MANIFEST

Security Admin Guide

The Manifest Platform

FedRAMP Compliance Documentation

Version	1.0
Date	January 2026
Classification	Public
Status	Final

Contents

1 Introduction

1.1 Purpose

This Security Admin Guide provides comprehensive documentation for securely setting up, configuring, operating, and decommissioning top-level administrative application accounts within The Manifest Platform. It serves as the authoritative reference for all admin-controlled application security settings along with their security implications.

This guide satisfies the FedRAMP Recommended Secure Configuration (RSC) requirements FRR-RSC-01, FRR-RSC-02, and FRR-RSC-09 as specified in the FedRAMP Rev5 Balance documentation.

1.2 Scope

This guide covers the customer-facing administrative functions of The Manifest Platform. It does not extend to backend or internal administrative functionality required for Manifest Cyber to deploy or administer the application infrastructure.

1.3 Audience

This document is intended for:

- Organization Administrators responsible for managing The Manifest Platform
- Security teams implementing access controls and compliance requirements
- IT administrators setting up user accounts and integrations
- Compliance officers verifying security configurations

1.4 Document Conventions

Throughout this document:

- **Bold text** indicates user interface elements, menu items, or important terms
- `Monospace text` indicates technical values, API endpoints, or configuration settings
- Tables marked with **Recommended** provide security best practice values

> This guide references the Manifest ACL (Access Control List) system. Permission identifiers use the format `action:resource` (for example, `read:asset` or `create:product`). These identifiers are used throughout the platform for authorization checks.

> Administrative access to The Manifest Platform should be limited to authorized personnel only. Regularly audit user access and remove unnecessary privileges following the principle of least privilege.

2 Overview of the Manifest Platform

The Manifest Platform empowers security teams to manage software supply chain risk with confidence, clarity, and control. The platform provides comprehensive software bill of materials (SBOM) management, vulnerability tracking, and risk assessment capabilities.

2.1 Platform Modules

The Manifest Platform consists of three primary product modules:

1. **Manifest Product Security** - Continuous visibility into vulnerabilities, helping teams prioritize what matters most
2. **Manifest AI Risk** - AI model inventory and risk assessment capabilities
3. **Manifest Supplier Risk** - Third-party software supply chain risk management

2.2 Authentication Architecture

The Manifest Platform uses a session-based authentication system with the following characteristics:

- JSON Web Token (`JWT`) based session management
- Secure, signed session cookies for web client authentication
- Bearer token authentication for API access
- Organization-scoped access controls
- Role-based access control (`RBAC`) for permission management

2.3 Settings Navigation Reference

The Settings area of The Manifest Platform is organized into three sections. This reference helps administrators locate specific configuration options.

Section	Menu Item	Path	Purpose
Organization	API Tokens	`/settings/apiT`	Manage organization-wide API tokens
	Integrations	`/settings/inte`	Configure GitHub, Jira, ServiceNow, Linear
	Labels	`/settings/labe`	Create and manage asset labels
	Licenses	`/settings/lice`	View and configure license information
	Policies	`/settings/poli`	Configure security policies
	Sharing Portal	`/settings/shar`	Configure external SBOM sharing
	SBOM Upload Alerts	`/settings/sbom`	Configure alerts for SBOM uploads
	SLAs	`/settings/sla`	Define vulnerability remediation timelines
	Upload Settings	`/settings/uplo`	Configure SBOM enrichment settings
	Vulnerability Alerts	`/settings/vulr`	Configure vulnerability notification rules
Membership	Roles	`/settings/role`	View role definitions and permissions
	People	`/settings/peop`	Manage users and invitations
	Sub-Organizations	`/settings/subo`	Manage child organizations
Account	Profile	`/settings/prof`	Personal profile settings
	API Tokens	`/settings/acco`	Manage personal API tokens

> Some menu items may not be visible depending on your role permissions, feature flags enabled for your organization, and subscription level.

3 Top-Level Administrative Account Role Definitions

3.1 Role Hierarchy Overview

The Manifest Platform implements a role-based access control (RBAC) system with three predefined roles. Each role represents a distinct level of access and capability within the platform.

Role	URN	Access Level	Primary Use Case
Admin	`admin`	Full administrative access	Organization administrators
Member	`member`	Standard operational access	Day-to-day platform users
View Only	`view-only`	Read-only access	Auditors, stakeholders

3.2 Admin Role

The Admin role represents the highest level of administrative privilege within a customer organization. Users with this role have complete control over organization settings, user management, and all platform features.

