 |
| **SC-28** | Protection at Rest | Database TDE, encrypted object storage, encrypted backups (all FIPS validated) | 11.1 |
| **SI-2** | Flaw Remediation | Vulnerability management lifecycle, remediation timelines | 16.3 |
| **SI-4** | System Monitoring | Application health checks, WAF logging, anomaly detection | 12.4, 15.4 |
| **SI-10** | Information Input Validation | Parameterized queries, server-side validation, output encoding | 7.1.5 |

# Appendix C — Glossary of Terms

| Term | Definition |
|---|---|
| **AEAD** | Authenticated Encryption with Associated Data |
| **AZ** | Availability Zone — an isolated data center within a cloud region |
| **CAC** | Common Access Card — a DoD smart card for identification and authentication |
| **CIS** | Center for Internet Security |
| **CSRF** | Cross-Site Request Forgery |
| **CTP** | Cloud Testing Platform — the subject of this guide |
| **CVE** | Common Vulnerabilities and Exposures |
| **DNSSEC** | DNS Security Extensions — provides authentication and integrity for DNS |
| **DRBG** | Deterministic Random Bit Generator — FIPS-approved random number generator |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FIPS** | Federal Information Processing Standards |
| **HSTS** | HTTP Strict Transport Security |
| **IdP** | Identity Provider |
| **ISSO** | Information System Security Officer |
| **JIT** | Just-in-Time — a privileged access model where elevation is temporary |
| **KMS** | Key Management Service |
| **MFA** | Multi-Factor Authentication |
| **NIST** | National Institute of Standards and Technology |
| **OIDC** | OpenID Connect — identity layer on OAuth 2.0 |
| **OWASP** | Open Web Application Security Project |
| **PAW** | Privileged Access Workstation — a hardened device for administrative tasks |
| **PII** | Personally Identifiable Information |
| **PIV** | Personal Identity Verification — a federal smart card standard |
| **PKI** | Public Key Infrastructure |
| **RBAC** | Role-Based Access Control |
| **RPO** | Recovery Point Objective |
| **RTO** | Recovery Time Objective |
| **SaaS** | Software as a Service |
| **SCG** | Secure Configuration Guide |
| **SIEM** | Security Information and Event Management |
| **STIG** | Security Technical Implementation Guide |
| **TDE** | Transparent Data Encryption |

| | |
|---|---|
| **TLS** | Transport Layer Security |
| **TOTP** | Time-Based One-Time Password |
| **VPC** | Virtual Private Cloud |
| **WAF** | Web Application Firewall |
| **WebAuthn** | Web Authentication — W3C standard for passwordless authentication |
| **XSS** | Cross-Site Scripting |
| **ZTNA** | Zero Trust Network Access |

# Appendix D — Version History and Change Log

## Version 1.0 — February 26, 2026

**Initial Release (Internal)**

Initial release establishing baseline security configuration recommendations. Now superseded by Version 2.0 Public Release.

# Appendix E — Secure Default Deviation Request Template

When an administrator determines that a deviation from a recommended secure default is necessary, the following template must be completed and approved before the change is implemented.

| Field | Value |
|---|---|
| **Deviation Request ID** | [Auto-generated] |
| **Date Submitted** | |
| **Requestor Name and Role** | |
| **Setting to be Changed** | [Reference Section 18 setting name] |
| **Current (Default) Value** | |
| **Proposed New Value** | |
| **Justification** | [Describe the operational requirement that necessitates the deviation] |
| **Risk Assessment** | [Describe the security risks introduced by the deviation and any compensating controls] |
| **Compensating Controls** | [List any additional security measures that will be implemented to offset the increased risk] |
| **Duration** | [Is this deviation permanent or temporary? If temporary, specify the end date] |
| **Review Schedule** | [How often will this deviation be reviewed? Minimum: quarterly] |
| **Approver Name and Role** | [Must be Organization Admin or higher] |
| **Approval Date** | |
| **ISSO Acknowledgment** | [For High-severity deviations, ISSO must acknowledge the risk acceptance] |

## Deviation Approval Workflow

1. The requestor completes the deviation request template and submits it through the CTP change management system.
2. The request is reviewed by the Organization Admin (or CTP Admin for platform-level settings). The reviewer evaluates the justification, risk assessment, and proposed compensating controls.
3. For deviations affecting High-severity settings (as identified in Section 7), the ISSO must acknowledge the risk acceptance.
4. Upon approval, the setting change is implemented through the standard change management process.
5. Approved deviations are recorded in the CTP compliance dashboard and are included in quarterly access and configuration reviews.
6. At each review interval, the deviation is re-evaluated. If the operational need no longer exists, the setting must be returned to the recommended default.

