VIOE - Vulnerability Intelligence & Orchestration Engine

Admin Setup & Configuration Guide

Document Version: 1.0 **Classification:** Internal - Administrator Only **Last Updated:** January 2026

Table of Contents

1. Introduction

1.1 Purpose of This Guide

This guide provides administrators with comprehensive instructions for setting up, configuring, and maintaining the VIOE platform. Following these procedures will ensure optimal system performance, security, and user adoption.

1.2 Administrator Responsibilities

As a VIOE administrator, you are responsible for:

- Initial platform configuration
- User account management and onboarding
- Team creation and organization
- Scanner integration setup
- Suppression rule management
- AI configuration tuning
- Notification settings
- Ongoing system maintenance

1.3 Prerequisites

Before beginning configuration:

- Administrator access credentials
- Organization structure documentation
- List of vulnerability scanning tools in use
- Team lead contact information
- Slack workspace details (if applicable)
- Jira project information (if applicable)

---

2. Initial System Setup

2.1 First Administrator Login

Step 1: Access your organization's VIOE URL

Step 2: Log in with the initial administrator credentials provided during deployment

Step 3: Complete the mandatory password change

Step 4: Enable multi-factor authentication (strongly recommended)

[Screenshot Placeholder: Initial administrator login screen]

2.2 System Configuration Checklist

Complete the following tasks in order:

Order	Task	Section Reference
1	Create organizational teams	Section 10
2	Configure AI ownership settings	Section 7
3	Set up scanner integrations	Section 8
4	Create initial suppression rules	Section 6
5	Configure notifications	Section 9
6	Onboard initial users	Section 3
7	Import first vulnerability scan	User Guide
8	Validate AI assignments	User Guide

2.3 Recommended Initial Configuration

AI Ownership Settings:

- Enable Git Commit Analysis: ON
- Enable CODEOWNERS Parsing: ON
- Directory Integration: Configure if Okta/AD available
- Minimum Confidence Threshold: 70% (balanced approach)

Notification Settings:

- New Critical Vulnerability: ON
- SLA Approaching: ON
- Low Confidence Assignment: ON
- Daily Summary: ON

---

3. User Onboarding

3.1 User Account Creation

VIOE uses the Base44 authentication system. User accounts are managed through the platform's identity provider.

To add a new user:

1. Ensure the user exists in your identity provider (Okta, Active Directory, or Base44 native)
2. The user can access VIOE using their organizational credentials
3. Upon first login, assign the user to appropriate teams

3.2 Onboarding Checklist for New Users

For each new user:

Step	Action	Responsible Party
1	Create account in identity provider	IT Admin
2	Communicate VIOE URL and login instructions	VIOE Admin
3	Assign user to team(s)	VIOE Admin
4	Provide role-appropriate training materials	VIOE Admin
5	Verify successful login	User
6	Complete initial orientation	User

3.3 User Communication Template

Subject: Welcome to VIOE - Your Vulnerability Management Platform

```
Dear [User Name],

You have been granted access to VIOE (Vulnerability Intelligence & Orchestration Engine

ACCESS INFORMATION:
- URL: [Your VIOE URL]
- Login: Use your organizational credentials
- Team Assignment: [Team Name]

GETTING STARTED:
1. Log in using the URL above
2. Review the Dashboard for current vulnerability status
3. Refer to the Product Owner Guide for detailed instructions

SUPPORT:
For technical issues, contact [Support Contact]
For questions about your assignments, contact [Team Lead Name]
```

```
Best regards,
[Administrator Name]
```

3.4 Bulk User Import

For large organizations, users can be imported via directory synchronization:

1. Navigate to Settings
2. Configure directory integration (Okta or Active Directory)
3. Enable automatic user provisioning
4. Map directory groups to VIOE teams

---

4. Roles & Permissions Management

4.1 Available Roles

VIOE supports the following user roles:

Role	Access Level	Primary Functions
Administrator	Full system access	Configuration, user management, all features
Security Manager	Elevated access	Dashboards, incidents, strategic features
Security Analyst	Standard access	Vulnerabilities, tasks, triage
Team Lead	Team-scoped access	Team vulnerabilities, performance metrics
Compliance Officer	Compliance focus	Compliance reports, evidence, frameworks
Remediation Engineer	Task focus	Remediation tasks, Jira integration
View Only	Read-only access	Dashboards and reports only

4.2 Role Assignment

To assign or change a user's role:

1. Access the user management section
2. Locate the user

3. Select the appropriate role from the dropdown
4. Save changes

Note: Role changes take effect immediately upon save.