3.2.1 Admin Role Permissions

The Admin role includes all composite permissions available in the platform:

Composite Permission	ACL Code	Capabilities
View All	`view-all`	Read all data
Manage API Tokens	`manage-api-tokens`	Create and delete tokens
Manage Settings	`manage-settings`	Configure integrations and settings
Manage Sub-Orgs	`manage-sub-organizations`	CRUD sub-organizations
Manage People	`manage-people`	CRUD users and invitations
Manage Roles	`manage-roles`	CRUD roles
Manage SBOMs/VEX	`manage-sboms-and-vex`	Upload, read, delete SBOMs
Manage Assets	`manage-assets`	Update assets and components
Manage Labels	`manage-labels`	CRUD labels
Share SBOM	`share-sbom`	Create and delete shares
Request SBOM	`request-sbom`	Request from vendors
Import OSS	`import-oss`	Import OSS SBOMs
Export Reports	`export-reports`	Generate PDF and VDR reports
Manage Products	`manage-products`	CRUD products
Manage Vuln Triage	`manage-vulnerability-triage`	Create and read triage
Manage Vuln Notifications	`manage-user-vulnerability-notif`	Configure alerts
Create Tickets	`create-tickets`	Create tickets
Manage Alert Config	`manage-alert`	Configure alert rules
Create AI Analysis	`create-ai-model-analysis`	Initiate AI analysis
Manage AI Inventory	`manage-ai-model-inventory`	Read and update AI models

3.2.2 Admin Role Actions

Administrators can perform the following actions:

1. **User Management**
   - Invite new users to the organization
   - Assign and modify user roles
   - Remove users from the organization
   - Configure invite-only access settings
2. **Organization Configuration**
   - Configure single sign-on (SSO) settings

- Set up domain-based access controls
- Manage IP allowlists and denylists
- Configure session timeout policies

3. **Integration Management**
   - Connect **GitHub** repositories for automated SBOM ingestion
   - Configure **Jira** integration for ticket creation
   - Set up **ServiceNow** integration for IT service management
   - Connect **Linear** for issue tracking
4. **Security Policy Configuration**
   - Define service level agreements (`SLAs`) for vulnerability remediation
   - Configure vulnerability enrichment settings
   - Set up organization-wide alerts
   - Manage **Sharing Portal** settings

3.3 Member Role

The Member role provides standard access for day-to-day platform usage. Members can manage content and perform operational tasks but cannot modify organization settings or manage other users.

3.3.1 Member Role Permissions

Composite Permission	ACL Code	Capabilities
View All	`view-all`	Read all data
Manage API Tokens	`manage-api-tokens`	Create and delete tokens
Create API Token	`create-api-token`	Create new tokens
Delete API Token	`delete-api-token`	Delete tokens
Manage SBOMs/VEX	`manage-sboms-and-vex`	Upload, read, delete SBOMs
Share SBOM	`share-sbom`	Create and delete shares
Request SBOM	`request-sbom`	Request from vendors
Import OSS	`import-oss`	Import OSS SBOMs
Manage Assets	`manage-assets`	Update assets and components
Manage Labels	`manage-labels`	CRUD labels
Export Reports	`export-reports`	Generate PDF and VDR reports
Manage Products	`manage-products`	CRUD products
Manage Vuln Triage	`manage-vulnerability-triage`	Create and read triage
Manage Vuln Notifications	`manage-user-vulnerability-notif`	Configure notifications
Create Tickets	`create-tickets`	Create tickets
Create AI Analysis	`create-ai-model-analysis`	Initiate AI analysis
Manage AI Inventory	`manage-ai-model-inventory`	Read and update AI models

3.3.2 Member Role Limitations

Members cannot:

- Manage other users or roles
- Configure organization-wide settings
- Manage integrations
- Configure SLAs or sharing portal
- Create or manage sub-organizations

3.4 View Only Role

The View Only role provides read-only access to platform data. This role is designed for stakeholders who need visibility into the organization's software security posture without the ability to modify data.

3.4.1 View Only Role Permissions

Composite Permission	ACL Code	Capabilities
View All	`view-all`	Read all data
Export Reports	`export-reports`	Generate PDF and VDR reports

3.4.2 View Only Role Use Cases

- External auditors reviewing compliance posture
- Executive stakeholders monitoring security metrics
- Third-party assessors validating SBOM inventory
- Compliance officers verifying vulnerability management

3.5 Detailed Permission Reference

3.5.1 Granular Permissions by Resource

The following tables provide a complete reference of all granular permissions available in the platform, organized by resource category. All API routes are prefixed with `/v1/`.

> Permission identifiers use the format **`action:resource`** (for example, `read:asset` or `create:product`). These identifiers are used for authorization checks throughout the platform. The tables below list each permission with its corresponding API endpoint.