# Appendix F — FedRAMP SCG Requirements Cross Reference

The following table maps each FedRAMP Secure Configuration Guide (SCG) requirement to the section(s) of this document that address it. This cross reference enables FedRAMP reviewers and security assessors to efficiently verify that all required content is present and complete.

| FedRAMP Requirement | Response Section Number |
|---|---|
| SCG-CSO-RSC: Instructions for securely accessing administrative accounts | Section 6.3 (Secure Access to Administrative Accounts) |
| SCG-CSO-RSC: Instructions for securely configuring administrative accounts | Section 6.4 (Configuring Administrative Accounts) |
| SCG-CSO-RSC: Instructions for securely operating administrative accounts | Section 6.5 (Operating Administrative Accounts) |
| SCG-CSO-RSC: Instructions for decommissioning administrative accounts | Section 6.7 (Decommissioning Administrative Accounts) |
| SCG-CSO-RSC: Emergency/break-glass access procedures | Section 6.6 (Emergency Access Procedures) |
| SCG-CSO-RSC: All security-related settings with recommended values | Section 7 (Security-Related Settings and Their Implications) |
| SCG-CSO-RSC: Security implications of each setting | Section 7, all subsections (7.1 through 7.3) |
| SCG-CSO-RSC: Authentication configuration | Section 8 (Authentication and Identity Management) |
| SCG-CSO-RSC: Multi-factor authentication | Section 8.2 (Multi-Factor Authentication) |
| SCG-CSO-RSC: CAC/PIV support | Section 8.2.3 (CAC/PIV Authentication) |
| SCG-CSO-RSC: Password policy | Section 7.1.2 (Password Policy) |
| SCG-CSO-RSC: System use notification (AC-8) | Section 8.4 (System Use Notification) |
| SCG-CSO-RSC: Role-based access control | Section 9 (Role-Based Access Control) |
| SCG-CSO-RSC: Just-in-time privileged access | Section 6.5.2 (Just-in-Time Privileged Access) |
| SCG-CSO-RSC: Privileged access workstation requirements | Section 6.3.2 (Privileged Access Workstation Requirements) |
| SCG-CSO-RSC: Credential storage guidance | Section 6.3.3 (Administrator Credential Storage) |
| SCG-CSO-RSC: Network security configuration | Section 10 (Network Security Configuration) |
| SCG-CSO-RSC: FIPS 140 cryptographic validation | Section 10.2 (FIPS 140 Cryptographic Validation) |
| SCG-CSO-RSC: DNSSEC configuration | Section 10.6 (DNSSEC Configuration) |
| SCG-CSO-RSC: Data protection and encryption | Section 11 (Data Protection and Encryption) |
| SCG-CSO-RSC: Logging, auditing, and monitoring | Section 12 (Logging, Auditing, and Monitoring) |
| SCG-CSO-RSC: Session management | Section 13 (Session Management) |
| SCG-CSO-RSC: Change management and approval workflows | Section 14 (Change Management and Approval Workflows) |
| SCG-CSO-RSC: WAF configuration | Section 15 (Web Application Firewall Configuration) |
| SCG-CSO-RSC: Vulnerability and compliance scanning | Section 16 (Vulnerability and Compliance Scanning) |

| | |
|---|---|
| SCG-CSO-RSC: Backup, recovery, and disaster recovery | Section 17 (Backup, Recovery, and Disaster Recovery) |
| SCG-CSO-AUP: How to obtain the SCG | Section 4.1 (Obtaining the Guide) |
| SCG-CSO-AUP: How to use the SCG | Section 4.4 (Using the Guide) |
| SCG-CSO-AUP: Document integrity verification | Section 4.2 (Document Integrity Verification) |
| SCG-CSO-AUP: Customer acknowledgment process | Section 4.3 (Customer Acknowledgment Process) |
| SCG-CSO-AUP: Document maintenance and update procedures | Section 4.5 (Document Maintenance) |
| SCG-CSO-PUB: SCG is publicly available | Section 4.1 (published at public URL); Title page (PUBLIC RELEASE classification) |
| SCG-CSO-PUB: Implementation-agnostic language for public release | All sections (technology-specific details in Restricted version only) |
| SCG-CSO-SDF: Secure defaults documented | Section 18 (Secure Defaults) |
| SCG-CSO-SDF: Verification methods for each default | Section 18, Verification Method column in defaults table |
| SCG-CSO-SDF: Deviation request and tracking process | Appendix E (Secure Default Deviation Request Template) |
| FedRAMP: NIST SP 800-53 Rev5 control mapping | Appendix B (NIST SP 800-53 Rev5 Control Mapping) |
| FedRAMP: Security configuration checklist for assessors | Appendix A (Security Configuration Checklist) |
| FedRAMP: Shared responsibility model | Section 5.4 (Shared Responsibility Model) |
| FedRAMP: Intended audience identification | Section 3 (Intended Audience) |
| FedRAMP: Document revision history | Document Revision History (page 2); Appendix D (Version History) |
| FedRAMP: Decommissioning procedures | Section 19 (Decommissioning and Account Removal) |
| FedRAMP: Glossary of terms | Appendix C (Glossary of Terms) |

## END OF DOCUMENT