CRISP Platform - Comprehensive User Manual

Cyber Risk Information Sharing Platform

Table of Contents

Introduction

Welcome to the CRISP (Cyber Risk Information Sharing Platform), a comprehensive threat intelligence sharing ecosystem designed to enhance cybersecurity through secure, collaborative information exchange between organizations.

Platform Overview

CRISP enables organizations to share threat intelligence, indicators of compromise (IoCs), and security insights while maintaining strict security controls and compliance standards. The platform supports multiple user roles with varying levels of access and functionality, ensuring that each user has the appropriate tools and permissions for their responsibilities.

Key Features

- **Secure Information Sharing**: Protected threat intelligence exchange between trusted organizations
- **Role-Based Access Control**: Four distinct user roles with appropriate permissions and capabilities
- **Trust Relationship Management**: Sophisticated trust networks enabling selective information sharing
- **Advanced Analytics**: Comprehensive reporting and analytics for threat intelligence effectiveness
- **STIX Compliance**: Industry-standard threat intelligence formats and protocols
- **Real-Time Alerts**: Immediate notification system for critical threats and updates
- **Audit & Compliance**: Complete audit trails and compliance reporting capabilities

Who Can Benefit

- **Security Operations Centers (SOCs)**: Enhanced threat detection and response capabilities
- **Threat Intelligence Teams**: Collaborative intelligence sharing and analysis
- **IT Security Departments**: Comprehensive organizational security oversight
- **Incident Response Teams**: Real-time threat information for faster response
- **Compliance Teams**: Audit trails and regulatory compliance support
- **Executive Leadership**: Strategic security insights and performance metrics

---

Getting Started

System Requirements

Minimum Requirements

- **Operating System**: Windows 10/11, macOS 10.14+, or Linux Ubuntu 18.04+
- **Web Browser**: Chrome 90+, Firefox 88+, Safari 14+, or Edge 90+
- **Internet Connection**: Broadband connection recommended
- **Screen Resolution**: 1280x720 minimum, 1920x1080 recommended
- **Memory**: 4GB RAM minimum, 8GB recommended

Recommended Setup

- **Dual Monitor**: For enhanced productivity with multiple dashboards
- **High-Speed Internet**: For real-time threat intelligence updates
- **Modern Browser**: Latest version for optimal performance and security

Initial Account Setup

1. Account Registration

Your organization's administrator will provide you with:

- Platform URL (e.g., `https://your-org.crisp-platform.com`)
- Username (typically your email address)
- Temporary password
- Role assignment information

2. First Login Process

1. Navigate to your organization's CRISP platform URL
2. Enter your username and temporary password
3. Complete two-factor authentication setup (if required)
4. Change your temporary password to a secure password
5. Review and accept terms of service and privacy policy
6. Complete your user profile information

3. Profile Configuration

Complete your user profile with:

- **Personal Information**: Name, department, job title
- **Contact Details**: Phone number, email verification
- **Security Preferences**: Notification settings, alert preferences
- **Organizational Context**: Department, security clearance level

4. Security Setup

- **Password Requirements**: Minimum 12 characters with complexity requirements
- **Two-Factor Authentication**: Setup using authenticator app or SMS
- **Trusted Devices**: Register frequently used devices
- **Session Management**: Configure session timeout preferences

---

Role-Based Access Overview

CRISP implements a hierarchical role-based access control system with four distinct user roles, each with specific capabilities and responsibilities.

Role Hierarchy

BlueVisionAdmin (Platform-wide administration)
↓
Admin (Organization-level administration)
↓
Publisher (Content creation and user management)
↓
Viewer (Read-only threat intelligence access)

Role Capabilities Matrix

Capability	Viewer	Publisher	Admin	BlueVisionAdmin
View Threat Intelligence	✅	✅	✅	✅
Export Data	✅	✅	✅	✅
Create Content	❌	✅	✅	✅
Manage Trust Relationships	❌	✅	✅	✅
Create Viewer Users	❌	✅	✅	✅
Create Publisher Users	❌	❌	✅	✅
Create Admin Users	❌	❌	✅	✅
Create Trust Groups	❌	❌	✅	✅
System Administration	❌	❌	❌	✅
Cross-Org Management	❌	❌	❌	✅

Role Assignment Process

Role assignments are determined by:

1. **Organizational Needs**: Based on job function and responsibilities
2. **Security Clearance**: Alignment with organizational security policies
3. **Business Requirements**: Access levels needed for effective job performance
4. **Approval Workflow**: Management approval for elevated roles

---

Dashboard Navigation

Main Navigation Menu

The CRISP platform features a responsive navigation menu that adapts based on your user role:

Universal Navigation Elements

- **Dashboard**: Central overview and activity feed
- **Threat Intelligence**: Access to threat data and indicators

- **Reports**: Analytics and reporting tools
- **Profile**: Personal account management
- **Help & Support**: Documentation and assistance

Role-Specific Navigation

Publisher Additional Elements:

- **User Management**: Create and manage Viewer accounts
- **Trust Management**: Establish and maintain trust relationships
- **Content Publishing**: Create and share threat intelligence
- **Email Alerts**: Manage threat notification campaigns

Admin Additional Elements:

- **Organization Management**: Configure organizational settings
- **Advanced User Management**: Manage all user types
- **Trust Groups**: Create and administer trust groups
- **Advanced Analytics**: Comprehensive organizational metrics

BlueVisionAdmin Additional Elements:

- **System Administration**: Platform-wide management
- **Global Analytics**: Cross-organizational insights
- **Platform Configuration**: System-level settings

Dashboard Customization

Widget Configuration

Users can customize their dashboard with:

- **Threat Summary Widgets**: Current threat levels and alerts
- **Activity Feed**: Recent actions and updates
- **Analytics Charts**: Visual representation of key metrics
- **Quick Actions**: Frequently used function shortcuts
- **Trust Network Status**: Health of trust relationships

Layout Options

- **Grid Layout**: Organize widgets in customizable grid
- **Responsive Design**: Automatic adjustment for different screen sizes

- **Theme Selection**: Light and dark mode options
- **Accessibility**: High contrast and screen reader support

Viewer User Guide

Overview

As a Viewer, you have read-only access to threat intelligence data within your organization's scope. This role is designed for security analysts, SOC operators, and other team members who need to consume threat intelligence without creating content or managing users.

Core Capabilities

Threat Intelligence Access

- **Real-Time Feeds**: Current threat intelligence from various sources
- **Historical Data**: Access to past threat reports and trends
- **Filtered Views**: Threats relevant to your organization and industry
- **Source Attribution**: Information about threat intelligence providers
- **Confidence Levels**: Reliability ratings for threat data

Dashboard Features

Threat Intelligence Summary:

- Recent threat indicators and warnings
- Critical security alerts for your organization
- Trending threat types and attack vectors
- Geographic threat distribution
- Industry-specific threat focus

Organization Metrics:

- Security posture indicators
- Recent threat intelligence updates
- Alert status summary
- Data freshness indicators
- Trust relationship status

Quick Access Panel:

- Links to recent reports

- Active personal alerts
- Bookmarked content
- Export tools and functions

Viewing Threat Intelligence

Threat Categories:

- **Malware**: Virus signatures, behavioral patterns, family classifications
- **Indicators of Compromise**: IP addresses, domains, file hashes, URLs
- **Attack Patterns**: Tactics, techniques, and procedures (TTPs)
- **Threat Actors**: Known adversary profiles and attribution
- **Vulnerabilities**: CVE information and exploit details
- **Incident Reports**: Security incident summaries and lessons learned

Data Presentation:

- **Tabular Views**: Sortable and filterable data tables
- **Visual Maps**: Geographic and network-based visualizations
- **Timeline Views**: Chronological threat intelligence
- **Relationship Graphs**: Connections between threats and indicators

Search and Filtering

Advanced Search Capabilities:

- **Text Search**: Full-text search across all accessible content
- **Metadata Filtering**: Filter by source, date, threat type, severity
- **Boolean Operators**: Complex search queries with AND, OR, NOT
- **Saved Searches**: Store frequently used search criteria
- **Search History**: Quick access to previous searches

Filter Options:

- **Date Range**: Specific time periods or relative dates
- **Threat Severity**: Critical, high, medium, low classifications
- **Source Type**: Internal, external, commercial, open source
- **Geographic Region**: Location-based threat filtering
- **Industry Sector**: Sector-specific threat intelligence

Reports and Analytics

Available Reports:

- **Threat Summary Reports**: Comprehensive threat landscape overview
- **Industry Reports**: Sector-specific threat analysis
- **Geographic Reports**: Regional threat intelligence
- **Trend Analysis**: Historical threat pattern analysis
- **IOC Reports**: Detailed indicator listings

Analytics Features:

- **Threat Trends**: Visual representation of threat patterns
- **Risk Assessment**: Current risk levels and indicators
- **Performance Metrics**: Platform usage and data quality
- **Comparative Analysis**: Benchmarking against industry standards

Data Export

Export Formats:

- **PDF Reports**: Formatted documents for sharing and archiving
- **CSV Data**: Raw data for spreadsheet analysis
- **JSON Format**: Structured data for technical analysis
- **XML/STIX**: Industry-standard threat intelligence formats

Export Process:

1. Navigate to the data or report you want to export
2. Select the "Export" option
3. Choose your preferred format
4. Configure export parameters (date range, filters)
5. Submit export request
6. Download when processing is complete

Personal Alerts and Notifications

Alert Types:

- **Critical Threats**: High-priority security concerns
- **Organization-Specific**: Threats targeting your organization
- **Industry Alerts**: Sector-relevant security threats
- **Geographic Warnings**: Regional security notifications

- **System Updates**: Platform maintenance and feature updates

Notification Management:

1. Access **Account Settings** → **Notifications**
2. Configure notification preferences:
   - Email notifications
   - In-platform alerts
   - Alert frequency settings
3. Set alert priorities and thresholds
4. Configure quiet hours and exceptions

Best Practices for Viewers

Daily Operations

- **Regular Monitoring**: Check dashboard and alerts daily
- **Threat Review**: Review new threat intelligence relevant to your role
- **Alert Response**: Respond promptly to critical notifications
- **Data Validation**: Verify threat intelligence before acting on it

Security Practices

- **Secure Access**: Always log out when finished
- **Data Handling**: Follow organizational policies for threat intelligence
- **Sharing Guidelines**: Understand what information can be shared externally
- **Incident Reporting**: Report suspicious activity or potential security issues

---

Publisher User Guide

Overview

Publishers serve as organizational trust managers and content creators with significant operational authority within their organization's boundaries. This role is designed for senior security analysts, threat intelligence coordinators, and team leads who need to manage trust relationships and share threat intelligence.

Core Responsibilities

- **Trust Management**: Establish and maintain relationships with other organizations
- **Content Publishing**: Create and share threat intelligence securely
- **User Management**: Manage Viewer accounts within your organization

- **Intelligence Sharing**: Facilitate secure data exchange through trust networks
- **Team Coordination**: Support organizational threat intelligence activities

User Management Capabilities

Creating Viewer Accounts

User Creation Process:

1. Navigate to **User Management** → **Create New User**
2. Complete user information:
   - Personal details (name, contact information)
   - Organizational role and department
   - Initial security settings
   - Access permissions and restrictions
3. Configure notification preferences
4. Send account invitation with temporary credentials
5. Monitor onboarding progress and provide support

User Profile Management:

- **Contact Information**: Maintain current email and phone details
- **Role Assignment**: Assign appropriate access levels
- **Security Settings**: Configure authentication and access controls
- **Activity Monitoring**: Track user engagement and platform usage

Account Administration

Password Management:

- Reset passwords for users experiencing login issues
- Enforce password policy compliance
- Manage temporary password assignments
- Monitor failed login attempts

Account Security:

- Unlock locked user accounts
- Manage two-factor authentication settings
- Configure trusted device settings
- Review user activity logs

Trust Relationship Management

Understanding Trust Relationships

Trust relationships enable secure information sharing between organizations while maintaining security and control. These relationships form the foundation of the collaborative threat intelligence network.