AI and Model Permissions

Permission	API Route	Method	Description
read:ai-model	/v1/models	GET	View AI models
create:ai-model-analys	/v1/model-analysis	POST	Start analysis
read:ai-model-analysis	/v1/model-analysis	GET	View results
read:ai-model-inventory	/v1/models/inventory	GET	View inventory
update:ai-model-invento	/v1/model-analysis/inventory	PUT	Update inventory
create:ai-model-reques	/v1/model-analysis/inventory	PUT	Create model request
update:ai-model-reques	/v1/model-analysis/inventory	PUT	Update model request
read:ai-risk-policy	/v1/policies/ai	GET	View AI risk policies
update:ai-risk-policy	/v1/policies/ai	PUT	Update AI risk policies

Asset and Component Permissions

Permission	API Route	Method	Description
read:asset	/v1/asset/:id	GET	View asset
update:asset	/v1/asset/:id	PUT	Update asset
read:component	/v1/component/:id	GET	View component
update:component	/v1/component/:id	PUT	Update component

Report Generation Permissions

Permission	API Route	Method	Description
read:asset-vdr-report	/v1/asset/exportVulnerabil	GET	Export vulnerability CSV
create:product-vdr-repo	/v1/file-request	POST	Request file generation
read:sbom-and-vex	/v1/download/:fileid?	GET	Download SBOM/VEX file
read:sbom-and-vex	/v1/download/bundle	GET	Download bundled SBOMs

API Token Permissions

Permission	API Route	Method	Description
`create:api-token`	`/v1/api-token/create`	POST	Create token
`read:api-token`	`/v1/api-token/:orgId?`	GET	List tokens
`delete:api-token`	`/v1/api-token/:id`	DELETE	Revoke token

Integration Permissions

Permission	API Route	Method	Description
`create:integration`	`/v1/integration/github`	POST	Create integration
`read:integration`	`/v1/integration`	GET	View integrations
`update:integration`	`/v1/integration/:id`	PUT	Update integration
`delete:integration`	`/v1/integration/:id`	DELETE	Remove integration

Label Permissions

Permission	API Route	Method	Description
`create:label`	`/v1/label`	POST	Create label
`read:label`	`/v1/labels`	GET	List labels
`update:label`	`/v1/label/:id`	PUT	Update label
`delete:label`	`/v1/label/:id`	DELETE	Delete label

License Permissions

Permission	API Route	Method	Description
`read:license`	`/v1/licenses`	GET	View licenses
`read:license`	`/v1/license/:id`	GET	View single license
`update:license`	`/v1/license/:id`	PUT	Update license attributes

Organization and Settings Permissions

Permission	API Route	Method	Description
`update:enrichment-setting`	`/v1/organizations`	PUT	Update org settings
`create:organization-alert`	`/v1/organization/notificat`	POST	Create alert
`read:organization-alert`	`/v1/organization/notificat`	GET	View alerts
`update:organization-alert`	`/v1/organization/notificat`	PUT	Update alert

Product Permissions

Permission	API Route	Method	Description
`create:product`	`/v1/product`	POST	Create product
`read:product`	`/v1/product/:id`	GET	View product
`update:product`	`/v1/product/:id`	PUT	Update product
`delete:product`	`/v1/product/:id`	DELETE	Delete product

Role Permissions

Permission	API Route	Method	Description
`read:role`	`/v1/roles`	GET	List roles
`read:role`	`/v1/role/:urn`	GET	View role details
`read:role` , `read:user`	`/v1/role/:urn/users`	GET	View users in role

> Roles are predefined in the platform. Create, update, and delete operations are not available via the API.

SBOM and VEX Permissions

Permission	API Route	Method	Description
`create:sbom-and-vex`	`/v1/upload`	PUT	Upload SBOM or VEX file
`create:sbom-and-vex`	`/v1/upload/sbom/initiate`	POST	Initiate async SBOM upload
`create:sbom-and-vex`	`/v1/upload/sbom/complete/:`	POST	Complete async SBOM upload
`read:sbom-and-vex`	`/v1/sboms`	GET	View SBOMs
`delete:sbom-and-vex`	`/v1/sboms/:id`	DELETE	Delete SBOM/VEX
`create:sbom-oss`	`/v1/asset/:id/syncOSSAsset`	POST	Import from OSS registry
`read:sbom-oss`	`/v1/oss-ingests`	GET	View OSS imports
`read:sbom-oss`	`/v1/oss-ingest/:ossIngestI`	GET	View single OSS import
`create:sbom-share`	`/v1/portal/sbomshare`	POST	Share SBOM via portal
`create:sbom-share`	`/v1/sboms/share`	POST	Share SBOM
`read:sbom-share`	`/v1/portal/sbom/:sbomId/us`	GET	View SBOM share recipients
`delete:sbom-share`	`/v1/portal/sbomshare/:sbom`	DELETE	Revoke SBOM share

> SBOM and VEX files are uploaded through the unified `/v1/upload` endpoint. The system automatically detects the file type. Separate `/v1/sbom` and `/v1/vex` endpoints are not available.

