SecTrail Certificate Manager

Documentation

v2.7.0

June 4, 2026

Table of Contents

SecTrail Certificate Manager

SecTrail Certificate Manager (CM) is a comprehensive platform designed for enterprise-grade SSL/TLS digital certificate lifecycle management.

> **VERSION INFORMATION**
>
> This documentation is prepared for **SecTrail CM v2.7.0**.

Overview

SecTrail CM addresses critical certificate management challenges that organizations face:

- **Inventory Gaps**: Tracking certificates in distributed systems
- **Manual Processing Burden**: Automation of time-consuming manual processes
- ⏱ **Expiration Date Tracking**: Monitoring certificate expirations
- **Operational Overhead**: Reducing workload and increasing efficiency

Why SecTrail CM?

With SecTrail Certificate Manager, organizations:

- [OK] Transition from reactive, crisis-driven management to **proactive automation**
- [OK] **Automate** repetitive manual processes
- [OK] Gain **complete visibility** in certificate inventory
- [OK] **Simplify operations** in digital transformation processes
- [OK] **Prevent** unexpected service disruptions

Key Features

Certificate Discovery

Automatically discover all certificates in your infrastructure and add them to your inventory.

Certificate Inventory

Track and manage all your certificates in a centralized catalog.

Certificate Authority (CA)

Manage your internal CA infrastructure and create internal certificates.

Certificate Monitoring

Continuously monitor certificate statuses and receive proactive alerts.

Certificate Workflow

Manage approval and request processes. Simplify your workflows with fully automated process management.

System Integrations

Seamless integration with third-party systems.

RBAC Authorization

Secure management with role-based access control.

Quick Start

To quickly get started with SecTrail CM:

1. **Installation Guide** - System installation and configuration
2. **Quick Start** - First steps and basic usage
3. **User Guide** - Detailed usage scenarios

Next Steps

You can continue your SecTrail CM journey with these steps:

Getting Started

Installation and basic configuration

Overview ->

Features

Explore all features

Certificate Discovery ->

Integrations

Integrate with your systems

Integration Guide ->

Support and Community

Do you have any questions or need support?

Channel	Description	Link
Support Portal	Technical support and ticketing system	destek.bntpro.com
Product Page	Product information and updates	www.sectrail.com/cm

Uninterrupted security and maximum efficiency with SecTrail Certificate Manager.

Overview

SecTrail Certificate Manager (CM) is a digital platform that enables end-to-end management of the entire SSL/TLS certificate lifecycle from a single portal.

What is SecTrail CM?

SecTrail Certificate Manager is a certificate lifecycle management system that enables organizations to discover, monitor, manage, and automate their digital certificates from a centralized platform.

Core Problem and Solution

Today, organizations must manage hundreds or even thousands of SSL/TLS certificates alongside their growing digital infrastructure. These certificates can be distributed across different servers, cloud platforms, load balancers, and CDNs. Certificates managed using manual tracking systems, Excel files, or scattered tools create serious risks for organizations:

- **Expiration Risks**: Certificates not renewed in time can cause critical service outages and business losses
- **Security Vulnerabilities**: Certificates with weak algorithms, low bit lengths, or signed by untrusted CAs pose security threats
- **Compliance Issues**: Failure to meet regulatory requirements can lead to audit process problems and potential penalties
- **Lack of Visibility**: It's unclear how many certificates the organization has, where they are used, and what their status is
- **High Operational Burden**: Extra time and human resources are spent on certificate management

SecTrail CM solves these challenges with automatic discovery, centralized management, proactive monitoring, and intelligent automation features, enabling organizations to perform certificate management in a secure, efficient, and scalable manner.

Challenge	SecTrail CM Solution
Scattered Infrastructure	View all certificates from a single point with automatic discovery
Manual Processes	Complete automation of the certificate lifecycle
Lack of Visibility	Centralized inventory and real-time monitoring
Expiration Risks	Proactive alerts and automatic renewal
Compliance Challenges	Detailed reporting and audit trail

Key Benefits

Category	Benefits
** Operational Efficiency**	Reduce manual operations by up to 80%, increase team productivity
** Risk Reduction**	Prevent outages, proactively detect security vulnerabilities, minimize non-compliance risk
** Cost Savings**	Reduce operational costs, prevent outage costs
** Visibility and Control**	Complete inventory, real-time monitoring, detailed reporting

Installation Guide

This section contains detailed installation steps for SecTrail Certificate Manager.