Trust Relationship Types:

Bilateral Trust:

- Two-way information sharing between organizations
- Mutual agreement on sharing policies and data types
- Equal trust levels and reciprocal access
- Balanced information exchange

Unilateral Trust:

- One-way trust where your organization trusts another
- Asymmetric sharing arrangements
- Different trust levels based on relationship needs
- Controlled information flow

Trust Groups:

- Multi-organization trust networks
- Shared policies and collective intelligence
- Group-wide information sharing protocols
- Community-driven threat intelligence

Creating Trust Relationships

Relationship Establishment Process:

1. **Partner Identification**
   - Research potential trust partners
   - Evaluate organizational compatibility
   - Assess shared security interests
   - Review partner reputation and verification status
2. **Relationship Configuration**
   - Navigate to **Trust Management** → **Create Trust Relationship**
   - Select target organization from directory

- Configure trust settings:
  - Trust level (low, medium, high)
  - Sharing policy (full, selective, limited)
  - Data types to be shared
  - Access restrictions and limitations

3. **Request Submission**
   - Provide justification for relationship
   - Specify expected benefits and use cases
   - Set proposed effective dates
   - Submit for partner review and approval
4. **Relationship Activation**
   - Monitor approval status
   - Negotiate terms if needed
   - Finalize relationship configuration
   - Begin collaborative information sharing

API Example for Trust Relationship Creation:

```
json

POST /api/trust/relationships/
{
  "target_organization": 123,
  "trust_level": "medium",
  "sharing_policy": "selective",
  "justification": "Enhanced regional threat intelligence sharing",
  "proposed_data_types": ["threat_indicators", "incident_reports"],
  "effective_date": "2024-01-01"
}
```

Trust Group Participation

Joining Trust Groups:

Trust groups provide access to collective threat intelligence from multiple organizations, enhancing threat detection capabilities and community collaboration.

Group Benefits:

- Access to aggregated threat intelligence
- Broader information sharing networks

- Enhanced threat detection capabilities
- Community-driven security insights
- Industry-specific intelligence sharing

Participation Process:

1. **Group Discovery**: Browse available trust groups by industry, region, or focus area
2. **Application Submission**: Request membership with organizational justification
3. **Requirements Compliance**: Meet group membership criteria and standards
4. **Approval Process**: Group administrators review and approve applications
5. **Active Participation**: Contribute to and benefit from group intelligence

Content Publishing

Threat Intelligence Creation

Content Types:

Threat Indicators:

- IP addresses, domains, URLs associated with threats
- File hashes and malware signatures
- Network indicators and attack patterns
- Behavioral indicators and anomalies

Incident Reports:

- Security incident summaries and analysis
- Attack methodology and timeline documentation
- Impact assessment and lessons learned
- Remediation steps and prevention measures

Alert Bulletins:

- Time-sensitive threat warnings
- Emergency security notifications
- Industry-specific threat alerts
- Geographic threat advisories

Intelligence Analysis:

- Threat actor profiles and attribution
- Campaign analysis and tracking

- Trend analysis and forecasting
- Strategic threat assessments

Publishing Workflow

Content Creation Process:

1. **Content Preparation**
   - Gather and verify threat intelligence data
   - Ensure data accuracy and completeness
   - Apply anonymization and sanitization procedures
   - Review organizational sharing policies
2. **Content Formatting**
   - Structure data according to CRISP standards
   - Add metadata and categorization tags
   - Include source attribution and confidence levels
   - Apply Traffic Light Protocol (TLP) classifications
3. **Sharing Configuration**
   - Select target organizations or trust groups
   - Configure sharing permissions and access levels
   - Set content expiration and update schedules
   - Define usage restrictions and handling requirements
4. **Publication and Distribution**
   - Submit content for internal review (if required)
   - Publish to selected recipients
   - Monitor delivery and access metrics
   - Track content usage and effectiveness

Publishing Tools:

STIX Export Capabilities:

- Export threat intelligence in industry-standard STIX format
- Automated formatting and structure validation
- Integration with external threat intelligence platforms
- Standards-compliant data exchange

Automated Publishing:

- Scheduled content publication workflows
- Rule-based sharing automation
- Integration with internal security tools
- Bulk publishing capabilities for large datasets

Email Alert Management

Alert Campaign Creation

Campaign Types:

- **Critical Threat Alerts**: Immediate security threats requiring urgent attention
- **Intelligence Updates**: New threat intelligence and indicator updates
- **Relationship Notifications**: Trust relationship status changes
- **System Notifications**: Platform updates and maintenance alerts

Campaign Creation Process:

1. **Campaign Setup**
   - Define alert type and priority level
   - Create compelling subject lines and content
   - Configure delivery timing and scheduling
   - Set up tracking and analytics
2. **Recipient Management**
   - Define target audience and recipient lists
   - Segment audiences based on roles and interests
   - Manage recipient preferences and opt-outs
   - Handle distribution list maintenance
3. **Content Development**
   - Use template-based email composition
   - Include rich text formatting and multimedia
   - Add variable insertion and personalization
   - Preview and test before sending
4. **Delivery and Analytics**
   - Schedule immediate or delayed delivery
   - Monitor delivery status and success rates
   - Track open rates and engagement metrics
   - Analyze campaign effectiveness

Email Configuration

SMTP Setup:

- Configure email service providers (Gmail SMTP, SMTP2GO, etc.)
- Set up authentication and security settings
- Configure delivery parameters and rate limits
- Test email connectivity and deliverability

Template Management:

- Create custom email templates for different alert types
- Implement organization branding and styling
- Use variable insertion for dynamic content
- Maintain template versions and updates

Organization Profile Management

Profile Maintenance

Organization Information Updates:

- **Basic Details**: Name, description, contact information
- **Classification**: Industry type, organization size, operational focus
- **Geographic Presence**: Locations, time zones, operational areas
- **Verification Status**: Maintain verification credentials
- **Policies**: Update sharing policies and data handling procedures

Profile Update Process:

1. Navigate to **Organization Settings**
2. Review current profile information
3. Update relevant sections:
    - Contact information and website
    - Organization description and mission
    - Industry classification and focus areas
    - Geographic and operational scope
4. Configure sharing preferences and policies
5. Submit updates for review and approval

Analytics and Reporting

Publisher Analytics

User Management Metrics:

- User creation and management trends
- User activity and engagement patterns
- Training effectiveness and completion rates
- User satisfaction and feedback analysis

Trust Relationship Analytics:

- Relationship health and performance metrics
- Network growth and expansion opportunities
- Information sharing effectiveness
- Partner engagement and collaboration levels

Content Publishing Metrics:

- Publication frequency and volume statistics
- Content quality and relevance scores
- Recipient engagement and feedback
- Intelligence sharing impact assessment

Report Generation

Standard Reports:

- Trust relationship status and health reports
- User activity and engagement summaries
- Content publication and distribution statistics
- Organization performance and metrics analysis

Custom Reporting:

- Build custom reports using drag-and-drop interface
- Select specific metrics and KPIs
- Configure flexible date ranges and filters
- Export in multiple formats (PDF, CSV, Excel)

Admin User Guide

Overview

Admins represent the highest level of organizational authority in CRISP, with comprehensive management capabilities over their organization's entire platform presence. This role encompasses strategic leadership, operational management, security oversight, and community engagement.

Core Administrative Authority

Complete User Management

User Creation Across All Roles:

- **Viewers**: Standard read-only threat intelligence access
- **Publishers**: Content creation and limited user management
- **Admins**: Full organizational administration (peer level)
- **Role Assignment**: Strategic role assignment based on organizational needs

Advanced User Creation Process:

1. **Navigate to User Management → Create New User**
2. **Complete Comprehensive User Profile:**
   - Personal information and contact details
   - Organizational role and department assignment
   - Security clearance and access requirements
   - Initial password and authentication setup
3. **Configure Role and Permissions:**
   - Select appropriate CRISP role
   - Set specific permissions and access levels
   - Configure data classification permissions
   - Establish trust relationship access rights
4. **Security Configuration:**
   - Multi-factor authentication requirements
   - Account security policies and restrictions
   - Session management and timeout settings
   - Trusted device and location configuration
5. **Onboarding and Training:**
   - Assign required training modules
   - Set onboarding milestones and checkpoints
   - Configure mentorship and support

- Establish performance monitoring

User Lifecycle Management:

Advanced User Operations:

- **Role Modifications**: Promote or demote users based on organizational changes
- **Permission Adjustments**: Fine-tune access levels and capabilities
- **Bulk Operations**: Mass user creation, updates, and role changes
- **Account Security**: Manage locks, resets, and security incidents

User Analytics and Monitoring:

- **Performance Metrics**: User activity, engagement, and productivity
- **Behavioral Analysis**: Login patterns, feature usage, collaboration metrics
- **Security Monitoring**: Risk indicators and security behavior analysis
- **Training Effectiveness**: Completion rates and knowledge retention

Full Organization Administration

Organization Profile Management:

Core Configuration:

- **Basic Information**: Name, description, mission, contact details
- **Industry Classification**: Type, size, operational focus
- **Geographic Presence**: Locations, time zones, operational areas
- **Verification Management**: Status, credentials, compliance frameworks
- **Legal and Compliance**: Regulatory requirements and frameworks

Advanced Configuration Example:

```
json
```

```
PUT /api/organizations/current/
{
  "name": "SecureOrg Inc",
  "description": "Leading cybersecurity services provider",
  "industry": "cybersecurity",
  "size": "large",
  "website": "https://secureorg.com",
  "verification_status": "verified",
  "compliance_frameworks": ["ISO27001", "NIST", "SOC2"],
  "sharing_policies": {
    "default_classification": "restricted",
    "auto_sharing_enabled": false,
    "trust_group_participation": true
  }
}
```

Policy Management:

Information Sharing Policies:

- **Classification Standards**: Define organizational data classification
- **Sharing Guidelines**: Rules for information distribution
- **Trust Relationship Policies**: Standards for relationship establishment
- **Content Publishing Rules**: Publication standards and guidelines

Security and Compliance Policies:

- **Access Control Policies**: User access and permission standards
- **Authentication Requirements**: MFA and security standards
- **Audit and Monitoring**: Logging and incident response procedures
- **Data Retention**: Information lifecycle and retention policies

Advanced Trust System Management

Trust Group Creation and Administration:

Trust groups enable multi-organizational collaboration and are a unique capability of Admin-level users.