Sharing Portal Permissions

Permission	API Route	Method	Description
`read:sharing-portal`	`/v1/portal`	GET	View portal settings
`update:sharing-portal`	`/v1/portal`	POST	Update portal settings

SLA Permissions

Permission	API Route	Method	Description
`read:sla`	`/v1/sla/setting`	GET	View SLA settings
`update:sla`	`/v1/sla/setting`	POST	Create or update SLA
`read:sla`	`/v1/sla/violations`	GET	View SLA violations

> SLA creation and updates are handled through the same POST endpoint using the `update:sla` permission.

Sub-Organization Permissions

Permission	API Route	Method	Description
`create:sub-organizatio`	`/v1/sub-organizations`	POST	Create sub-org
`read:sub-organization`	`/v1/organization/child`	GET	View sub-orgs
`update:sub-organizatio`	`/v1/sub-organizations/:subOrg`	PUT	Update sub-org
`delete:sub-organizatio`	`/v1/sub-organizations/:subOrg`	DELETE	Delete sub-org

Triage Permissions

Permission	API Route	Method	Description
`create:vulnerability-tria`	`/v1/triage`	POST	Record triage decision
`read:vulnerability-triage`	`/v1/triage/statuses`	GET	View triage statuses
`read:vulnerability-triage`	`/v1/triage/history`	GET	View triage history

User Management Permissions

Permission	API Route	Method	Description
`create:user`	`/v1/member`	POST	Invite user
`read:user`	`/v1/member/:id?`	GET	View user
`delete:user`	`/v1/member/:id`	DELETE	Remove user
`read:user`	`/v1/users`	GET	List users
`update:member-invite-onl`	`/v1/organizations/invite`	PUT	Update invite settings

Vulnerability Permissions

Permission	API Route	Method	Description
`read:vulnerability`	`/v1/vulnerabilities`	GET	View vulnerabilities
`read:vulnerability`	`/v1/vulnerability/:id`	GET	View vulnerability details
`create:vulnerability-alert-co`	`/v1/vulnerabilities/al`	POST	Create vuln alert config
`read:vulnerability-alert-conf`	`/v1/vulnerabilities/al`	GET	View vuln alert config
`read:user-vulnerability-notif`	`/v1/user/notification-`	GET	View notification prefs
`update:user-vulnerability-not`	`/v1/user/notification-`	PUT	Update notification prefs

Custom Vulnerability Permissions

Permission	API Route	Method	Description
`create:custom-vulnerabil`	`/v1/vulnerabilities/cust`	POST	Create custom vuln
`read:custom-vulnerabilit`	`/v1/vulnerabilities/cust`	GET	View custom vulns
`update:custom-vulnerabil`	`/v1/vulnerabilities/cust`	PUT	Update custom vuln

Policy Permissions

Permission	API Route	Method	Description
`read:policy`	`/v1/policies`	GET	View policies
`read:policy`	`/v1/policies/:id`	GET	View policy details
`create:policy`	`/v1/policies`	POST	Create policy
`update:policy`	`/v1/policies/:id`	PUT	Update policy

4 Admin Account Lifecycle Procedures

4.1 Account Setup

4.1.1 Initial Organization Setup

When a new organization is created on The Manifest Platform, the following setup process occurs:

1. **Organization Creation**
   - Organization name and identifier are established
   - Default security settings are applied
   - Primary admin account is created
2. **First Admin Account**
   - The first user to register becomes the organization admin
   - Full **Admin** role permissions are automatically assigned
   - `MFA` enrollment is prompted (recommended)
3. **Initial Configuration**
   - Review and configure authentication settings
   - Set up `SSO` if using enterprise identity provider
   - Configure session timeout policies
   - Enable audit logging

4.1.2 Creating Admin Accounts

To create additional administrator accounts:

1. Navigate to **Settings** > **People** (under the Membership section)
2. Click **Add User**
3. Enter the user's email address
4. Select **Admin** from the role dropdown
5. Click **Send Invitation**

The invited user will receive an email with instructions to complete their account setup.

> Limit the number of Admin accounts to the minimum necessary. Each Admin account represents a potential security risk if compromised.