Installation Overview

SecTrail CM is delivered as a **Virtual Appliance** in OVA format. This approach greatly simplifies installation:

- [OK] **Easy Installation**: Deploy the OVA file to your virtualization environment
- [OK] **Pre-configured**: All components (database, web server, etc.) come ready
- [OK] **Quick Start**: Just configure network settings and start using
- [OK] **No Manual Installation**: No package management, dependency resolution, or service configuration needed

Basic Steps:

1. Import the OVA image to your virtualization platform
2. Start the VM and log in with the `stadmin` user
3. Configure network settings with the `config` command
4. Access the system from the web interface

System Requirements

Hardware Requirements

Minimum Requirements

- **CPU**: 4 Cores
- **RAM**: 8 GB
- **Disk**: 100 GB
- **Network**: 1 Gbps

Recommended Requirements (Production Environment)

- **CPU**: 8 Cores
- **RAM**: 16 GB
- **Disk**: 200 GB
- **Network**: 1 Gbps

Pre-Installation Preparation

1. Virtualization Environment Requirements

SecTrail CM is distributed as a virtual machine image in OVA format.

2. Network Configuration Preparation

Have the following network information ready before installation:

Parameter	Description
IP Address	Static IP address for SecTrail CM (in CIDR notation)
Gateway	Default gateway IP address
DNS Servers	Primary (and optionally secondary/tertiary) DNS server addresses

3. Firewall and Port Configuration

The following ports must be open for SecTrail CM to function properly:

Port	Protocol	Usage	Direction
443	HTTPS	Web Interface	Inbound
22	SSH	Remote management (optional)	Inbound

Installation Steps

SecTrail CM is delivered as a Virtual Appliance and distributed in OVA (Open Virtualization Archive) format. Manual package management is not required for installation.

1. Deploying the OVA Image to Virtualization Environment

Deploy the SecTrail CM OVA image to your virtualization environment.

2. Initial Login and Network Configuration

After starting the VM, follow these steps from the console screen:

Login Credentials

Use the following username for initial login:

- **Username**: `stadmin`
- **Password**: Password will be shared with you

Network Configuration

After logging in, start network configuration:

```
stadmin@SecTrailCM ~]$ config
```

When the command is executed, the **SecTrail CM Configurator** will start.

Step 1: IP Address Configuration

```
Please enter a valid IP Address in CIDR Notation (e.g. 192.168.1.10/24)

IP Address: 10.34.24.56/24
OK
```

- Enter the IP address and subnet mask in CIDR notation (e.g., `10.34.24.56/24`)
- Press Enter to confirm

Step 2: Gateway Address Configuration

```
Please enter a valid Gateway Address

Gateway IP Address: 10.34.24.1
OK
```

- Enter the default gateway IP address
- Press Enter to confirm

Step 3: DNS Server Configuration

```
How many DNS servers do you want to configure? (1-3)
1

Please enter a valid DNS Server Address

DNS Server IP Address: 10.34.24.150
```

- Enter the number of DNS servers you want to configure (between 1-3)
- Enter the IP address for each DNS server

Step 4: Configuration Summary and Confirmation

```
IP: 10.34.24.56/24 -- GW: 10.34.24.1 -- DNS SERVERS: 10.34.24.150

Network Configuration will be set. Do you want to continue? (y/n)y
```

- Review the information you entered
- If correct, press `y` to continue

Configuration Activation

```
Activating Network Configuration

Setting IP Address
IP Address Set

Setting Default Gateway
Default Gateway Set

DNS Servers Set
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/2)

Settings Saved

Network Configuration Completed Successfully
```

You will see the above messages when network configuration is completed successfully.