4.3 Permission Inheritance

- Team-level permissions are inherited by all team members
- Users can belong to multiple teams
- The highest permission level applies when conflicts exist
- Administrator role overrides all other permissions

4.4 Role-Based Access Matrix

Feature	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
Dashboard	✓	✓	✓	✓	✓	✓	✓
Vulnerabilities	✓	✓	✓	✓ (team)	✓	✓ (team)	✓
Remediation Tasks	✓	✓	✓	✓ (team)	✓	✓	✓
Create Tasks	✓	✓	✓	✓	-	✓	-
Import Vulns	✓	✓	✓	-	-	-	-
Incidents	✓	✓	✓	-	-	-	✓
Threat Hunting	✓	✓	✓	-	-	-	✓
Compliance Reports	✓	✓	-	-	✓	-	✓
Settings	✓	-	-	-	-	-	-
Team Management	✓	✓	-	-	-	-	-

---

5. Admin Panel Walkthrough

5.1 Accessing Settings

1. Click "Settings" in the left navigation panel
2. The Settings page displays four main configuration tabs

[Screenshot Placeholder: Settings page with four configuration tabs visible]

5.2 Settings Tabs Overview

Tab 1: Noise Suppression

- Create and manage suppression rules
- View suppression statistics
- Toggle rules active/inactive

Tab 2: AI Ownership

- Configure AI assignment methods
- Set confidence thresholds
- Enable/disable data sources

Tab 3: Integrations

- Configure vulnerability scanner connections
- Set up Jira integration
- Manage Slack notifications

Tab 4: Notifications

- Configure alert preferences
- Set notification channels
- Manage digest schedules

5.3 Settings Navigation

Each settings tab contains:

- Configuration options with toggle switches
- Save/Apply buttons for changes
- Help text explaining each option

- Status indicators showing current state

---

6. Noise Suppression Configuration

6.1 Understanding Suppression Rules

Suppression rules automatically filter out findings that are not actionable, reducing noise and allowing teams to focus on real risks.

Why Suppression Matters:

- Reduces analyst fatigue from reviewing false positives
- Focuses attention on production-relevant issues
- Improves signal-to-noise ratio
- Accelerates triage process

6.2 Suppression Rule Types

Rule Type	Description	Use Case
Environment	Filter by environment	Suppress non-production findings
Asset Pattern	Regex match on asset names	Ignore legacy systems being retired
Severity + Environment	Combination rule	Suppress Low severity in staging
Duplicate	Same CVE in same asset	Prevent duplicate tracking
Age-Based	Findings older than threshold	Filter old unexploited issues

6.3 Creating a Suppression Rule

Step 1: Navigate to Settings → Noise Suppression tab

Step 2: Click "Create Rule" or "Add New Rule"

Step 3: Configure the rule:

- **Rule Name:** Descriptive name (e.g., "Non-Production Environment Filter")
- **Rule Type:** Select from dropdown
- **Conditions:** Specify criteria based on rule type

- **Active:** Toggle ON to enable immediately

Step 4: Click Save

[Screenshot Placeholder: Create suppression rule dialog with fields filled in]

6.4 Recommended Suppression Rules

Rule 1: Non-Production Environment Filter

- Type: Environment
- Condition: Environment NOT IN ['production']
- Purpose: Focus on production vulnerabilities