4.1.3 Admin Account Configuration

After creating an admin account, configure the following settings:

Setting	Location	Recommended Configuration
MFA	Configured via Identity Provider (IdP)	Enable TOTP or hardware key
Session Timeout	Managed by IdP	8 hours maximum
Organization API Token	**Settings** > **API Tokens**	Create only if needed
User API Token	**Settings** > **Account** > **API Tokens**	Create only if needed
Vulnerability Alerts	**Settings** > **Vulnerability Alerts**	Enable security alerts

> MFA and session management are handled through your organization's identity provider (IdP) when using SSO, or through The Manifest Platform's authentication system for direct login.

4.2 Multi-Factor Authentication (MFA)

> MFA is strongly recommended for all users, especially administrators. Enabling MFA significantly reduces the risk of account compromise from credential theft or phishing attacks.

4.2.1 MFA Overview

The Manifest Platform supports multi-factor authentication through integration with identity providers. `MFA` provides an additional layer of security by requiring users to verify their identity using multiple factors.

> MFA configuration is managed through your identity provider (IdP), not directly within The Manifest Platform UI. The platform enforces MFA policies set by your IdP during authentication.

4.2.2 MFA Configuration Options

MFA Method	Security Level	User Experience	Recommended For
Email `OTP`	Moderate	Simple	Basic accounts
`TOTP` App	High	Moderate complexity	All users
Hardware Key (`FIDO2`)	Highest	Requires device	Administrators
`SSO` with `MFA`	Varies by IdP	Seamless	Enterprise users

4.2.3 Enabling MFA via Identity Provider

Organizations should configure `MFA` through their identity provider:

1. Configure `MFA` policies in your IdP (**Okta**, **Azure AD**, **Google Workspace**)
2. Set up `SSO` integration with The Manifest Platform
3. `MFA` will be enforced by the IdP during authentication
4. Users will be prompted for MFA as configured in the IdP

For organizations using The Manifest Platform's built-in passwordless authentication (magic link):

1. Users receive a one-time login link via email
2. The email-based authentication provides a form of two-factor verification
3. For enhanced security, enterprise SSO with IdP-managed MFA is recommended

4.2.4 MFA Recovery

If a user loses access to their `MFA` device:

1. Use saved recovery codes (if available from IdP)
2. Contact your IdP administrator for account recovery
3. Follow your organization's IdP recovery procedures
4. User must re-enroll in `MFA` after reset through the IdP

4.3 Session Management

4.3.1 Session Parameters

Parameter	Default Value	Configurable Range	Security Consideration
Session Duration	24 hours	1 to 72 hours	Shorter is more secure
Idle Timeout	30 minutes	5 to 60 minutes	Shorter prevents unauthorized access
Concurrent Sessions	Unlimited	1 to unlimited	Limiting detects credential sharing
Remember Device	30 days	Disabled to 90 days	Convenience vs. security tradeoff

> Session parameters are managed at the platform level. For organizations using SSO, session policies may also be controlled through your identity provider.

4.3.2 Session Security Features

The Manifest Platform implements several session security features:

1. **Secure Cookies**
   - `HTTPOnly` flag prevents JavaScript access
   - `Secure` flag ensures HTTPS-only transmission
   - `SameSite` attribute prevents CSRF attacks
2. **Session Binding**
   - Sessions are bound to the originating IP range
   - User agent validation detects session theft
   - Geographic anomaly detection (enterprise)
3. **Token Rotation**
   - `JWT` tokens are short-lived
   - Refresh tokens enable seamless rotation
   - Compromised tokens expire quickly

4.3.3 Terminating Sessions

Session termination is handled through the following methods:

1. **User Removal**
   - When a user is removed from the organization via **Settings** > **People**, all their active sessions are automatically terminated
2. **API Token Revocation**
   - Revoking a user's API tokens immediately invalidates programmatic access
3. **SSO-Based Session Management**
   - For organizations using SSO, session termination can be managed through the identity provider
   - Disabling a user in the IdP will prevent new session creation
4. **User Self-Service**
   - Users can log out from their current session using the logout option in the application

4.4 API Token Management

> API tokens provide programmatic access to your organization's data. Treat tokens like passwords. Never share them, store them securely, and rotate them regularly.

4.4.1 API Token Overview

API tokens enable programmatic access to The Manifest Platform. Tokens are scoped to specific permissions and have configurable expiration periods.

4.4.2 Creating API Tokens

For Organization Tokens:

1. Navigate to **Settings** > **API Tokens** (under the Organization section)
2. Click **Create Token**
3. Enter a descriptive name for the token
4. Optionally add a description
5. Select the token expiration period (1, 3, 6 months, or 1 year)
6. Click **Create**
7. **Copy the token immediately.** It will not be shown again.

