AI PQC Audit

Comprehensive How To Guide

Complete User Manual for Post-Quantum Cryptography Auditing Platform

Generated: November 06, 2025
Version 1.0

Platform Features:
• 13 Comprehensive Audit Areas
• Multi-AI Analysis Engine
• CISO-Ready Reporting
• Real-Time Threat Monitoring
• Enterprise Security Controls
• Automated NIST Updates

Table of Contents

1. Getting Started

Welcome to AI PQC Audit

AI PQC Audit is a comprehensive platform for assessing your organization's readiness for post-quantum cryptography threats. This guide will walk you through every feature and capability of the platform.

What This Platform Does

• **13 Audit Areas:** Domain TLS, Documents, Networks, Devices, Code, Software, IoT, IAM, PKI, Cloud, Vendor, Email, Mobile, and Blockchain
• **Multi-AI Analysis:** Uses OpenAI GPT-4o, Anthropic Claude, Google Gemini, and xAI Grok for consensus analysis
• **CISO-Ready Reports:** Executive summaries with individual asset analysis and prioritized action plans
• **Latest Standards:** Automatically updated with NIST and industry developments

Quick Start Process

1. Create an account and log in
2. Start a new audit session
3. Upload files or enter domains for scanning
4. Review AI-powered analysis results
5. Download comprehensive reports

> **Tip:** Have your network inventory, device lists, and domain names ready before starting your first audit.

2. Account Setup

Creating Your Account

1. Click "Start Free Trial" on the homepage
2. Enter your email address and create a secure password
3. Verify your email address (check spam folder if needed)
4. Complete your profile with organization details

Security Settings

After logging in, enhance your account security:
1. Go to your user dropdown → Security Settings
2. Set up Multi-Factor Authentication (MFA)
3. Choose between authenticator app or SMS verification
4. Save backup codes in a secure location

Organization Management

For team accounts:
• Create or join an organization
• Invite team members with role-based access
• Configure organization settings and preferences
• Set up shared audit templates

3. Starting Audits

Creating a New Audit Session

1. Click "Start New Audit" from the homepage or dashboard
2. Enter a descriptive audit name (e.g., "Q4 2025 Security Assessment")
3. Select audit type: Comprehensive (recommended for full analysis)
4. Click "Start Audit" to create your session

Planning Your Audit

Before starting, gather:
• **Domain Lists:** All organizational domains and subdomains
• **Network Inventory:** CSV files with network configurations
• **Device Lists:** Hardware inventory with firmware versions
• **Code Archives:** Source code ZIP files for analysis
• **Policy Documents:** Cryptographic policies and procedures

4. Scan Types

The platform supports 13 comprehensive audit areas:

Scan Type	Purpose	Input Format
Domain TLS/SSL	Analyze TLS configurations	Domain names
Document Analysis	Review policies and strategies	PDF, DOCX, TXT
Network Assessment	Evaluate infrastructure	CSV, JSON, YAML
Device Inventory	Assess hardware readiness	CSV files
Code Analysis	Scan source code	ZIP archives
Software Inventory	Analyze packages	JSON, TXT
IoT/Edge Devices	Evaluate IoT security	CSV files
IAM Systems	Review access management	YAML, JSON
PKI Certificates	Analyze certificates	PEM, P7B, CRT
Cloud Infrastructure	Assess cloud security	YAML, JSON
Vendor Assessment	Evaluate third parties	JSON files
Email Systems	Analyze email security	JSON files
Mobile Applications	Review mobile security	JSON files
Blockchain	Assess blockchain crypto	JSON files

5. File Preparation

Supported File Formats

Scan Type	File Formats	Size Limit	Notes
Documents	PDF, DOCX, TXT	10MB	Policies, procedures
Network	CSV, JSON, YAML	5MB	Network inventories
Devices	CSV	5MB	Hardware specifications
Code	ZIP	25MB	Source code archives
Software	JSON, TXT	5MB	Package lists
PKI	PEM, P7B, CRT	1MB	Certificate files
Cloud/IAM	YAML, JSON	5MB	Infrastructure configs
Others	JSON	5MB	Various configurations