Rule 2: Legacy System Exclusion

- Type: Asset Pattern
- Condition: Asset name matches 'legacy-' *or* '*deprecated*-'
- Purpose: Exclude systems being decommissioned

Rule 3: Low Severity in Development

- Type: Severity + Environment
- Condition: Severity = 'low' AND Environment = 'development'
- Purpose: Deprioritize low-risk development findings

Rule 4: Duplicate CVE Prevention

- Type: Duplicate
- Condition: Same CVE ID + Same Asset
- Purpose: Prevent tracking same issue multiple times

6.5 Managing Existing Rules

To edit a rule:

1. Locate the rule in the suppression rules list
2. Click the edit icon
3. Modify settings as needed
4. Save changes

To disable a rule temporarily:

1. Locate the rule

2. Toggle the "Active" switch to OFF
3. The rule will stop suppressing new findings

To delete a rule:

1. Locate the rule
2. Click the delete icon
3. Confirm deletion

Note: Deleting a rule does not un-suppress previously suppressed findings.

6.6 Monitoring Suppression Effectiveness

The suppression dashboard shows:

- **Suppressed Count:** Total findings suppressed per rule
- **Active Rules:** Number of rules currently active
- **Noise Reduction %:** Percentage of findings suppressed

Review suppression effectiveness monthly to ensure rules are working as intended and not hiding legitimate issues.

---

7. AI Ownership Settings

7.1 Understanding AI Assignment

VIOE uses artificial intelligence to automatically determine which team should own each vulnerability. The AI analyzes multiple data sources to make this determination.

7.2 AI Data Sources

Git Commit Analysis

- Analyzes code repository history
- Identifies who modified affected files
- Maps committers to teams
- Enable: Recommended for all organizations with Git

CODEOWNERS File Parsing

- Reads CODEOWNERS files in repositories

- Provides explicit ownership mapping
- High accuracy when maintained
- Enable: Recommended if CODEOWNERS files exist

Directory Integration

- Connects to Okta or Active Directory
- Maps users to organizational structure
- Enhances team identification
- Enable: Recommended for enterprise organizations

7.3 Configuring AI Settings

Step 1: Navigate to Settings → AI Ownership tab

Step 2: Configure data sources:

Setting	Recommendation	Toggle
Git Commit Analysis	Enable for code-based ownership	ON
CODEOWNERS Parsing	Enable if files exist	ON
Directory Integration	Enable for org structure	ON (if available)

Step 3: Set confidence threshold:

- **50%:** Accept more AI assignments (higher volume, lower accuracy)
- **70%:** Balanced approach (recommended for most organizations)
- **90%:** High accuracy only (lower volume, requires more manual triage)

Step 4: Save configuration

[Screenshot Placeholder: AI Ownership settings with toggles and threshold slider]

7.4 Confidence Threshold Guidelines

Threshold	Best For	Trade-off
50%	High-volume, mature security teams	More assignments accepted, some may need correction
70%	Most organizations	Balanced accuracy and automation
90%	Compliance-sensitive environments	Only high-confidence assignments, more manual work

7.5 Tuning AI Performance

If too many assignments are incorrect:

1. Increase confidence threshold
2. Verify CODEOWNERS files are accurate
3. Review Git repository configurations
4. Ensure directory integration is mapping correctly

If too many items require manual assignment:

1. Decrease confidence threshold
2. Enable additional data sources
3. Review team definitions for overlaps
4. Ensure all relevant repositories are connected

7.6 AI Assignment Audit Trail

All AI assignments are logged in the Ownership History for each vulnerability:

- Previous team assignment
- New team assignment
- Confidence score at time of assignment
- Change type (AI vs. manual)
- Timestamp

---

8. Scanner Integration Setup

8.1 Supported Vulnerability Scanners

VIOE supports integration with the following vulnerability scanning tools:

Scanner	Type	Integration Method
Snyk	Application Security	API / File Import
SonarQube	Code Quality & Security	API / File Import
Checkmarx	Static Application Security	API / File Import
Qualys	Infrastructure Vulnerability	API / File Import
Tenable	Infrastructure Vulnerability	API / File Import
Rapid7	Infrastructure Vulnerability	API / File Import