3. Application Key Generation (Optional)

After network configuration is completed, SecTrail CM offers the option to generate an application key:

```
SecTrail CM Application Key Generator

regenerate Application Key

Do you want to generate SecTrail CM Application Key (y/n)?y
```

- Press `y` to generate a new application key
- Press `n` to keep the existing key

```
Application key set successfully.
```

4. Configuration Completed

After configuration is completed, you can use the IP address you set to access the web interface.

Post-Installation Checks

1. Web Interface Access

After network configuration is completed, go to the following address from your browser:

```
https://your-server-ip
```

> **SSL CERTIFICATE WARNING**
>
> On first access, your browser may display a security warning due to the self-signed SSL certificate. For production environments, it is recommended to use a certificate signed by a corporate CA.

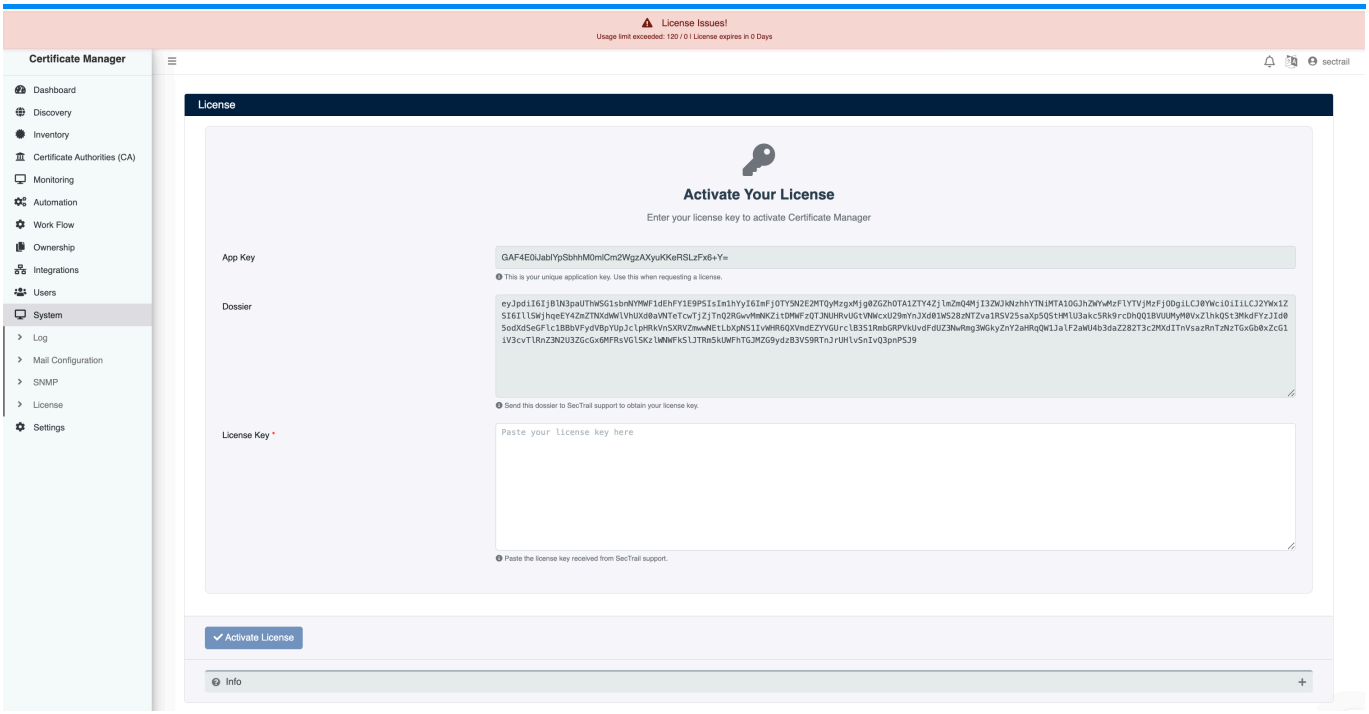
Initial Login Credentials

Default administrator account for initial web interface login:

- **Username**: `admin`
- **Password**: `admin`

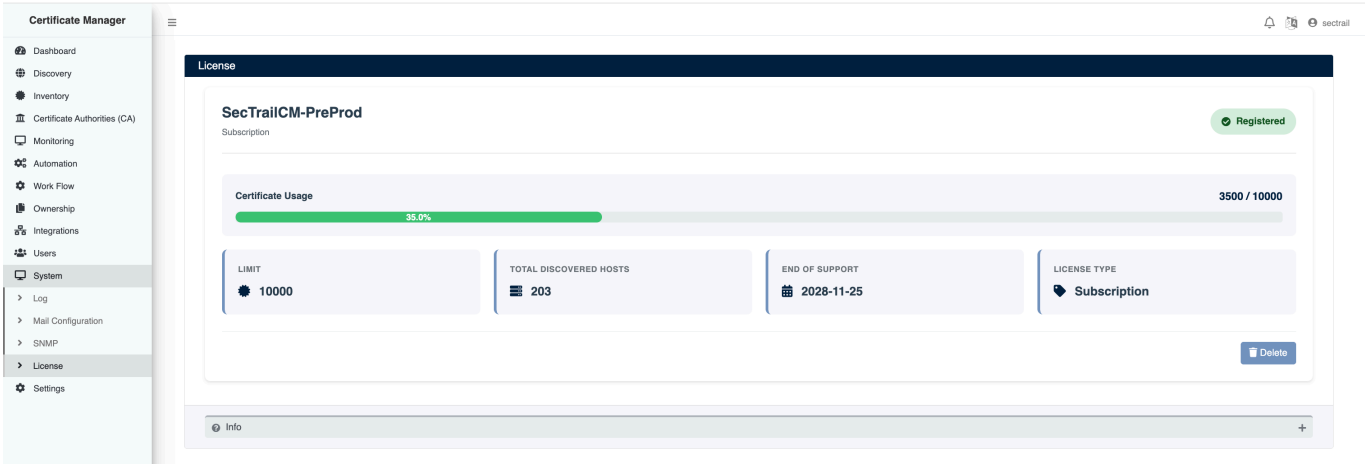
2. License Activation

You need to activate the license on first login. Follow these steps for license activation:



1. The license activation screen will appear when you first log in to the web interface
2. Share the **App Key** and **Dossier** information shown on the screen with the SecTrail CM support team
3. Enter the **License Key** provided by the support team in the relevant field
4. License verification will be performed automatically

After license activation is completed, you can view your license details:



CERTIFICATE COUNTING

SecTrail CM counts certificates as **unique** under the license scope. Even if the same certificate is used on different systems (for example, on different servers or load balancers), it is counted only once. This allows you to manage your actual certificate count and use your license efficiently.

OBTAINING LICENSE

You can obtain your license key by sending your App Key and Dossier information to destek@sectrail.com or sdg-dev@bntpro.com.

Quick Start

Welcome to SecTrail Certificate Manager! This guide contains the essential steps to get you started with the platform.