For User Tokens:

1. Navigate to **Settings** > **Account** > **API Tokens**
2. Click **Create Token**
3. Enter a descriptive name for the token
4. Optionally add a description
5. Select the token expiration period (1, 3, or 6 months)
6. Select the permissions to grant to the token

7. Click **Create**
8. **Copy the token immediately.** It will not be shown again.

> User tokens are scoped to the individual user's permissions and provide more granular access control than organization tokens.

4.4.3 API Token Security

Security Measure	Implementation	Purpose
Token Hashing	SHA-256	Tokens stored as hashes only
Rate Limiting	Per-token limits	Prevents abuse
IP Restrictions	Optional allowlist	Limits token usage location
Audit Logging	All API calls logged	Enables investigation

4.4.4 API Token Best Practices

1. **Use descriptive names** that indicate the token's purpose
2. **Set appropriate expiration** based on use case
3. **Store tokens securely** in secrets management systems
4. **Rotate tokens regularly**, at least annually
5. **Monitor token usage** through audit logs
6. **Revoke unused tokens** promptly

4.4.5 Revoking API Tokens

To revoke an API token:

1. Navigate to **Settings** > **API Tokens** (for organization tokens) or **Settings** > **Account** > **API Tokens** (for user tokens)
2. Locate the token to revoke in the token list
3. Click the delete icon (trash icon) in the Actions column
4. Confirm the deletion

> Revoking a token immediately invalidates it. Any systems using the token will lose access.

4.5 Account Decommissioning

> Proper account decommissioning is critical for security. Always revoke access promptly when users leave the organization or change roles. Failure to do so may result in unauthorized access to sensitive data.

4.5.1 User Account Removal

To remove a user from the organization:

1. Navigate to **Settings** > **People** (under the Membership section)
2. Locate the user to remove in the table
3. Click the delete icon (trash icon) in the row actions
4. Confirm the removal in the confirmation dialog

Upon removal:

- All active sessions are terminated
- API tokens created by the user are revoked
- The user loses access to all organization data
- Audit logs retain the user's historical actions

4.5.2 Admin Account Transition

When transitioning admin responsibilities:

1. **Create the new admin account** before removing the old one
2. **Transfer ownership** of critical configurations:
    - Integration credentials
    - API tokens used by external systems
    - Scheduled reports
3. **Document the transition** including date and reason
4. **Verify the new admin** can perform all necessary functions
5. **Remove the old admin account** or downgrade to Member role

4.5.3 Organization Decommissioning

To fully decommission an organization:

1. **Export required data**
    - Download SBOMs and reports
    - Export vulnerability history
    - Save audit logs
2. **Revoke all integrations**
    - Disconnect **GitHub** repositories
    - Remove **Jira**/**ServiceNow** connections
    - Revoke API tokens

3. **Remove all users**
    - Remove Member and View Only users first
    - Remove secondary Admin accounts
    - Primary admin remains until final deletion
4. **Request organization deletion**
    - Contact Manifest Cyber support
    - Provide organization identifier
    - Confirm data deletion requirements

5 Security Settings Reference Table

This section provides a comprehensive reference for security-related settings available in The Manifest Platform. Settings are organized by category and include UI location where applicable.

5.1 Organization Security Settings

5.1.1 Access Control Settings

Setting	Function	Security Impact	Recommended Value
Invite Only	Restricts account creation to invited users	Prevents unauthorized registration	`Enabled`
Domain Restriction	Limits sign-up to specific email domains	Controls organizational boundary	`Configured`
SSO Enforcement	Requires `SSO` for authentication	Centralizes identity management	`Enabled` if using IdP
Role Assignment	Default role for new users	Controls initial access level	**View Only** or **Member**

> **UI Location:** The **Invite Only** setting can be toggled in **Settings** > **People** (Membership section). Domain restrictions and SSO settings are configured through your identity provider.

5.1.2 Session Settings

Setting	Function	Security Impact	Recommended Value
Session Duration	Maximum session length	Limits exposure window	8 to 24 hours
Idle Timeout	Timeout for inactive sessions	Prevents unattended access	15 to 30 minutes
Concurrent Sessions	Number of simultaneous logins	Detects credential sharing	3 to 5 sessions

> Session settings are managed at the platform level and through your identity provider (IdP) when using SSO. Contact Manifest Cyber support to modify platform-level session parameters.