Data Preparation Tips

- **Accuracy:** Ensure all data is current and accurate
- **Completeness:** Include all relevant systems and components
- **Privacy:** Remove sensitive personal information before upload
- **Format:** Follow template structures exactly for best results
- **Organization:** Group related systems logically

6. Running Scans

Step-by-Step Scanning Process

1. **Access Scan Wizard:** From your audit session, click "Scan Files & Generate Reports"
2. **Select Scan Type:** Choose from 13 available audit areas
3. **Upload Files or Enter Data:** Domain names, file uploads, or direct text input
4. **Initiate Scan:** Click "Scan [Type] & Generate Report"
5. **Wait for Analysis:** AI engines process your data (30-60 seconds)
6. **Review Results:** Automatic redirect to results page

Multi-AI Processing

Each scan uses multiple AI engines:
• **OpenAI GPT-4o:** Advanced reasoning and analysis
• **Anthropic Claude:** Safety-focused vulnerability assessment
• **Google Gemini:** Multimodal analysis and insights
• **xAI Grok:** Real-time threat intelligence

7. Understanding Results

Risk Scoring System

• **Critical (8.0-10.0):** Immediate action required
• **Moderate (5.0-7.9):** Address within 30 days
• **Low Risk (3.0-4.9):** Monitor and plan
• **Compliant (0.0-2.9):** Quantum-ready

Individual Asset Analysis

For each asset, results include:
• **Asset Name:** Specific identifier
• **Current State:** Present configuration/status
• **Vulnerability:** Specific security weakness
• **Action Required:** Step-by-step remediation
• **Business Impact:** Operational consequences
• **Timeline:** Recommended implementation schedule
• **Effort Level:** Resource requirements (Low/Medium/High)

8. Reports & Exports

Report Generation

The platform provides multiple report formats:
• **Text Reports (Copy Function):** Complete text version for sharing
• **PDF Reports:** Professional formatted documents for presentations
• **Executive Summary:** High-level overview with key findings
• **Technical Analysis:** Detailed vulnerability descriptions
• **Methodology Section:** AI analysis details and criteria

Advanced Analytics

• **Analytics Dashboard:** Executive charts and trends
• **Q-Day Monitor:** Quantum threat timeline analysis
• **Multi-AI Engine:** Consensus analysis details
• **Compliance Dashboard:** Standards alignment tracking

9. Advanced Features

Q-Day Timeline Monitoring

- **Q-Day Analysis:** X + Y > Z assessment
- **Threat Timeline:** Real-time quantum progress tracking
- **Migration Planning:** Automated PQ migration timelines
- **Risk Forecasting:** Predictive quantum threat analysis

Organization Management

- **Role-Based Access:** Admin, Manager, Analyst, Viewer roles
- **Team Collaboration:** Shared audit sessions and templates
- **Centralized Reporting:** Organization-wide security posture
- **Policy Management:** Custom organizational policies

Security Monitoring

- **Security Monitor:** Real-time threat detection
- **Audit Logging:** Complete activity tracking
- **IP Monitoring:** Geographic and behavioral analysis
- **Alert System:** Email and SMS notifications

10. Troubleshooting

Common Issues and Solutions

Error Code	Description	Solution
AUTH_001	Authentication failure	Log out and log back in
UPLOAD_002	File format not supported	Check supported formats
SCAN_003	AI engine timeout	Retry scan, reduce file size
REPORT_004	PDF generation failure	Use text report, contact support
SESSION_005	Invalid audit session	Start new audit session

Getting Additional Help

- **Submit Ticket:** Support → Submit Ticket with detailed description
- **Live Chat:** Available during business hours
- **Email Support:** Include session ID and error details
- **FAQ:** Check FAQ section for additional answers
- **Video Tutorials:** Step-by-step visual guides

> **Support Hours:** Monday-Friday 9 AM - 6 PM EST. Emergency support available for enterprise customers.