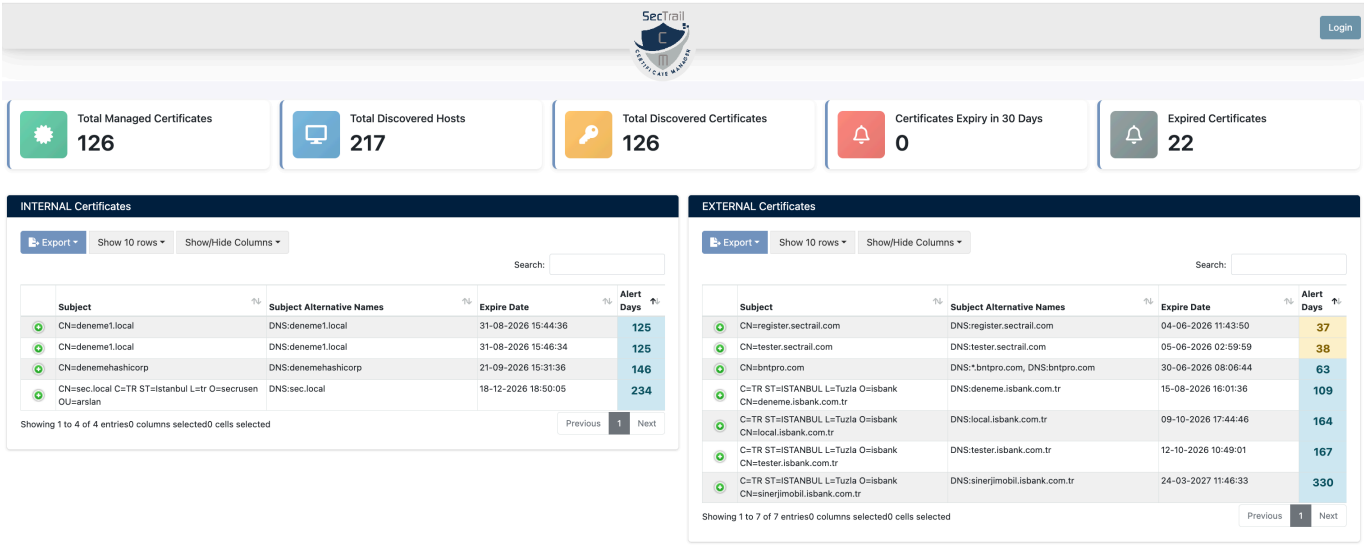
1. Platform Access

Navigate to your SecTrail CM address from your web browser:

```
https://your-sectrailcm-server
```

2. Public Dashboard

> **PUBLIC DASHBOARD**
>
> You can view the **Public Dashboard** before logging into SecTrail CM. This screen displays the general status of certificates in your infrastructure publicly.



SecTrail CM Public Dashboard - General Certificate Status

Dashboard Metrics

You can see the following important metrics on the Public Dashboard:

Metric	Description
Total Managed Certificates	Total number of managed certificates
Total Discovered Hosts	Total number of discovered hosts
Total Discovered Certificates	Total number of discovered certificates
Certificates Expiry in 30 Days	Certificates expiring within 30 days
Expired Certificates	Expired certificates

Certificate Views

The dashboard lists certificates under two main categories:

- **INTERNAL Certificates**: Certificates on the internal network
- **EXTERNAL Certificates**: Certificates on the external network

Certificate Details

The following information is displayed for each certificate:

- **Subject** - Certificate subject
- **Subject Alternative Names** - Alternative names (SAN)
- **Expiry Date** - Expiration date
- **Days to Expiry** - Days until expiration

> **TIP**
>
> - You can customize the columns you want to see with the **Show/Hide Columns** button
> - You can access certificate details by clicking the **+** button