8.2 Integration Methods

API Integration (Recommended)

- Real-time synchronization
- Automatic import of new findings
- Bidirectional status updates

File Import

- Manual upload of scan results
- Supported formats: CSV, JSON, Excel, PDF
- Suitable for air-gapped environments

8.3 Configuring Scanner Integration

Step 1: Navigate to Settings → Integrations tab

Step 2: Locate the scanner you wish to configure

Step 3: Click "Configure" button for that scanner

Step 4: Enter required credentials:

- API URL/Endpoint
- API Key or Token
- Project/Organization identifier (if applicable)

Step 5: Test connection

Step 6: Save configuration

[Screenshot Placeholder: Scanner integration configuration dialog]

8.4 Scanner-Specific Configuration

Snyk Configuration:

- API Token: Generate from Snyk dashboard
- Organization ID: Found in Snyk settings
- Project filter: Optional, to limit which projects sync

SonarQube Configuration:

- Server URL: Your SonarQube instance URL
- API Token: Generate from SonarQube user settings
- Project Key: Specific project to monitor

Qualys Configuration:

- API URL: Qualys platform URL
- Username/Password or API credentials
- Asset group filter: Optional

8.5 Import Scheduling

For API integrations, configure import frequency:

- **Real-time:** Immediate sync (may impact performance)
- **Hourly:** Balanced approach
- **Daily:** Lower system load
- **Manual:** On-demand only

8.6 Jira Integration Setup

Step 1: Navigate to Settings → Integrations → Jira

Step 2: Enter Jira configuration:

- Jira URL: Your Atlassian instance URL
- API Token: Generated from Atlassian account settings
- Project Key: Target project for vulnerability tasks

- Issue Type: Default issue type (e.g., Bug, Task)

Step 3: Configure field mappings:

- Severity → Jira Priority
- Title → Summary
- Description → Description
- Assigned Team → Assignee (optional)

Step 4: Test connection and save

---

9. Notification Configuration

9.1 Available Notification Types

Notification	Trigger	Default State
New Critical Vulnerability	Critical severity finding imported	Enabled
SLA Approaching	48 hours before remediation deadline	Enabled
Low Confidence Assignment	AI confidence below threshold	Enabled
Daily Summary	End of business day digest	Enabled

9.2 Configuring Notifications

Step 1: Navigate to Settings → Notifications tab

Step 2: For each notification type:

- Toggle ON/OFF as desired
- Configure timing (where applicable)
- Set recipient preferences

Step 3: Save configuration

9.3 Notification Channels

Email Notifications:

- Sent to user's registered email

- Configurable digest format
- HTML-formatted for readability

Slack Integration:

- Post to team channels
- Real-time alerts
- Interactive buttons for quick actions

9.4 Slack Integration Setup

Step 1: Navigate to Settings → Integrations → Slack

Step 2: Click "Connect to Slack"

Step 3: Authorize VIOE in your Slack workspace

Step 4: Configure channel mappings:

- Map each team to their Slack channel
- Set notification preferences per channel

Step 5: Test notification delivery

9.5 Notification Best Practices

- Enable Critical Vulnerability alerts for immediate response
- Use Daily Summary to prevent alert fatigue
- Configure team-specific channels for relevant notifications
- Review notification effectiveness quarterly

---

10. Team Management

10.1 Creating Teams

Step 1: Navigate to the Teams page

Step 2: Click "Create Team" button

Step 3: Enter team details:

- **Team Name:** Descriptive name (e.g., "Platform Engineering", "Frontend Team")

- **Lead Email:** Team lead's email address
- **Slack Channel:** Team's Slack channel (optional but recommended)

Step 4: Save team

[Screenshot Placeholder: Create team dialog with form fields]