Trust Group Creation Process:

1. **Navigate to Trust Management → Create Trust Group**
2. **Group Configuration:**
   - Group name, description, and purpose
   - Membership criteria and requirements

- Sharing policies and data classification standards
- Governance structure and decision-making processes

3. **Initial Membership:**
   - Invite founding member organizations
   - Set membership approval processes
   - Define roles and responsibilities
   - Establish communication protocols

4. **Policy Framework:**
   - Information sharing agreements
   - Security requirements and compliance frameworks
   - Dispute resolution procedures
   - Performance metrics and evaluation criteria

Trust Group Management API Example:

```
json

POST /api/trust/groups/
{
  "name": "Regional Financial Services ISAC",
  "description": "Information sharing for regional financial institutions",
  "industry_focus": "financial_services",
  "geographic_scope": "northeast_region",
  "membership_criteria": {
    "industry": "financial_services",
    "verification_required": true,
    "minimum_trust_score": 75
  },
  "sharing_policy": {
    "default_classification": "restricted",
    "member_only_sharing": true,
    "retention_period": "365_days"
  },
  "governance": {
    "voting_threshold": 0.6,
    "leadership_rotation": "annual",
    "dispute_resolution": "mediation"
  }
}
```

Ongoing Group Administration:

Membership Management:

- **Recruitment**: Identify and invite potential members
- **Application Review**: Evaluate applications against criteria
- **Onboarding**: Facilitate new member integration
- **Performance Monitoring**: Track participation and contribution
- **Conflict Resolution**: Mediate disputes and maintain relationships

Group Operations:

- **Policy Development**: Create and update group procedures
- **Communication**: Facilitate group collaboration
- **Event Management**: Organize meetings and training
- **Performance Monitoring**: Track effectiveness and satisfaction
- **Continuous Improvement**: Implement operational improvements

System Health Monitoring

Comprehensive System Oversight

System Health Dashboard (`/api/v1/admin/system-health/`):

Database Health Monitoring:

- **Connection Status**: Monitor database connectivity and performance
- **Query Performance**: Track slow queries and optimization needs
- **Storage Utilization**: Monitor growth and capacity planning
- **Backup Status**: Verify backup completion and integrity
- **Replication Health**: Monitor synchronization and data consistency

Authentication System Health:

- **Login Success Rates**: Track authentication performance
- **Session Management**: Monitor active sessions and cleanup
- **Security Service Status**: Verify MFA and device management
- **Failed Authentication Tracking**: Monitor suspicious activity
- **Token Management**: Monitor JWT performance and validation

Trust System Health:

- **Relationship Status**: Monitor trust relationship availability
- **Service Performance**: Track response times and error rates

- **Group Health**: Monitor activity and member participation
- **Audit Integrity**: Verify logging and data integrity
- **Score Calculations**: Monitor trust score accuracy

Performance Monitoring

Application Performance:

- **API Response Times**: Monitor endpoint performance
- **User Experience Metrics**: Track page loads and interactions
- **Error Rates**: Monitor application errors and exceptions
- **Resource Utilization**: Track CPU, memory, and network usage
- **Scalability Metrics**: Monitor capacity and scaling needs

Data Quality and Integrity:

- **Validation Processes**: Monitor data quality checks
- **Synchronization Status**: Track data sync between systems
- **Backup Verification**: Verify backup integrity and restoration
- **Audit Trail Integrity**: Ensure log completeness and accuracy
- **Compliance Monitoring**: Monitor regulatory compliance

Security and Audit Administration

Security Event Monitoring

Security Events Dashboard (`/api/v1/admin/security-events/`):

Authentication Security:

- **Failed Login Attempts**: Monitor and investigate suspicious activity
- **Account Lockouts**: Track automated and manual lockouts
- **Unusual Access Patterns**: Detect anomalous user behavior
- **MFA Events**: Monitor two-factor authentication usage
- **Session Anomalies**: Detect hijacking and unauthorized access

Data Access Security:

- **Unauthorized Access Attempts**: Monitor restricted data access
- **Data Export Monitoring**: Track exports and potential exfiltration
- **Permission Escalation**: Detect unauthorized privilege attempts
- **Cross-Organizational Access**: Monitor trust relationship usage

- **API Abuse Detection**: Identify unusual usage patterns

Comprehensive Audit Management

Enhanced Audit Logging (`/api/v1/admin/audit-logs/`):

Complete Audit Trail Access:

- **User Activities**: Comprehensive logging of all user actions
- **Administrative Actions**: Detailed logs of admin decisions
- **System Changes**: Complete configuration and policy changes
- **Data Access**: Detailed logging of access and modifications
- **Security Events**: Comprehensive incident and response logging

Advanced Audit Analytics (`/api/v1/admin/comprehensive-audit-logs/`):

```
json

GET /api/v1/admin/comprehensive-audit-logs/?filters={
    "user_id": 123,
    "date_from": "2024-01-01",
    "date_to": "2024-12-31",
    "event_type": "trust_relationship_creation",
    "severity": "high"
}
```

Audit Categories:

- **Authentication Events**: Login patterns, failures, security incidents
- **Authorization Events**: Permission changes, role modifications
- **Data Events**: Information access, modification, deletion, sharing
- **Trust Events**: Relationship creation, modification, termination
- **Administrative Events**: System configuration and user management

Advanced Analytics and Reporting

Strategic Business Intelligence

Organizational Performance Metrics:

- **User Growth and Retention**: Track acquisition and retention rates
- **Trust Network Analysis**: Monitor network expansion and effectiveness
- **Content Impact Measurement**: Assess publishing effectiveness
- **Security Posture Improvements**: Track security enhancements

- **ROI and Value Measurement**: Quantify platform value

Competitive Intelligence:

- **Market Positioning**: Analyze position in threat intelligence community
- **Capability Comparison**: Compare performance against peers
- **Innovation Tracking**: Monitor platform innovation adoption
- **Industry Trends**: Track emerging threat landscape changes
- **Strategic Opportunities**: Identify growth and development opportunities

Custom Reporting and Dashboards

Advanced Report Generation:

- **Drag-and-Drop Builder**: Create custom reports with intuitive interface
- **Multi-Dimensional Analysis**: Analyze across multiple metrics
- **Dynamic Filtering**: Apply complex conditional logic
- **Real-Time Data**: Access live dashboard updates
- **Automated Scheduling**: Schedule report generation and distribution

Executive Reporting:

- **Executive Dashboards**: High-level strategic KPI visualization
- **Board Reports**: Governance reports for board presentation
- **Regulatory Reports**: Compliance reporting for external stakeholders
- **Performance Reviews**: Regular assessment and improvement tracking
- **Strategic Planning**: Data-driven strategic planning insights

---

BlueVision Admin Guide

Overview

BlueVision Admin represents the highest-level administrative role in the CRISP system, with system-wide administrative capabilities across all organizations and users. This role manages the entire platform infrastructure, ensures security and compliance, and oversees global platform operations.

System-Wide Administrative Powers

Comprehensive User Management

Global User Administration:

- **Cross-Organizational Access**: Manage users across all organizations

- **Role Assignment Authority**: Grant any role to any user
- **Account Security Management**: Global account lockout and security controls
- **Session Management**: Monitor and control sessions platform-wide
- **Security Incident Response**: Respond to security events across the platform

User Creation and Management:

```
json

POST /api/v1/admin/users/
{
    "email": "admin@organization.com",
    "first_name": "Jane",
    "last_name": "Admin",
    "role": "admin",
    "organization": "target_organization_id",
    "department": "IT Security",
    "security_clearance": "high",
    "requires_2fa": true,
    "onboarding_required": true
}
```

Account Security Actions:

Account Unlock API (`/api/v1/admin/unlock-account/`):

```
json

POST /api/v1/admin/unlock-account/
{
    "user_id": 123,
    "reason": "Administrative unlock after security review"
}
```

Global Organization Management

Organization Oversight:

- **Creation and Configuration**: Set up new organizations
- **Verification Management**: Control organization verification status
- **Compliance Monitoring**: Ensure platform-wide compliance
- **Resource Allocation**: Manage organizational resources and limits
- **Policy Enforcement**: Implement platform-wide policies

Organization Administration Interface:

- **Complete Organizational Profiles**: Manage all organizational information
- **User Distribution**: Monitor user allocation across organizations
- **Trust Relationship Oversight**: Supervise inter-organizational connections
- **Performance Analytics**: Platform-wide organizational metrics

Trust System Administration

Global Trust Oversight

Trust Relationship Authority:

- **Create Relationships**: Between any organizations (bypasses ownership checks)
- **Approve/Deny Requests**: All trust relationship requests require BlueVision approval
- **Modify Trust Levels**: Adjust sharing permissions and access levels globally
- **Trust Group Oversight**: Create and manage platform-wide trust groups
- **Relationship Auditing**: Monitor all trust activities across the platform

Trust Administration Dashboard (`/api/v1/admin/trust-overview/`):

Key Metrics:

- Total trust relationships across the platform
- Trust relationship effectiveness scores platform-wide
- Pending approval requests from all organizations
- Trust group membership statistics and health
- Cross-organizational collaboration metrics

Trust Management Actions:

Create Trust Relationships:

```
json

POST /api/trust-relationships/
{
    "source_organization": 1,
    "target_organization": 2,
    "trust_level": "high",
    "sharing_policy": "selective",
    "admin_approval": true,
    "bluevision_override": true
}
```

Trust Group Management:

- Create trust groups spanning multiple organizations
- Manage group memberships and permissions globally
- Set platform-wide sharing policies
- Monitor group activity and effectiveness across all groups
- Resolve trust disputes and conflicts

Trust Audit and Monitoring

Global Trust Metrics:

- **Platform-Wide Usage**: Monitor trust relationship utilization
- **Effectiveness Analysis**: Measure trust relationship value
- **Security Monitoring**: Detect trust-related security events
- **Compliance Reporting**: Generate platform compliance reports
- **Performance Optimization**: Identify improvement opportunities

Security and Audit Management

Platform-Wide Security Monitoring

Security Events Dashboard (`/api/v1/admin/security-events/`):

Global Security Monitoring:

- **Failed Login Attempts**: Track suspicious activity across all organizations
- **Account Lockouts**: Monitor security lockouts platform-wide
- **Unusual Access Patterns**: Detect anomalous behavior across users
- **Trust Violations**: Monitor unauthorized access attempts globally
- **Data Breach Detection**: Identify potential security incidents

Authentication Security Management:

- **Multi-Factor Authentication**: Monitor MFA usage and enforcement
- **Session Security**: Track session anomalies and hijacking attempts
- **Device Management**: Monitor trusted device registrations globally
- **Password Security**: Enforce password policies and monitor breaches

Comprehensive Audit Management

System-Wide Audit Trail (`/api/v1/admin/audit-logs/`):

Complete Platform Audit:

- **User Authentication**: All login and authentication events
- **Authorization Events**: Permission changes and role modifications
- **Data Access**: Information access and modification across organizations
- **Trust Events**: All trust relationship activities
- **Administrative Actions**: System configuration and management changes

Enhanced Audit Features (`/api/v1/admin/comprehensive-audit-logs/`):

Advanced Filtering Example:

```
json

GET /api/v1/admin/comprehensive-audit-logs/?user=123&date_from=2024-01-01&event_type=trust_creation&organ
```

Audit Categories:

- **Authentication Events**: Logins, logouts, failed attempts globally
- **Authorization Events**: Permission changes across all organizations
- **Data Events**: Information access, modifications, deletions platform-wide
- **Trust Events**: Relationship creation, modification, termination
- **Administrative Events**: System configuration and user management

System Health Monitoring

Real-Time Platform Health

System Health Dashboard (`/api/v1/admin/system-health/`):

Database Health:

- **Connection Status**: Database connectivity and performance monitoring
- **Query Performance**: Slow query detection and optimization
- **Storage Utilization**: Database size and growth trend analysis
- **Backup Status**: Backup completion and integrity verification
- **Replication Health**: Data synchronization monitoring

Authentication System Health:

- **Login Success Rates**: Authentication system performance tracking
- **Session Management**: Active session counts and cleanup processes

- **Security Service Status**: 2FA, device management, password services
- **Failed Authentication Tracking**: Suspicious activity detection
- **Token Management**: JWT token generation and validation monitoring

Trust System Health:

- **Trust Relationship Status**: Active and inactive relationships
- **Trust Service Performance**: Response times and error rates
- **Trust Group Health**: Group membership and activity status
- **Trust Audit System**: Audit logging performance and integrity
- **Trust Score Calculations**: Trust score computation monitoring

Performance Monitoring:

- **API Response Times**: Monitor endpoint performance platform-wide
- **User Activity Levels**: Track platform usage patterns
- **Resource Utilization**: Server performance and capacity monitoring
- **Error Rates**: Application error monitoring and alerting
- **Scalability Metrics**: Platform scaling and capacity planning

Platform Configuration and Management

System Configuration

Global Settings Management:

- **Platform Policies**: Configure platform-wide policies and standards
- **Security Settings**: Implement global security configurations
- **Integration Management**: Manage third-party integrations
- **Feature Flags**: Enable/disable features across organizations
- **Resource Limits**: Set organizational resource quotas and limits

Maintenance and Updates:

- **Scheduled Maintenance**: Plan and coordinate maintenance windows
- **Update Management**: Deploy platform updates and security patches
- **Capacity Planning**: Monitor growth and plan infrastructure scaling
- **Performance Tuning**: Optimize platform performance and responsiveness
- **Disaster Recovery**: Maintain and test disaster recovery procedures

Emergency Response Procedures

Security Incident Response

Critical Issue Escalation:

Security Incident Response Process:

1. **Immediate Assessment**: Quickly assess incident severity and impact
2. **Containment**: Implement immediate containment measures
3. **Investigation**: Conduct thorough incident investigation
4. **Communication**: Notify affected organizations and stakeholders
5. **Recovery**: Implement recovery procedures and service restoration
6. **Post-Incident Review**: Analyze incident and implement improvements

System Outage Response:

1. **Impact Assessment**: Assess outage scope and business impact
2. **Communication**: Notify all users and stakeholders
3. **Resolution**: Coordinate with technical teams on resolution
4. **Monitoring**: Monitor restoration progress and system stability
5. **Documentation**: Document outage cause and resolution steps
6. **Prevention**: Implement measures to prevent future occurrences

---

Trust Relationship Management

Understanding Trust Relationships

Trust relationships form the foundation of secure information sharing in CRISP, enabling organizations to collaborate on threat intelligence while maintaining security and control over sensitive information.