5.1.3 Authentication Settings

Setting	Function	Security Impact	Recommended Value
MFA Requirement	Enforces multi-factor authentication	Reduces credential theft risk	`Enabled` for all users
Password Policy	Minimum password requirements	Ensures password strength	`Strong` (12+ characters)
Account Lockout	Locks account after failed attempts	Prevents brute force attacks	`5` attempts, `15` min lockout

> Authentication settings including MFA, password policies, and account lockout are configured through your identity provider (IdP). The Manifest Platform uses passwordless magic-link authentication for users not on SSO.

5.2 Integration Security Settings

> **UI Location:** All integrations are configured in **Settings** > **Integrations** (Organization section).

5.2.1 GitHub Integration

Setting	Function	Security Impact	Recommended Value
App Installation	GitHub App for repository access	Controls code access scope	Limit to required repos
Webhook Secret	Validates webhook authenticity	Prevents spoofed events	Unique, random secret
Repository Selection	Which repos to monitor	Limits data exposure	Explicit selection

5.2.2 Jira Integration

Setting	Function	Security Impact	Recommended Value
API Token	Authentication for Jira API	Controls Jira access	Dedicated service account
Project Selection	Target projects for tickets	Limits ticket visibility	Security project only
Field Mapping	Maps vulnerability data to fields	Controls data exposure	Minimal required fields

5.2.3 ServiceNow Integration

Setting	Function	Security Impact	Recommended Value
Instance URL	ServiceNow instance endpoint	Identifies target system	Production instance
Authentication	OAuth or basic authentication	Secures API access	OAuth 2.0 preferred
Table Access	Which tables can be modified	Limits ServiceNow impact	Incident table only

5.2.4 Linear Integration

Setting	Function	Security Impact	Recommended Value
API Key	Authentication for Linear API	Controls Linear access	Dedicated service account
Team Selection	Target team for issues	Controls issue visibility	Security team
Label Mapping	Maps severity to Linear labels	Ensures prioritization	Map severity to labels

5.3 Data Security Settings

5.3.1 SBOM Management

Setting	Function	Security Impact	Recommended Value
Auto-Enrichment	Auto-enriches SBOMs with CVE vulnerability data	Enhances visibility	`Enabled`
Enrichment Sources	CVE vulnerability databases used	Controls data sources	`NVD` , `OSV` , `KEV` enabled
Component Matching	Algorithm for matching components	Affects detection accuracy	`Strict` matching
SBOM Retention	Duration to retain SBOM versions	Affects audit trail	`2+` years for compliance

5.3.2 Sharing Portal

Setting	Function	Security Impact	Recommended Value
Portal Enabled	Enables external sharing portal	Allows external sharing	`Enabled` only if needed
Portal URL	Custom URL path for portal	Identifies your portal	Non-guessable path
Logo URL	Custom branding for portal	Visual customization	Use `HTTPS` URL only
Asset Sharing	Controls shareable assets	Limits data exposure	Explicit selection

> **UI Location:** Configure at **Settings** > **Sharing Portal** (Organization section).

5.3.3 Vulnerability Management

Setting	Function	Security Impact	Recommended Value
SLA, Critical	Days to remediate critical CVE vulns	Remediation timeline	`7` days
SLA, High	Days to remediate high CVE vulns	Remediation timeline	`30` days
SLA, Medium	Days to remediate medium CVE vulns	Remediation timeline	`90` days
SLA, Low	Days to remediate low CVE vulns	Remediation timeline	`180` days
EPSS Threshold	Minimum `EPSS` score to flag	Focuses on exploitable	`0.1` (10%)
KEV Alerts	Alert on CISA `KEV` additions	Highlights exploitation	`Enabled`

> **UI Location:** SLA settings are configured at **Settings** > **SLAs** (Organization section). Vulnerability alert settings including KEV and EPSS thresholds are configured at **Settings** > **Vulnerability Alerts** (Organization section).

5.4 Notification and Alerting Settings

5.4.1 Organization Alerts

Setting	Function	Security Impact	Recommended Value
New Critical Vuln	Alert for critical CVE vulnerabilities	Enables rapid response	`Enabled`
New High Vuln	Alert for high CVE vulnerabilities	Enables timely response	`Enabled`
KEV Addition	Alert for `KEV` catalog additions	Highlights exploitation	`Enabled`
SLA Breach Warning	Alert before `SLA` deadline	Prevents violations	`Enabled`, 7 days before
SLA Breach	Alert when `SLA` is missed	Tracks compliance	`Enabled`

> **UI Location:** Configure organization-wide vulnerability alerts at **Settings** > **Vulnerability Alerts** (Organization section). SBOM upload alerts are configured at **Settings** > **SBOM Upload Alerts** (Organization section).