10.2 Team Structure Recommendations

Option 1: By Technical Domain

- Platform Team
- Frontend Team
- Backend Team
- Infrastructure Team
- Data Team

Option 2: By Product Area

- Core Product Team
- Payments Team
- User Management Team
- Integrations Team

Option 3: Hybrid Approach

- Combine domain and product for larger organizations
- Example: "Payments - Backend", "Payments - Frontend"

10.3 Managing Team Members

Team membership is determined by:

1. User's organizational assignment (from directory integration)
2. Manual assignment by administrators
3. Self-assignment (if permitted)

10.4 Team Performance Monitoring

The Teams page displays performance metrics:

- Total vulnerabilities assigned

- Critical and High severity counts
- Open vs. Resolved counts
- Resolution trends over time

Use these metrics to:

- Identify teams needing additional resources
- Recognize high-performing teams
- Balance workload across organization

10.5 Team Archival

To deactivate a team:

1. Reassign all open vulnerabilities to another team
2. Archive the team (maintains historical data)
3. Archived teams do not appear in assignment options

---

11. Environment & Configuration Settings

11.1 Environment Definitions

VIOE recognizes the following environments:

Environment	Description	Typical SLA	Suppression
Production	Live customer-facing systems	Shortest	No
Staging	Pre-production testing	Medium	Optional
Development	Developer workstations	Longest	Often

11.2 SLA Configuration

Service Level Agreements define remediation deadlines by severity:

Severity	Recommended SLA	Configurable Range
Critical	7 days	1-14 days
High	30 days	7-60 days
Medium	60 days	30-90 days
Low	90 days	60-180 days

To configure SLAs:

1. Contact your system administrator
2. SLA configuration may require platform-level access

11.3 Data Retention Settings

Configure how long data is retained:

- **Active vulnerabilities:** Indefinite
- **Resolved vulnerabilities:** Configurable (default: 2 years)
- **Audit logs:** Configurable (default: 3 years)
- **Reports:** Configurable (default: 5 years)

11.4 Backup Configuration

Ensure data protection:

- Automatic backups are managed by the platform
- Verify backup schedule meets organizational requirements
- Test restore procedures periodically

---

12. Configuration Best Practices

12.1 Initial Setup Best Practices

1. **Start with conservative AI settings** - Use 70% confidence threshold initially
2. **Create teams before importing data** - Enables immediate AI assignment
3. **Configure critical notifications first** - Ensures no critical issues are missed
4. **Test with a small data set** - Validate configuration before full import

12.2 Ongoing Maintenance Best Practices

Weekly Tasks:

- Review low-confidence assignments
- Monitor suppression rule effectiveness
- Check for failed integrations

Monthly Tasks:

- Review team performance metrics
- Audit suppression rules
- Validate AI assignment accuracy
- Update team configurations as needed

Quarterly Tasks:

- Comprehensive configuration review
- User access audit
- Integration health check
- SLA appropriateness review

12.3 Security Best Practices

1. **Limit administrator access** - Only essential personnel
2. **Enable MFA for all administrators** - Required for security
3. **Audit admin actions** - Review logs regularly
4. **Rotate API credentials** - Annual rotation at minimum
5. **Review suppression rules** - Ensure no security issues are hidden

12.4 Performance Best Practices

1. **Use appropriate import schedules** - Daily for most organizations
2. **Archive old data** - Follow retention policies
3. **Monitor system metrics** - Watch for performance degradation
4. **Scale resources as needed** - Based on data volume

12.5 Documentation Best Practices

Maintain documentation of:

- Custom suppression rules and rationale
- Team structure and ownership mapping
- Integration configurations
- SLA definitions
- Exception approvals

12.6 Troubleshooting Quick Reference

Issue	Likely Cause	Resolution
AI not assigning	Threshold too high	Lower confidence threshold
Too much noise	Insufficient suppression	Create appropriate rules
Missing vulnerabilities	Suppression too aggressive	Review and adjust rules
Jira sync failing	Credential expiry	Refresh API token
Slow performance	Large data volume	Optimize retention settings

---

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document is confidential and intended for authorized administrators only.