Trust Relationship Framework

Relationship Types

Bilateral Trust Relationships:

- **Mutual Information Sharing**: Two-way exchange of threat intelligence
- **Equal Partnership**: Balanced sharing arrangements between organizations
- **Reciprocal Access**: Both organizations have equal access to shared data
- **Symmetric Trust Levels**: Similar trust levels and sharing policies

Unilateral Trust Relationships:

- **One-Way Information Flow**: Single direction information sharing

- **Asymmetric Arrangements**: Different levels of access and sharing
- **Source Protection**: Protecting sensitive source information
- **Controlled Distribution**: Limited and controlled information flow

Trust Groups:

- **Multi-Organization Networks**: Collaborative sharing among multiple organizations
- **Collective Intelligence**: Aggregated threat intelligence from all members
- **Shared Standards**: Common policies and procedures across the group
- **Community Governance**: Democratic decision-making and group management

Trust Levels

High Trust Level:

- **Full Information Sharing**: Complete access to threat intelligence
- **Real-Time Sharing**: Immediate sharing of critical threats
- **Bidirectional Flow**: Full two-way information exchange
- **Minimal Restrictions**: Limited sharing restrictions and constraints

Medium Trust Level:

- **Selective Sharing**: Curated information sharing based on relevance
- **Delayed Sharing**: Information shared after initial internal analysis
- **Partial Access**: Limited access to specific types of information
- **Moderate Restrictions**: Some limitations on information usage

Low Trust Level:

- **Limited Information Sharing**: Minimal sharing of basic threat indicators
- **Public Information Only**: Sharing of non-sensitive, public information
- **One-Way Flow**: Primarily receiving rather than sharing information
- **Strict Restrictions**: Significant limitations on information access and use

Trust Relationship Lifecycle

Establishment Phase

Partner Discovery and Evaluation:

1. **Research Potential Partners**: Identify organizations with compatible interests
2. **Due Diligence**: Verify organization legitimacy and security posture
3. **Compatibility Assessment**: Evaluate shared security interests and goals

4. **Risk Analysis**: Assess potential risks and benefits of partnership

Relationship Negotiation:

1. **Initial Contact**: Establish communication with potential partner
2. **Scope Definition**: Define the scope and objectives of the relationship
3. **Policy Alignment**: Ensure compatible sharing policies and procedures
4. **Agreement Terms**: Negotiate specific terms and conditions

Technical Configuration:

1. **Access Setup**: Configure technical access and authentication
2. **Data Classification**: Establish data classification and handling procedures
3. **Sharing Protocols**: Implement sharing protocols and procedures
4. **Testing**: Test information sharing capabilities and procedures

Operational Phase

Ongoing Management:

- **Regular Communication**: Maintain regular contact with trust partners
- **Performance Monitoring**: Track relationship effectiveness and value
- **Policy Compliance**: Ensure adherence to agreed-upon policies
- **Issue Resolution**: Address conflicts and problems promptly

Relationship Optimization:

- **Feedback Collection**: Gather feedback from both organizations
- **Performance Analysis**: Analyze sharing effectiveness and impact
- **Adjustment Implementation**: Make necessary adjustments to improve value
- **Expansion Opportunities**: Identify opportunities to expand cooperation

Review and Renewal

Periodic Review Process:

1. **Performance Evaluation**: Assess relationship effectiveness and value
2. **Policy Review**: Review and update sharing policies as needed
3. **Risk Assessment**: Re-evaluate risks and security considerations
4. **Stakeholder Feedback**: Collect feedback from internal stakeholders

Renewal or Termination:

1. **Renewal Decision**: Decide whether to continue the relationship
2. **Term Renegotiation**: Update terms and conditions as needed
3. **Termination Process**: If needed, properly terminate the relationship
4. **Transition Planning**: Plan for data handling and access changes

Trust Group Management

Trust Group Structure

Group Governance:

- **Leadership Structure**: Defined roles and responsibilities for group leaders
- **Decision-Making Process**: Democratic or consensus-based decision making
- **Policy Development**: Collaborative development of group policies
- **Conflict Resolution**: Procedures for resolving disputes and conflicts

Membership Management:

- **Membership Criteria**: Clear requirements for group membership
- **Application Process**: Structured process for evaluating new members
- **Onboarding Procedures**: Comprehensive onboarding for new members
- **Member Responsibilities**: Clear expectations for member participation

Group Operations

Information Sharing:

- **Shared Intelligence Pool**: Centralized repository of group intelligence
- **Contribution Requirements**: Expectations for member contributions
- **Access Controls**: Role-based access to group information
- **Quality Standards**: Standards for information quality and reliability

Communication and Collaboration:

- **Regular Meetings**: Scheduled meetings for group coordination
- **Communication Channels**: Secure communication platforms and procedures
- **Working Groups**: Specialized groups for specific topics or projects
- **Knowledge Sharing**: Formal and informal knowledge sharing activities

Trust Metrics and Analytics

Relationship Performance Metrics

Quantitative Metrics:

- **Sharing Volume**: Amount of information shared between partners
- **Sharing Frequency**: Frequency of information sharing activities
- **Response Time**: Time to share critical threat information
- **Access Patterns**: Patterns of information access and usage

Qualitative Metrics:

- **Information Quality**: Relevance and accuracy of shared information
- **Relationship Health**: Overall health and satisfaction with the relationship
- **Mutual Benefit**: Perceived value and benefit by both parties
- **Trust Level**: Level of trust and confidence in the partnership

Trust Network Analysis

Network Visualization:

- **Relationship Mapping**: Visual representation of trust relationships
- **Network Topology**: Analysis of network structure and connections
- **Influence Analysis**: Identification of influential nodes and connections
- **Growth Patterns**: Analysis of network growth and expansion

Network Health Assessment:

- **Connectivity Metrics**: Measures of network connectivity and reach
- **Redundancy Analysis**: Assessment of network resilience and redundancy
- **Vulnerability Assessment**: Identification of potential vulnerabilities
- **Optimization Opportunities**: Identification of network improvement opportunities

---

Content Publishing & Sharing

Content Creation Framework

Threat Intelligence Content Types

Indicators of Compromise (IoCs):

- **Network Indicators**: IP addresses, domains, URLs, network signatures
- **File Indicators**: File hashes, malware signatures, behavioral patterns
- **System Indicators**: Registry keys, file paths, process names
- **Email Indicators**: Sender addresses, subject patterns, attachment hashes

Threat Reports:

- **Incident Analysis**: Detailed analysis of security incidents
- **Threat Actor Profiles**: Information about specific threat actors
- **Campaign Analysis**: Analysis of attack campaigns and operations
- **Technical Analysis**: Deep technical analysis of threats and vulnerabilities

Alerts and Bulletins:

- **Critical Alerts**: Time-sensitive warnings about immediate threats
- **Industry Bulletins**: Sector-specific threat information
- **Geographic Alerts**: Location-based threat warnings
- **Tactical Alerts**: Specific recommendations for defensive actions

Strategic Intelligence:

- **Trend Analysis**: Long-term threat trends and patterns
- **Risk Assessments**: Comprehensive risk analysis and assessment
- **Threat Landscape Reports**: Overview of current threat environment
- **Predictive Intelligence**: Forward-looking threat predictions

Content Standards and Quality

Data Quality Requirements:

- **Accuracy**: Verification of information accuracy and reliability
- **Completeness**: Comprehensive information with sufficient detail
- **Timeliness**: Current and relevant information
- **Source Attribution**: Clear attribution and source information

Content Structure Standards:

- **STIX Compliance**: Adherence to STIX format standards
- **Metadata Requirements**: Complete and accurate metadata
- **Classification Standards**: Proper classification and handling markings
- **Format Consistency**: Consistent formatting and presentation

Content Publishing Process

Pre-Publication Phase

Content Development:

1. **Information Gathering**: Collect relevant threat intelligence data
2. **Analysis and Verification**: Analyze and verify information accuracy
3. **Content Creation**: Develop structured content following standards
4. **Internal Review**: Conduct internal review and quality assurance

Content Preparation:

1. **Format Validation**: Ensure compliance with format standards
2. **Classification Assignment**: Apply appropriate classification levels
3. **Metadata Addition**: Add comprehensive metadata and tags
4. **Quality Check**: Final quality assurance before publication

Publication Configuration

Audience Selection:

- **Target Organizations**: Select specific recipient organizations
- **Trust Groups**: Publish to trust groups and communities
- **Public Distribution**: Make available to public threat intelligence feeds
- **Custom Distribution**: Create custom distribution lists

Sharing Permissions:

- **Access Levels**: Define who can access the content
- **Usage Restrictions**: Specify how content can be used
- **Redistribution Rights**: Control further distribution of content
- **Expiration Settings**: Set content expiration and refresh schedules

Publication Settings:

```
json
```

```
POST /api/content/publish/
{
  "title": "Critical Malware Campaign Alert",
  "content_type": "alert",
  "classification": "TLP:AMBER",
  "target_audiences": ["trust_group_123", "organization_456"],
  "sharing_policy": {
    "redistribution": "restricted",
    "modification": "prohibited",
    "attribution": "required"
  },
  "expiration_date": "2024-12-31",
  "auto_update": true
}
```

Post-Publication Management

Distribution Monitoring:

- **Delivery Tracking**: Monitor content delivery to recipients
- **Access Analytics**: Track who accesses the content and when
- **Usage Patterns**: Analyze how content is being used
- **Feedback Collection**: Gather feedback from recipients

Content Maintenance:

- **Updates and Revisions**: Publish updates and corrections
- **Version Control**: Maintain version history and changes
- **Lifecycle Management**: Manage content through its lifecycle
- **Archive Management**: Archive outdated or expired content

STIX Integration and Export

STIX Format Support

STIX Objects:

- **Indicators**: Threat indicators in STIX format
- **Malware**: Malware analysis and characteristics
- **Attack Patterns**: Tactics, techniques, and procedures
- **Threat Actors**: Adversary profiles and attribution
- **Campaigns**: Attack campaign information
- **Intrusion Sets**: Collections of related activities

STIX Relationships:

- **Indicator-to-Malware**: Link indicators to specific malware
- **Actor-to-Campaign**: Connect threat actors to campaigns
- **Pattern-to-Technique**: Map attack patterns to techniques
- **Campaign-to-Infrastructure**: Link campaigns to infrastructure