5.4.2 Personal Notification Settings

Setting	Function	Security Impact	Recommended Value
Email Notifications	Receive alerts via email	Ensures awareness	`Enabled` for security
Daily Digest	Consolidated daily summary	Reduces fatigue	`Enabled`
Immediate Alerts	Real-time critical alerts	Enables rapid response	`Critical` only

> Personal notification preferences are configured through the organization's vulnerability alert settings when the user is included as a target recipient.

5.5 API Security Settings

5.5.1 API Token Configuration

Setting	Function	Security Impact	Recommended Value
Maximum Token Age	Maximum token expiration	Limits exposure window	`6` months maximum
Token Permissions	Available permission scopes	Controls API access	Minimal permissions
Rate Limiting	Maximum requests per period	Prevents abuse	Platform default

> **UI Location:** Organization tokens are managed at **Settings** > **API Tokens** (Organization section). User tokens are managed at **Settings** > **Account** > **API Tokens**.

5.5.2 API Access Logging

Setting	Function	Security Impact	Recommended Value
Request Logging	Log all API requests	Enables auditing	`Enabled`
Log Retention	Duration to retain API logs	Supports investigation	`1+` year
Data Masking	Mask sensitive data in logs	Prevents exposure	`Enabled`

5.6 Compliance and Audit Settings

5.6.1 Audit Logging

Setting	Function	Security Impact	Recommended Value
User Activity	Log user actions	Enables accountability	`Enabled`
Admin Actions	Log admin changes	Tracks modifications	`Enabled`
Auth Logging	Log login attempts	Detects unauthorized access	`Enabled`
Log Export	Export logs to `SIEM`	Centralized monitoring	`Enabled` for enterprise

5.6.2 Data Export

Setting	Function	Security Impact	Recommended Value
SBOM Export Format	Default SBOM download format	Ensures compatibility	`CycloneDX` or `SPDX`
Report Generation	Who can generate reports	Controls data extraction	Based on role
Bulk Export	Enable bulk data export	Affects exfiltration risk	**Admin** role only

6 Appendix A: Glossary

Term	Full Name	Definition
SBOM	Software Bill of Materials	A formal record of the components used to build software
VEX	Vulnerability Exploitability eXchange	A document that communicates the exploitability status of vulnerabilities
CVE	Common Vulnerabilities and Exposures	A standardized identifier for publicly known security vulnerabilities
EPSS	Exploit Prediction Scoring System	A model that predicts the probability of vulnerability exploitation
KEV	Known Exploited Vulnerabilities	CISA's catalog of vulnerabilities that are actively exploited in the wild
RBAC	Role-Based Access Control	An access control method based on user roles within an organization
MFA	Multi-Factor Authentication	Authentication requiring multiple verification methods
SSO	Single Sign-On	Authentication allowing one login for multiple applications
SLA	Service Level Agreement	Defined timelines and expectations for vulnerability remediation
NVD	National Vulnerability Database	The U.S. government repository of vulnerability management data
OSV	Open Source Vulnerabilities	Google's distributed vulnerability database for open source software
JWT	JSON Web Token	A compact, URL-safe token format for securely transmitting information
TOTP	Time-based One-Time Password	An algorithm that generates temporary passwords based on time
FIDO2	Fast Identity Online 2	A passwordless authentication standard using public key cryptography
IdP	Identity Provider	A service that creates, maintains, and manages user identity information

7 Appendix B: Compliance Mapping

7.1 FedRAMP Control Coverage

This Security Admin Guide addresses the following FedRAMP Recommended Secure Configuration (RSC) requirements:

Control	Requirement	Guide Section
FRR-RSC-01	Guidance on securely accessing, configuring, operating, and decommissioning top-level administrative accounts	Section 3: Role Definitions, Section 4: Lifecycle Procedures
FRR-RSC-02	Guidance on security-related settings operated by top-level administrative accounts and their security implications	Section 5: Security Settings Reference
FRR-RSC-09	Publish recommended secure configuration guidance publicly	Entire document (publicly available)

7.2 Additional Standards Alignment

This guide also supports compliance with:

- NIST SP 800-53 (Access Control family)
- SOC 2 Type II (Security, Availability)
- ISO 27001 (Access Control, Operations Security)
- CIS Controls (Account Management, Access Control Management)

8 Appendix C: Document History

Version	Date	Author	Changes
1.0	January 2026	Manifest Cyber	Initial Release

9 Appendix D: Contact Information

For questions about this guide or The Manifest Platform security:

- **Security Team:** security@manifestcyber.com
- **Support:** support@manifestcyber.com