3. Login

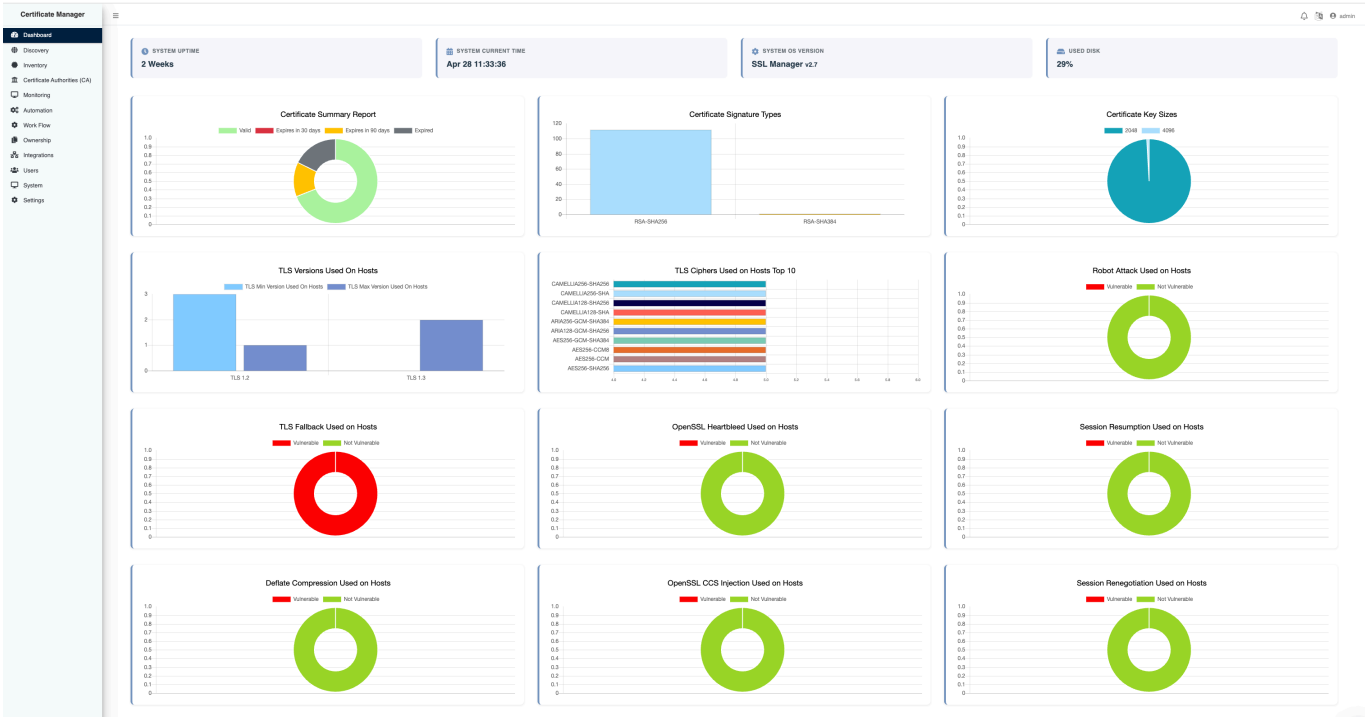
> **DEFAULT LOGIN CREDENTIALS**
>
> Default login credentials are used in the initial installation. For security, you must change these credentials after the first login.

Enter your login credentials:

- **Username**: `admin`
- **Password**: `admin`

4. Main Dashboard

After logging in, you will see the main dashboard. This screen provides a comprehensive view of your system.



SecTrail CM Main Dashboard - System Overview

On the dashboard, you can see:

- **System Metrics**: Uptime, current time, OS version, disk usage
- **Certificate Status Charts**: Valid/expiring/expired certificates
- **Security Charts**: TLS versions, cipher suites, security vulnerabilities
- **Left Menu**: Access to all platform features

> **DETAILED INFORMATION**
>
> For detailed explanations of all charts and metrics on the dashboard, please review the **Dashboard User Guide** page.

Left Menu - Main Navigation

You can access all platform features from the left menu:

Dashboard : Main screen and overall system status

Discovery : Discover new certificates

Inventory : Certificate inventory

Certificate Authorities (CA) : Certificate authorities management

Monitoring : Certificate monitoring and alerts

Automation : Manage automated tasks

Work Flow : Workflow management

Ownership : Certificate ownership

Integrations : Integrations

Users : User management

Certificate Discovery

Certificate Discovery is a powerful feature of SecTrail CM that automatically finds all SSL/TLS certificates in your infrastructure and adds them to inventory.

Overview

> **WHY IS CERTIFICATE DISCOVERY IMPORTANT?**
>
> Not knowing where certificates are used in organizations poses a major security risk. Expired or forgotten certificates can lead to service interruptions and security vulnerabilities.

Key Features

SecTrail CM's Certificate Discovery feature simplifies certificate management:

Feature	Description
Automatic Discovery	Automatically finds all certificates in your infrastructure
Centralized Inventory	Collects all certificates in a single centralized system
Regular Scanning	Keeps inventory up-to-date with scheduled scans
Fast Scanning	Scans large networks quickly and efficiently
Multiple Methods	Comprehensive discovery with network scanning and CT Logs

Discovery Methods

SecTrail CM offers two powerful discovery methods suitable for different scenarios:

1. Network Scanning

> **WHAT IS NETWORK SCANNING?**
>
> Network Scanning detects SSL/TLS certificates on devices in the network by scanning specified IP ranges or subnets.