Export Capabilities

STIX Export Process:

1. **Content Selection**: Select content for export
2. **Format Conversion**: Convert to STIX format
3. **Validation**: Validate STIX format compliance
4. **Export Generation**: Generate export package
5. **Download and Distribution**: Provide secure download

Export Configuration:

```
json

POST /api/content/export/stix/
{
    "content_ids": [123, 456, 789],
    "stix_version": "2.1",
    "include_relationships": true,
    "include_metadata": true,
    "export_format": "json",
    "compression": "zip"
}
```

Content Collaboration

Collaborative Content Development

Multi-Author Content:

- **Collaborative Editing**: Multiple authors working on single content
- **Version Control**: Track changes and author contributions
- **Review Workflows**: Structured review and approval processes
- **Comment and Feedback**: In-line comments and feedback system

Cross-Organizational Collaboration:

- **Joint Analysis**: Collaborative analysis across organizations
- **Shared Workspaces**: Secure collaborative workspaces
- **Information Fusion**: Combining intelligence from multiple sources
- **Collective Assessment**: Group consensus on threat assessments

Content Validation and Peer Review

Peer Review Process:

1. **Reviewer Assignment**: Assign qualified reviewers
2. **Review Criteria**: Establish clear review criteria and standards
3. **Review Execution**: Conduct thorough content review
4. **Feedback Integration**: Incorporate reviewer feedback
5. **Final Approval**: Final approval and publication authorization

Quality Assurance:

- **Technical Accuracy**: Verify technical accuracy of content
- **Source Validation**: Validate source information and attribution
- **Compliance Check**: Ensure compliance with policies and standards
- **Format Verification**: Verify format and structure compliance

---

Security & Compliance

Security Framework

Access Control and Authentication

Authentication Mechanisms:

- **Multi-Factor Authentication (MFA)**: Required for all sensitive operations
- **Single Sign-On (SSO)**: Integration with organizational identity systems
- **Certificate-Based Authentication**: PKI-based authentication for high security
- **Biometric Authentication**: Advanced biometric options where available

Access Control Models:

- **Role-Based Access Control (RBAC)**: Access based on organizational roles
- **Attribute-Based Access Control (ABAC)**: Fine-grained access based on attributes
- **Mandatory Access Control (MAC)**: Strict access control for classified information
- **Discretionary Access Control (DAC)**: User-controlled access permissions

Data Security and Encryption

Encryption Standards:

- **Data at Rest**: AES-256 encryption for stored data
- **Data in Transit**: TLS 1.3 for all network communications
- **Key Management**: Hardware security modules for key storage
- **End-to-End Encryption**: Optional end-to-end encryption for sensitive data

Data Classification:

- **Traffic Light Protocol (TLP)**: Industry-standard classification system
- **Organizational Classifications**: Custom classification schemes
- **Handling Requirements**: Specific handling requirements for each classification
- **Access Restrictions**: Access controls based on classification levels

Compliance Management

Regulatory Compliance

Compliance Frameworks:

- **NIST Cybersecurity Framework**: Alignment with NIST standards
- **ISO 27001**: Information security management compliance
- **SOC 2**: Service organization control compliance
- **GDPR**: General Data Protection Regulation compliance
- **Industry-Specific**: Sector-specific regulatory requirements

Compliance Monitoring:

- **Automated Compliance Checks**: Continuous compliance monitoring
- **Policy Enforcement**: Automated policy enforcement mechanisms
- **Compliance Reporting**: Regular compliance status reporting
- **Gap Analysis**: Identification and remediation of compliance gaps

Audit and Logging

Comprehensive Audit Trails:

- **User Activities**: Complete logging of all user actions
- **System Events**: Comprehensive system event logging
- **Security Events**: Detailed security incident logging

- **Data Access**: Complete data access and modification logging
- **Administrative Actions**: Full administrative action logging

Audit Log Management:

- **Log Retention**: Configurable log retention policies
- **Log Integrity**: Cryptographic protection of audit logs
- **Log Analysis**: Automated log analysis and alerting
- **Log Export**: Secure export capabilities for external analysis

Audit API Example:

```
json

GET /api/v1/admin/comprehensive-audit-logs/
{
  "filters": {
    "date_range": "last_30_days",
    "event_types": ["data_access", "user_management"],
    "severity": "high",
    "user_roles": ["admin", "publisher"]
  },
  "format": "json",
  "include_metadata": true
}
```

Privacy Protection

Data Privacy Framework

Privacy Principles:

- **Data Minimization**: Collect only necessary information
- **Purpose Limitation**: Use data only for specified purposes
- **Accuracy**: Maintain accurate and up-to-date information
- **Storage Limitation**: Retain data only as long as necessary
- **Integrity and Confidentiality**: Protect data from unauthorized access

Privacy Controls:

- **Consent Management**: User consent tracking and management
- **Data Subject Rights**: Support for data subject access requests
- **Data Anonymization**: Automatic anonymization of personal data
- **Privacy Impact Assessments**: Regular privacy impact assessments

Cross-Border Data Transfer

International Data Transfer:

- **Adequacy Decisions**: Compliance with adequacy decisions
- **Standard Contractual Clauses**: Use of approved transfer mechanisms
- **Binding Corporate Rules**: Internal data transfer policies
- **Local Data Residency**: Options for local data storage

Transfer Safeguards:

- **Encryption**: Mandatory encryption for international transfers
- **Access Controls**: Strict access controls for transferred data
- **Audit Trails**: Complete logging of international data transfers
- **Legal Compliance**: Compliance with applicable transfer laws

Security Incident Management

Incident Response Framework

Incident Classification:

- **Security Incidents**: Unauthorized access, data breaches, system compromises
- **Privacy Incidents**: Unauthorized disclosure of personal information
- **Operational Incidents**: System outages, performance degradation
- **Compliance Incidents**: Violations of regulatory requirements

Incident Response Process:

1. **Detection and Identification**: Rapid incident detection and classification
2. **Containment**: Immediate containment to prevent further damage
3. **Investigation**: Thorough investigation to determine scope and impact
4. **Eradication**: Removal of threats and vulnerabilities
5. **Recovery**: Restoration of normal operations
6. **Lessons Learned**: Post-incident analysis and improvement

Incident Communication

Internal Communication:

- **Incident Team**: Immediate notification of incident response team
- **Management**: Executive briefings on significant incidents

- **Users**: User communication for incidents affecting operations
- **Legal**: Legal team notification for regulatory implications

External Communication:

- **Regulatory Notifications**: Required notifications to regulatory authorities
- **Customer Notifications**: Customer communication for data breaches
- **Partner Notifications**: Notification of trusted partners when relevant
- **Public Disclosure**: Public disclosure when required by law

Risk Management

Risk Assessment Framework

Risk Identification:

- **Threat Modeling**: Systematic identification of potential threats
- **Vulnerability Assessment**: Regular vulnerability scanning and assessment
- **Risk Registers**: Comprehensive risk registers and tracking
- **Impact Analysis**: Assessment of potential impact and consequences

Risk Analysis:

- **Probability Assessment**: Evaluation of threat likelihood
- **Impact Assessment**: Analysis of potential business impact
- **Risk Scoring**: Quantitative risk scoring and prioritization
- **Risk Mapping**: Visual representation of risk landscape

Risk Mitigation

Risk Treatment Options:

- **Risk Avoidance**: Elimination of risky activities or processes
- **Risk Mitigation**: Implementation of controls to reduce risk
- **Risk Transfer**: Transfer of risk through insurance or contracts
- **Risk Acceptance**: Formal acceptance of residual risk

Control Implementation:

- **Technical Controls**: Automated security controls and protections
- **Administrative Controls**: Policies, procedures, and training
- **Physical Controls**: Physical security measures and protections
- **Compensating Controls**: Alternative controls when primary controls are not feasible

Analytics & Reporting

Analytics Framework

Performance Analytics

User Analytics:

- **User Engagement**: Activity levels, session duration, feature usage
- **User Productivity**: Content creation, sharing, collaboration metrics
- **User Satisfaction**: Feedback scores, support tickets, user surveys
- **User Growth**: Registration trends, retention rates, churn analysis

Content Analytics:

- **Content Performance**: View counts, sharing rates, engagement metrics
- **Content Quality**: Accuracy ratings, feedback scores, peer reviews
- **Content Impact**: Threat prevention, incident response improvements
- **Content Lifecycle**: Creation, publication, usage, expiration patterns

Trust Relationship Analytics:

- **Relationship Health**: Trust scores, activity levels, mutual satisfaction
- **Network Analysis**: Connectivity patterns, influence measures, network growth
- **Sharing Effectiveness**: Information flow, utilization rates, response times
- **Collaboration Impact**: Joint activities, shared outcomes, mutual benefits

Security Analytics

Threat Intelligence Analytics:

- **Threat Trends**: Emerging threats, attack patterns, threat evolution
- **Geographic Analysis**: Regional threat patterns, attack origins
- **Industry Analysis**: Sector-specific threats, industry targeting patterns
- **Temporal Analysis**: Time-based threat patterns, seasonal variations

Security Posture Analytics:

- **Risk Metrics**: Overall risk levels, risk trends, risk mitigation effectiveness
- **Incident Metrics**: Incident frequency, response times, resolution rates
- **Vulnerability Metrics**: Vulnerability discovery, patching rates, exposure levels

- **Compliance Metrics**: Compliance status, audit results, regulatory adherence

Reporting Capabilities

Standard Reports

Executive Reports:

- **Executive Dashboard**: High-level KPIs and strategic metrics
- **Performance Summary**: Organizational performance overview
- **Risk Assessment**: Current risk status and mitigation progress
- **Compliance Status**: Regulatory compliance and audit results

Operational Reports:

- **User Activity Reports**: Detailed user activity and productivity metrics
- **Content Reports**: Content creation, publication, and usage statistics
- **Trust Relationship Reports**: Relationship status and performance metrics
- **Security Reports**: Security events, incidents, and response metrics

Technical Reports:

- **System Performance**: Platform performance and availability metrics
- **Integration Status**: Third-party integration health and performance
- **API Usage**: API utilization patterns and performance metrics
- **Data Quality**: Data accuracy, completeness, and consistency metrics

Custom Reporting

Report Builder Features:

- **Drag-and-Drop Interface**: Intuitive report creation interface
- **Custom Metrics**: Define custom KPIs and metrics
- **Advanced Filtering**: Complex filtering and segmentation options
- **Visualization Options**: Charts, graphs, tables, and dashboards

Report Configuration:

```
json
```

```
POST /api/reports/custom/
{
  "report_name": "Monthly Trust Relationship Performance",
  "data_sources": ["trust_relationships", "sharing_metrics"],
  "filters": {
    "date_range": "last_30_days",
    "organization": "current",
    "trust_level": ["medium", "high"]
  },
  "metrics": [
    "relationship_count",
    "sharing_volume",
    "response_time",
    "satisfaction_score"
  ],
  "visualizations": [
    {"type": "line_chart", "metric": "sharing_volume"},
    {"type": "bar_chart", "metric": "satisfaction_score"}
  ],
  "schedule": {
    "frequency": "monthly",
    "day": 1,
    "recipients": ["admin@org.com"]
  }
}
```

Automated Reporting

Scheduled Reports:

- **Daily Reports**: Critical metrics and alerts
- **Weekly Reports**: Operational performance and trends
- **Monthly Reports**: Strategic metrics and analysis
- **Quarterly Reports**: Executive summaries and strategic planning

Alert-Based Reports:

- **Threshold Alerts**: Automatic reports when metrics exceed thresholds
- **Anomaly Detection**: Reports triggered by unusual patterns
- **Incident Reports**: Automatic generation of incident summary reports
- **Compliance Reports**: Triggered reports for compliance violations

Data Visualization

Dashboard Design

Dashboard Types:

- **Executive Dashboards**: High-level strategic view for leadership
- **Operational Dashboards**: Day-to-day operational metrics and KPIs
- **Technical Dashboards**: Detailed technical metrics and system health
- **Analytical Dashboards**: In-depth analysis and research tools

Visualization Components:

- **Key Performance Indicators (KPIs)**: Critical metrics at a glance
- **Trend Charts**: Time-series data showing trends and patterns
- **Comparison Charts**: Side-by-side comparisons of metrics
- **Geographic Maps**: Location-based data visualization
- **Network Diagrams**: Relationship and network visualizations

Interactive Analytics

Self-Service Analytics:

- **Ad-Hoc Queries**: User-defined queries and analysis
- **Data Exploration**: Interactive data exploration tools
- **Drill-Down Capabilities**: Deep dive into specific data points
- **Real-Time Analysis**: Live data analysis and visualization

Collaborative Analytics:

- **Shared Dashboards**: Team-accessible dashboard sharing
- **Annotation Tools**: Comments and notes on charts and data
- **Export and Sharing**: Easy export and sharing of analysis results
- **Version Control**: Track changes and versions of analysis

---

API Reference

API Overview

The CRISP platform provides a comprehensive RESTful API that enables programmatic access to all platform functionality. The API is designed with security, scalability, and ease of use in mind.

API Architecture

RESTful Design:

- **Resource-Based URLs**: Intuitive resource-based endpoint structure
- **HTTP Methods**: Standard HTTP methods (GET, POST, PUT, DELETE, PATCH)
- **Status Codes**: Meaningful HTTP status codes for all responses
- **JSON Format**: Consistent JSON request and response format

API Versioning:

- **Version Control**: API versioning through URL path (e.g., `/api/v1/`)
- **Backward Compatibility**: Maintained backward compatibility across versions
- **Deprecation Policy**: Clear deprecation timeline and migration support
- **Version Documentation**: Comprehensive documentation for each API version

Authentication and Authorization

API Authentication

JWT Token Authentication:

```http
Authorization: Bearer <jwt-token>
Content-Type: application/json
```

Authentication Flow:

1. **Login Request**: Submit credentials to obtain JWT token
2. **Token Usage**: Include token in Authorization header for all requests
3. **Token Refresh**: Refresh tokens before expiration
4. **Token Revocation**: Revoke tokens when no longer needed

Authentication Endpoints:

```http
POST /api/v1/auth/login/
POST /api/v1/auth/refresh/
POST /api/v1/auth/logout/
```

Authorization Model

Role-Based Permissions:

- **Viewer**: Read-only access to threat intelligence
- **Publisher**: Content creation and user management

- **Admin**: Full organizational administration
- **BlueVisionAdmin**: Platform-wide administration

Permission Validation:

- **Endpoint-Level**: Permissions checked at endpoint level
- **Resource-Level**: Permissions validated for specific resources
- **Organization-Scoped**: Access limited to organizational boundaries
- **Trust-Based**: Access extended through trust relationships

Core API Endpoints

User Management APIs

User CRUD Operations:

```
http

GET    /api/v1/users/              # List users
POST   /api/v1/users/              # Create user
GET    /api/v1/users/{id}/         # Get user details
PUT    /api/v1/users/{id}/         # Update user
DELETE /api/v1/users/{id}/         # Delete user
PATCH  /api/v1/users/{id}/         # Partial update
```

User Management:

```
http

POST   /api/v1/users/{id}/unlock/       # Unlock user account
POST   /api/v1/users/{id}/reset-password/ # Reset password
GET    /api/v1/users/{id}/activity/     # User activity logs
```

Example User Creation:

```
json
```

```
POST /api/v1/users/
{
  "email": "user@organization.com",
  "first_name": "John",
  "last_name": "Doe",
  "role": "viewer",
  "organization": "org_123",
  "department": "Security Operations",
  "security_clearance": "medium",
  "requires_2fa": true
}
```

Trust Relationship APIs

Trust Relationship Management:

```
http

GET    /api/v1/trust/relationships/      # List relationships
POST   /api/v1/trust/relationships/      # Create relationship
GET    /api/v1/trust/relationships/{id}/ # Get relationship details
PUT    /api/v1/trust/relationships/{id}/ # Update relationship
DELETE /api/v1/trust/relationships/{id}/ # Delete relationship
```

Trust Groups:

```
http

GET    /api/v1/trust/groups/            # List trust groups
POST   /api/v1/trust/groups/            # Create trust group
GET    /api/v1/trust/groups/{id}/       # Get group details
PUT    /api/v1/trust/groups/{id}/       # Update group
DELETE /api/v1/trust/groups/{id}/       # Delete group
POST   /api/v1/trust/groups/{id}/join/  # Join group
POST   /api/v1/trust/groups/{id}/leave/ # Leave group
```

Trust Metrics:

```
http

GET    /api/v1/trust/metrics/           # Trust analytics
GET    /api/v1/trust/health/            # Trust system health
GET    /api/v1/trust/network/           # Trust network analysis
```

Content Management APIs

Content Publishing:

```http
GET    /api/v1/content/                # List content
POST   /api/v1/content/                # Create content
GET    /api/v1/content/{id}/           # Get content details
PUT    /api/v1/content/{id}/           # Update content
DELETE /api/v1/content/{id}/           # Delete content
POST   /api/v1/content/{id}/publish/   # Publish content
POST   /api/v1/content/{id}/unpublish/ # Unpublish content
```

Content Export:

```http
POST   /api/v1/content/export/stix/    # Export as STIX
POST   /api/v1/content/export/csv/     # Export as CSV
POST   /api/v1/content/export/pdf/     # Export as PDF
GET    /api/v1/content/export/{job_id}/ # Check export status
```

Example Content Creation:

```json
POST /api/v1/content/
{
  "title": "Critical Malware Campaign Alert",
  "content_type": "alert",
  "classification": "TLP:AMBER",
  "description": "New malware campaign targeting financial institutions",
  "indicators": [
    {
      "type": "domain",
      "value": "malicious-domain.com",
      "confidence": "high"
    }
  ],
  "sharing_policy": {
    "trust_groups": ["financial_services_isac"],
    "organizations": ["org_456"],
    "public": false
  }
}
```

Organization Management APIs

Organization Operations:

```http
GET    /api/v1/organizations/           # List organizations
POST   /api/v1/organizations/           # Create organization
GET    /api/v1/organizations/{id}/      # Get organization details
PUT    /api/v1/organizations/{id}/      # Update organization
GET    /api/v1/organizations/current/   # Get current organization
PUT    /api/v1/organizations/current/   # Update current organization
```

Organization Analytics:

```http
GET    /api/v1/organizations/{id}/analytics/     # Organization metrics
GET    /api/v1/organizations/{id}/users/         # Organization users
GET    /api/v1/organizations/{id}/content/       # Organization content
GET    /api/v1/organizations/{id}/relationships/ # Organization relationships
```

Analytics and Reporting APIs

Analytics Endpoints:

```http
GET    /api/v1/analytics/dashboard/     # Dashboard metrics
GET    /api/v1/analytics/users/         # User analytics
GET    /api/v1/analytics/content/       # Content analytics
GET    /api/v1/analytics/trust/         # Trust analytics
GET    /api/v1/analytics/security/      # Security analytics
```

Reporting:

```http
GET    /api/v1/reports/                 # List available reports
POST   /api/v1/reports/                 # Create custom report
GET    /api/v1/reports/{id}/            # Get report details
POST   /api/v1/reports/{id}/generate/   # Generate report
GET    /api/v1/reports/{id}/download/   # Download report
```

Example Analytics Query:

```json
```

```
GET /api/v1/analytics/dashboard/?filters={
    "date_range": "last_30_days",
    "metrics": ["user_activity", "content_creation", "trust_health"],
    "organization": "current"
}
```

Admin-Specific APIs

System Administration

System Health:

```
http

GET    /api/v1/admin/system-health/      # System health status
GET    /api/v1/admin/dashboard/          # Admin dashboard
GET    /api/v1/admin/performance/        # Performance metrics
```

Audit and Logging:

```
http

GET    /api/v1/admin/audit-logs/         # Basic audit logs
GET    /api/v1/admin/comprehensive-audit-logs/  # Enhanced audit logs
GET    /api/v1/admin/security-events/    # Security events
POST   /api/v1/admin/audit/export/       # Export audit logs
```

User Administration:

```
http

GET    /api/v1/admin/users/              # List all users
POST   /api/v1/admin/users/              # Create user (any role)
POST   /api/v1/admin/unlock-account/     # Unlock user account
POST   /api/v1/admin/bulk-operations/    # Bulk user operations
```

BlueVision Admin APIs

Platform Management:

```
http

GET    /api/v1/bluevision/organizations/ # All organizations
GET    /api/v1/bluevision/users/         # All users platform-wide
GET    /api/v1/bluevision/trust-overview/ # Platform trust overview
POST   /api/v1/bluevision/maintenance/   # Schedule maintenance
```

Global Configuration:

```http
GET  /api/v1/bluevision/config/      # Platform configuration
PUT  /api/v1/bluevision/config/      # Update configuration
GET  /api/v1/bluevision/features/    # Feature flags
PUT  /api/v1/bluevision/features/    # Update feature flags
```

API Response Formats

Standard Response Structure

Success Response:

```json
{
  "status": "success",
  "data": {
    "id": 123,
    "name": "Example Resource",
    "created_at": "2024-01-01T00:00:00Z"
  },
  "message": "Operation completed successfully",
  "pagination": {
    "page": 1,
    "per_page": 20,
    "total": 100,
    "pages": 5
  }
}
```

Error Response:

```json
```

```
{
  "status": "error",
  "error": {
    "code": "VALIDATION_ERROR",
    "message": "Invalid input data",
    "details": {
      "field": "email",
      "reason": "Invalid email format"
    }
  },
  "timestamp": "2024-01-01T00:00:00Z"
}
```


Error Codes

Authentication Errors:

- `UNAUTHORIZED`: Missing or invalid authentication
- `TOKEN_EXPIRED`: JWT token has expired
- `TOKEN_INVALID`: JWT token is malformed or invalid

Authorization Errors:

- `FORBIDDEN`: Insufficient permissions for operation
- `ROLE_REQUIRED`: Specific role required for operation
- `ORG_ACCESS_DENIED`: Organization access denied

Validation Errors:

- `VALIDATION_ERROR`: Input validation failed
- `REQUIRED_FIELD`: Required field missing
- `INVALID_FORMAT`: Field format invalid

Resource Errors:

- `NOT_FOUND`: Requested resource not found
- `ALREADY_EXISTS`: Resource already exists
- `CONFLICT`: Resource conflict detected

Rate Limiting and Throttling

Rate Limiting Policies

Default Rate Limits:

- **Authenticated Users**: 1000 requests per hour
- **API Key Access**: 5000 requests per hour
- **Admin Operations**: 2000 requests per hour
- **Public Endpoints**: 100 requests per hour

Rate Limit Headers:

```http
X-RateLimit-Limit: 1000
X-RateLimit-Remaining: 999
X-RateLimit-Reset: 1640995200
X-RateLimit-Retry-After: 3600
```

Rate Limit Response:

```json
{
  "status": "error",
  "error": {
    "code": "RATE_LIMIT_EXCEEDED",
    "message": "Rate limit exceeded",
    "retry_after": 3600
  }
}
```

API Testing and Development

Testing Environment

Sandbox API:

- **Base URL**: `https://sandbox-api.crisp-platform.com/v1/`
- **Test Data**: Pre-populated test data for development
- **Reset Capability**: Periodic reset of test environment
- **Rate Limits**: Relaxed rate limits for testing

Development Tools:

- **API Explorer**: Interactive API documentation and testing
- **Postman Collection**: Complete Postman collection for all endpoints
- **SDK Libraries**: Official SDKs for Python, JavaScript, Java
- **Code Examples**: Comprehensive code examples and tutorials

API Documentation

Interactive Documentation:

- **Swagger/OpenAPI**: Complete OpenAPI 3.0 specification
- **Try It Out**: Live API testing from documentation
- **Code Generation**: Automatic client code generation
- **Schema Validation**: Request/response schema validation

Documentation Features:

- **Comprehensive Examples**: Real-world usage examples
- **Error Scenarios**: Common error cases and solutions
- **Best Practices**: API usage best practices and guidelines
- **Migration Guides**: Version migration assistance

System Administration

Infrastructure Management

System Architecture

Platform Components:

- **Web Application**: User interface and frontend services
- **API Gateway**: Centralized API management and routing
- **Application Services**: Core business logic and processing
- **Database Cluster**: Primary and replica database instances
- **Cache Layer**: Redis-based caching for performance
- **Message Queue**: Asynchronous task processing
- **File Storage**: Secure file storage and content delivery
- **Monitoring Stack**: Comprehensive monitoring and alerting

Security Infrastructure:

- **Web Application Firewall (WAF)**: Protection against web attacks
- **DDoS Protection**: Distributed denial of service protection
- **SSL/TLS Termination**: Secure communication encryption
- **Identity Provider**: Authentication and authorization services
- **Security Information and Event Management (SIEM)**: Security monitoring

- **Intrusion Detection System (IDS)**: Network intrusion detection

Performance Monitoring

Application Performance:

- **Response Time Monitoring**: API and web application response times
- **Throughput Metrics**: Request volume and processing capacity
- **Error Rate Tracking**: Application error rates and patterns
- **Resource Utilization**: CPU, memory, and disk usage monitoring
- **Database Performance**: Query performance and optimization

Infrastructure Monitoring:

- **Server Health**: Operating system and hardware monitoring
- **Network Performance**: Network latency and bandwidth monitoring
- **Storage Systems**: Disk space and I/O performance
- **Load Balancer Health**: Traffic distribution and failover monitoring
- **CDN Performance**: Content delivery network performance

Monitoring Tools and Dashboards:

```json
```

```
GET /api/v1/admin/system-health/
{
  "database": {
    "status": "healthy",
    "connections": 45,
    "slow_queries": 2,
    "storage_used": "68%"
  },
  "application": {
    "status": "healthy",
    "response_time_avg": "245ms",
    "error_rate": "0.02%",
    "active_sessions": 1247
  },
  "infrastructure": {
    "cpu_usage": "45%",
    "memory_usage": "72%",
    "disk_usage": "58%",
    "network_latency": "12ms"
  }
}
```

Backup and Recovery

Backup Strategy

Backup Types:

- **Full Backups**: Complete system and data backups
- **Incremental Backups**: Changes since last backup
- **Differential Backups**: Changes since last full backup
- **Transaction Log Backups**: Real-time transaction logging

Backup Schedule:

- **Daily Backups**: Automated daily backup operations
- **Weekly Full Backups**: Comprehensive weekly system backups
- **Real-Time Replication**: Continuous data replication
- **Geographic Distribution**: Multi-location backup storage

Backup Verification:

- **Integrity Checks**: Regular backup integrity validation
- **Restore Testing**: Periodic restore testing procedures

- **Recovery Time Objectives (RTO)**: Target recovery timeframes
- **Recovery Point Objectives (RPO)**: Data loss tolerance levels

Disaster Recovery

Recovery Procedures:

1. **Incident Detection**: Automatic detection of system failures
2. **Impact Assessment**: Evaluation of failure scope and impact
3. **Recovery Initiation**: Activation of recovery procedures
4. **System Restoration**: Restoration of services and data
5. **Validation**: Verification of system integrity and functionality
6. **Communication**: Stakeholder notification and updates

Business Continuity:

- **Failover Systems**: Automatic failover to backup systems
- **Geographic Redundancy**: Multi-region deployment capabilities
- **Service Level Agreements**: Guaranteed uptime and performance
- **Emergency Communication**: Crisis communication procedures

Security Administration

Security Monitoring

Security Event Detection:

- **Intrusion Detection**: Network and host-based intrusion detection
- **Anomaly Detection**: Behavioral anomaly identification
- **Threat Intelligence Integration**: Real-time threat intelligence feeds
- **Log Analysis**: Comprehensive security log analysis
- **Incident Correlation**: Multi-source security event correlation

Security Metrics:

- **Security Incidents**: Number and severity of security incidents
- **Vulnerability Metrics**: Identified vulnerabilities and remediation status
- **Compliance Status**: Regulatory and policy compliance levels
- **Security Training**: Staff security awareness and training metrics
- **Risk Assessment**: Ongoing risk assessment and mitigation

Vulnerability Management

Vulnerability Assessment:

- **Automated Scanning**: Regular automated vulnerability scanning
- **Manual Testing**: Periodic manual security testing
- **Penetration Testing**: External penetration testing exercises
- **Code Review**: Security-focused code review processes
- **Third-Party Assessment**: External security assessments

Patch Management:

- **Patch Identification**: Systematic identification of required patches
- **Impact Assessment**: Evaluation of patch impact and risks
- **Testing Procedures**: Patch testing in development environments
- **Deployment Planning**: Coordinated patch deployment schedules
- **Verification**: Post-deployment verification and monitoring

Configuration Management

System Configuration

Configuration Standards:

- **Baseline Configurations**: Standardized system configurations
- **Security Hardening**: Security-focused configuration hardening
- **Compliance Configuration**: Regulatory compliance configurations
- **Performance Optimization**: Performance-optimized settings
- **Documentation**: Comprehensive configuration documentation

Change Management:

- **Change Control**: Formal change control processes
- **Approval Workflows**: Multi-stage approval workflows
- **Testing Requirements**: Mandatory testing before deployment
- **Rollback Procedures**: Automated rollback capabilities
- **Change Documentation**: Complete change history and documentation

Environment Management

Environment Types:

- **Development**: Development and testing environment
- **Staging**: Pre-production testing environment

- **Production**: Live production environment
- **Disaster Recovery**: Backup production environment

Environment Synchronization:

- **Code Deployment**: Automated code deployment pipelines
- **Configuration Sync**: Environment configuration synchronization
- **Data Migration**: Secure data migration procedures
- **Testing Automation**: Automated testing across environments

Maintenance and Updates

Scheduled Maintenance

Maintenance Windows:

- **Regular Maintenance**: Scheduled weekly maintenance windows
- **Emergency Maintenance**: Unscheduled critical maintenance
- **Major Updates**: Planned major system updates
- **Security Patches**: Critical security patch deployment

Maintenance Procedures:

1. **Pre-Maintenance**: System backup and preparation
2. **Notification**: User and stakeholder notification
3. **Service Interruption**: Controlled service shutdown
4. **Maintenance Execution**: Maintenance task execution
5. **Testing**: Post-maintenance system testing
6. **Service Restoration**: Service restoration and verification
7. **Post-Maintenance**: Monitoring and documentation

Update Management

Update Types:

- **Security Updates**: Critical security patches and fixes
- **Feature Updates**: New functionality and improvements
- **Performance Updates**: Performance optimizations and enhancements
- **Bug Fixes**: Issue resolution and stability improvements

Update Process:

1. **Update Planning**: Update planning and scheduling
2. **Testing**: Comprehensive testing in staging environment
3. **Approval**: Change approval and authorization
4. **Deployment**: Controlled update deployment
5. **Verification**: Post-deployment verification and testing
6. **Monitoring**: Enhanced monitoring during update period
7. **Documentation**: Update documentation and communication

Troubleshooting

Common Issues and Solutions

User Access Issues

Problem: Users Cannot Log In

Possible Causes:

- Invalid credentials
- Account locked due to failed attempts
- Multi-factor authentication issues
- Network connectivity problems
- System maintenance or outages

Troubleshooting Steps:

1. **Verify Credentials**: Confirm username and password accuracy
2. **Check Account Status**: Verify account is active and not locked
3. **MFA Verification**: Ensure MFA device is working correctly
4. **Network Connectivity**: Test internet connection and DNS resolution
5. **System Status**: Check platform status and maintenance schedules

Solutions:

- **Password Reset**: Use password reset functionality
- **Account Unlock**: Contact administrator for account unlock
- **MFA Reset**: Reset MFA device with administrator assistance
- **Network Troubleshooting**: Resolve network connectivity issues
- **Alternative Access**: Use alternative access methods if available

Admin Resolution:

```
json

POST /api/v1/admin/unlock-account/
{
    "user_id": 123,
    "reason": "Failed login attempts - user verified via phone"
}
```

Trust Relationship Issues

Problem: Trust Relationships Not Working

Possible Causes:

- Relationship not properly configured
- Insufficient permissions
- Network connectivity issues
- Partner organization problems
- Policy misalignment

Troubleshooting Steps:

1. **Relationship Status**: Verify relationship is active and approved
2. **Permission Check**: Confirm user has appropriate permissions
3. **Configuration Review**: Validate trust relationship configuration
4. **Partner Communication**: Contact partner organization
5. **Network Testing**: Test connectivity to partner systems

Solutions:

- **Reconfigure Relationship**: Update relationship configuration
- **Permission Grant**: Grant necessary permissions to users
- **Policy Alignment**: Align sharing policies with partner
- **Technical Support**: Engage technical support for connectivity issues
- **Relationship Renewal**: Renew or renegotiate relationship terms

Content Publishing Issues

Problem: Content Not Publishing Successfully

Possible Causes:

- Format validation errors
- Classification issues
- Insufficient permissions
- Network problems
- System capacity limits

Troubleshooting Steps:

1. **Format Validation**: Check content format and structure
2. **Classification Review**: Verify proper classification assignment
3. **Permission Verification**: Confirm publishing permissions
4. **Network Check**: Test network connectivity
5. **System Status**: Check system capacity and performance

Solutions:

- **Format Correction**: Fix content format and validation errors
- **Classification Update**: Correct classification assignments
- **Permission Grant**: Request additional publishing permissions
- **Retry Publication**: Retry after resolving network issues
- **Support Contact**: Contact technical support for system issues

Performance Issues

Problem: Slow System Performance

Possible Causes:

- High system load
- Network latency
- Database performance issues
- Client-side problems
- Resource constraints

Troubleshooting Steps:

1. **System Health Check**: Monitor system health dashboard
2. **Network Testing**: Test network speed and latency
3. **Browser Testing**: Try different browsers or devices
4. **Cache Clearing**: Clear browser cache and cookies

5. **Resource Monitoring**: Check system resource utilization

Solutions:

- **Load Balancing**: Distribute load across multiple servers
- **Performance Optimization**: Optimize database queries and caching
- **Network Optimization**: Improve network configuration
- **Client Optimization**: Update browsers and clear caches
- **Capacity Scaling**: Scale system resources as needed

Diagnostic Tools and Techniques

System Health Monitoring

Health Check Endpoints:

```http
GET /api/v1/health/                    # Basic health check
GET /api/v1/health/detailed/           # Detailed health information
GET /api/v1/admin/system-health/       # Comprehensive system health
```

Health Check Response:

```json
{
    "status": "healthy",
    "timestamp": "2024-01-01T12:00:00Z",
    "services": {
        "database": "healthy",
        "cache": "healthy",
        "message_queue": "healthy",
        "external_apis": "degraded"
    },
    "metrics": {
        "response_time": "185ms",
        "cpu_usage": "45%",
        "memory_usage": "67%",
        "disk_usage": "52%"
    }
}
```

Log Analysis

Log Categories:

- **Application Logs**: Application-specific events and errors
- **Security Logs**: Security events and audit information
- **Access Logs**: User access and API usage logs
- **Error Logs**: System errors and exceptions
- **Performance Logs**: Performance metrics and statistics

Log Analysis Tools:

- **Real-Time Monitoring**: Live log monitoring and analysis
- **Search and Filter**: Advanced search and filtering capabilities
- **Pattern Recognition**: Automated pattern detection and alerting
- **Correlation Analysis**: Multi-log correlation and analysis
- **Historical Analysis**: Historical log analysis and trending

Network Diagnostics

Network Testing Tools:

- **Connectivity Tests**: Basic network connectivity verification
- **Latency Measurement**: Network latency and response time testing
- **Bandwidth Testing**: Network bandwidth and throughput testing
- **DNS Resolution**: DNS lookup and resolution testing
- **Certificate Validation**: SSL/TLS certificate validation

Network Troubleshooting:

1. **Ping Tests**: Basic connectivity verification
2. **Traceroute**: Network path analysis
3. **Port Testing**: Specific port connectivity testing
4. **DNS Lookup**: DNS resolution verification
5. **Certificate Check**: SSL certificate validation

Error Resolution Procedures

Error Classification

Error Severity Levels:

- **Critical**: System down, major functionality unavailable
- **High**: Significant functionality impaired, security issues
- **Medium**: Minor functionality issues, performance degradation

- **Low**: Cosmetic issues, documentation problems

Error Categories:

- **System Errors**: Infrastructure and platform errors
- **Application Errors**: Business logic and functional errors
- **User Errors**: User-generated errors and mistakes
- **Integration Errors**: Third-party integration failures
- **Security Errors**: Security-related incidents and violations

Escalation Procedures

Level 1 Support:

- **Basic Troubleshooting**: Standard troubleshooting procedures
- **User Assistance**: Direct user support and guidance
- **Documentation**: Issue documentation and tracking
- **Resolution**: Simple issue resolution and follow-up

Level 2 Support:

- **Advanced Troubleshooting**: Complex technical troubleshooting
- **System Analysis**: In-depth system analysis and diagnosis
- **Configuration Changes**: System configuration modifications
- **Escalation**: Escalation to development or operations teams

Level 3 Support:

- **Development Team**: Complex application issues and bugs
- **Operations Team**: Infrastructure and platform issues
- **Security Team**: Security incidents and violations
- **Vendor Support**: Third-party vendor support coordination

Resolution Documentation

Incident Documentation:

- **Issue Description**: Detailed description of the problem
- **Impact Assessment**: Analysis of issue impact and scope
- **Root Cause Analysis**: Identification of underlying causes
- **Resolution Steps**: Detailed resolution procedures
- **Prevention Measures**: Steps to prevent recurrence

Knowledge Base:

- **Solution Database**: Searchable database of known solutions
- **Best Practices**: Documented best practices and procedures
- **Troubleshooting Guides**: Step-by-step troubleshooting guides
- **FAQ Section**: Frequently asked questions and answers
- **Video Tutorials**: Visual troubleshooting and training materials

Support Resources

Internal Support

Support Team Structure:

- **Help Desk**: First-line user support and assistance
- **Technical Support**: Advanced technical troubleshooting
- **System Administration**: Infrastructure and platform support
- **Development Team**: Application development and bug fixes
- **Security Team**: Security incident response and support

Support Channels:

- **Help Desk Portal**: Online support ticket system
- **Email Support**: Direct email support and assistance
- **Phone Support**: Emergency phone support for critical issues
- **Live Chat**: Real-time chat support during business hours
- **Self-Service**: Comprehensive self-service knowledge base

External Support

Vendor Support:

- **Platform Vendor**: CRISP platform vendor support
- **Infrastructure Providers**: Cloud and hosting provider support
- **Security Vendors**: Security tool and service vendor support
- **Integration Partners**: Third-party integration support
- **Professional Services**: Consulting and implementation services

Community Support:

- **User Forums**: Community-driven support forums
- **User Groups**: Local and industry user groups

- **Documentation**: Comprehensive online documentation
- **Training Resources**: Training materials and courses
- **Best Practice Sharing**: Community best practice sharing

Best Practices

Security Best Practices

Account Security

Password Management:

- **Complex Passwords**: Use passwords with minimum 12 characters including uppercase, lowercase, numbers, and symbols
- **Unique Passwords**: Use unique passwords for CRISP platform separate from other systems
- **Password Rotation**: Change passwords regularly, at least every 90 days
- **Password Managers**: Use enterprise password managers for secure password storage
- **Avoid Common Passwords**: Never use dictionary words, personal information, or common patterns

Multi-Factor Authentication (MFA):

- **Enable MFA**: Always enable MFA for additional account security
- **Authenticator Apps**: Use authenticator apps rather than SMS when possible
- **Backup Codes**: Securely store backup authentication codes
- **Device Management**: Regularly review and clean up trusted devices
- **MFA Policies**: Implement organizational MFA policies and enforcement

Session Management:

- **Secure Logout**: Always log out when finished, especially on shared devices
- **Session Timeouts**: Configure appropriate session timeout periods
- **Concurrent Sessions**: Monitor and limit concurrent session usage
- **Suspicious Activity**: Report unusual account activity immediately
- **Session Review**: Regularly review active sessions and terminate unnecessary ones

Data Handling

Information Classification:

- **Proper Classification**: Ensure all content is properly classified according to organizational policies
- **TLP Compliance**: Follow Traffic Light Protocol standards for information sharing

- **Sensitivity Assessment**: Regularly assess information sensitivity and adjust classifications
- **Classification Training**: Ensure all users understand classification requirements
- **Review and Update**: Periodically review and update classification assignments

Secure Sharing:

- **Need-to-Know Basis**: Share information only with those who need it
- **Trust Verification**: Verify trust relationships before sharing sensitive information
- **Sharing Policies**: Follow organizational information sharing policies
- **Access Controls**: Implement appropriate access controls for shared information
- **Sharing Audit**: Maintain audit trails of information sharing activities

Data Protection:

- **Encryption**: Use encryption for sensitive data transmission and storage
- **Access Logging**: Log all access to sensitive information
- **Data Retention**: Follow data retention policies and procedures
- **Secure Disposal**: Securely dispose of information when no longer needed
- **Privacy Protection**: Protect personal and sensitive information appropriately

Operational Best Practices

Daily Operations

Routine Monitoring:

- **Dashboard Review**: Check dashboard and system status daily
- **Alert Response**: Respond promptly to alerts and notifications
- **Activity Review**: Review user and system activity regularly
- **Performance Check**: Monitor system performance and capacity
- **Security Scan**: Conduct regular security scans and assessments

Content Management:

- **Quality Assurance**: Ensure all published content meets quality standards
- **Timeliness**: Publish time-sensitive information promptly
- **Accuracy Verification**: Verify information accuracy before publication
- **Source Attribution**: Properly attribute information sources
- **Update Management**: Keep published information current and relevant

User Management:

- **Account Monitoring**: Monitor user account activity and compliance
- **Permission Reviews**: Regularly review and update user permissions
- **Training Management**: Ensure users complete required training
- **Support Response**: Provide timely support and assistance to users
- **Feedback Collection**: Collect and act on user feedback

Trust Relationship Management

Relationship Maintenance:

- **Regular Communication**: Maintain regular communication with trust partners
- **Performance Review**: Regularly review relationship performance and value
- **Policy Compliance**: Ensure compliance with trust relationship policies
- **Issue Resolution**: Address relationship issues promptly and professionally
- **Value Assessment**: Continuously assess relationship value and benefits

Trust Network Development:

- **Strategic Planning**: Develop strategic plans for trust network expansion
- **Partner Evaluation**: Carefully evaluate potential trust partners
- **Due Diligence**: Conduct thorough due diligence before establishing relationships
- **Risk Management**: Assess and manage trust relationship risks
- **Community Engagement**: Actively participate in trust communities and groups

Technical Best Practices

API Usage

Authentication:

- **Secure Token Storage**: Store API tokens securely and never in code
- **Token Rotation**: Rotate API tokens regularly
- **Scope Limitation**: Use tokens with minimal required scope
- **Secure Transmission**: Always use HTTPS for API communications
- **Token Monitoring**: Monitor API token usage and detect anomalies

Rate Limiting:

- **Respect Limits**: Stay within published rate limits
- **Efficient Requests**: Optimize API requests for efficiency
- **Batch Operations**: Use batch operations when available

- **Caching**: Implement client-side caching to reduce API calls
- **Error Handling**: Implement proper error handling and retry logic

Data Processing:

- **Input Validation**: Validate all input data before processing
- **Error Handling**: Implement comprehensive error handling
- **Data Sanitization**: Sanitize data to prevent injection attacks
- **Output Encoding**: Properly encode output data
- **Logging**: Log API usage and errors for troubleshooting

Integration Best Practices

System Integration:

- **API-First Design**: Design integrations using APIs when possible
- **Loose Coupling**: Implement loosely coupled integration architectures
- **Error Recovery**: Design systems for graceful error recovery
- **Monitoring**: Monitor integration health and performance
- **Documentation**: Maintain comprehensive integration documentation

Data Synchronization:

- **Consistency**: Ensure data consistency across integrated systems
- **Conflict Resolution**: Implement conflict resolution strategies
- **Version Control**: Manage data version control and updates
- **Backup Strategies**: Implement backup strategies for integrated data
- **Testing**: Thoroughly test all integration scenarios

Compliance Best Practices

Regulatory Compliance

Compliance Framework:

- **Requirements Understanding**: Understand applicable regulatory requirements
- **Policy Implementation**: Implement policies to ensure compliance
- **Regular Assessment**: Conduct regular compliance assessments
- **Documentation**: Maintain comprehensive compliance documentation
- **Training**: Provide compliance training to all relevant personnel

Audit Preparation:

- **Audit Readiness**: Maintain audit-ready documentation and processes
- **Evidence Collection**: Systematically collect and organize audit evidence
- **Process Documentation**: Document all compliance-related processes
- **Continuous Monitoring**: Implement continuous compliance monitoring
- **Improvement**: Continuously improve compliance processes and controls

Privacy Protection

Data Privacy:

- **Privacy by Design**: Implement privacy by design principles
- **Data Minimization**: Collect and process only necessary data
- **Consent Management**: Implement proper consent management procedures
- **Subject Rights**: Support data subject rights and requests
- **Cross-Border**: Manage cross-border data transfer requirements

Privacy Controls:

- **Access Controls**: Implement strong access controls for personal data
- **Encryption**: Use encryption for personal data protection
- **Anonymization**: Implement data anonymization techniques
- **Retention**: Follow data retention and deletion policies
- **Incident Response**: Implement privacy incident response procedures

Performance Optimization

System Performance

Performance Monitoring:

- **Baseline Establishment**: Establish performance baselines and benchmarks
- **Continuous Monitoring**: Implement continuous performance monitoring
- **Trend Analysis**: Analyze performance trends and patterns
- **Capacity Planning**: Plan for future capacity requirements
- **Optimization**: Continuously optimize system performance

Resource Management:

- **Resource Allocation**: Optimize resource allocation and utilization
- **Scaling Strategies**: Implement appropriate scaling strategies
- **Load Distribution**: Distribute load effectively across system components

- **Caching**: Implement effective caching strategies
- **Compression**: Use compression to reduce bandwidth usage

User Experience Optimization

Interface Design:

- **User-Centric Design**: Design interfaces with user needs in mind
- **Accessibility**: Ensure accessibility for all users
- **Responsive Design**: Implement responsive design for all devices
- **Performance**: Optimize interface performance and responsiveness
- **Feedback**: Collect and act on user interface feedback

User Training:

- **Comprehensive Training**: Provide comprehensive user training programs
- **Role-Specific Training**: Tailor training to specific user roles
- **Ongoing Education**: Provide ongoing education and updates
- **Self-Service**: Develop self-service training and help resources
- **