How Does it Work?

The Network Scanning method detects active SSL/TLS connections by scanning IP ranges and ports you specify. Each certificate found is automatically added to inventory, and the scan is repeated at configured intervals to discover new certificates.

Use Cases

The Network Scanning method is used in the following scenarios:

- ** Server Infrastructure** - Regularly scan your entire server infrastructure
- ** Datacenter Scanning** - Scan a specific datacenter or subnet

- ** New Servers** - Automatically discover newly added servers
- ** Port-based Scanning** - Find services running on non-standard ports

2. Certificate Transparency Logs (CT Logs)

> **WHAT ARE CERTIFICATE TRANSPARENCY LOGS?**
>
> Certificate Transparency Logs are records of publicly issued certificates. Certificate Authorities (CAs) register the certificates they issue in these logs. This method is used for domain-based certificate discovery.

How Does it Work?

The Certificate Transparency Logs method scans public certificate authority (CA) records for the domain you specify. This way, you can discover all public certificates belonging to your organization that you may not be aware of. SecTrail CM uses trusted CT Log services like crt.sh and SSLMate.

Advantages

Advantage	Description
Public Certificates	Finds all publicly issued certificates
Unknown Certificates	Discovers certificates belonging to your organization that you didn't know about
Shadow IT	Detects certificates obtained by unauthorized departments
Subdomain Discovery	Finds all subdomain certificates linked to the main domain

Use Cases

The Certificate Transparency Logs method is used in the following scenarios:

- ** Public Certificates** - Discover all your internet-facing certificates
- ** Organization Inventory** - Scan all domains belonging to the organization
- ** Shadow IT Detection** - Find unauthorized certificates
- ** Subdomain Monitoring** - Track all subdomain certificates

3. Discovery from Integration Systems

> **WHAT IS INTEGRATION DISCOVERY?**
>
> Integration Discovery automatically discovers certificates in these systems by directly integrating with existing systems in your infrastructure (load balancer, web server, keystore, etc.). It provides real-time certificate inventory through API or protocol-based connections.

How Does it Work?

SecTrail CM automatically discovers all certificates in integrated systems by establishing secure API or protocol connections. After configuring integration, the system automatically scans at specified intervals and adds newly added or updated certificates to inventory.

Supported Integration Systems

SecTrail CM can perform automatic certificate discovery from the following systems:

- **F5 BIG-IP** - **Citrix NetScaler** - **FortiWeb** - **FortiGate** - **FortiManager**
- **NGINX / NGINX Plus** - **Palo Alto Networks** - **PaloAlto Panorama**
- **Apache** - **IIS** - **Apache Tomcat**
- **Windows TrustStore** - **Java Keystore (JKS)**
- **IBM DataPower** - **HashiCorp Vault**

Use Cases

Integration Discovery is used in the following scenarios:

- ** Configuration Management** - Centrally manage certificates on load balancers and web servers
- ** Keystore Monitoring** - Track certificates in Java Keystore and Windows TrustStore
- ** Automatic Synchronization** - Instantly capture changes in production systems
- ** Secret Management** - Discover certificates in secret management systems like HashiCorp Vault

> **INTEGRATION SETUP**
>
> Visit the Integrations page to set up integrations with supported systems.

Recommended Approaches

Recommendation	Description
⏲ **Regular Scanning**	Quickly capture new certificates by performing daily automatic scans
Test Environment	Test in a test environment before moving to production
⏱ **Proper Scheduling**	Run scans outside business hours (at night)

Considerations

Topic	Description
Network Load	Avoid large network scans during peak hours
Traffic Monitoring	Monitor network traffic during scanning
Firewall Rules	Ensure the ports SecTrail CM will scan are open
⏲ **Rate Limiting**	Don't open too many connections simultaneously, pay attention to rate limiting
Permissions	Obtain necessary permissions for networks you will scan

Discovery Operations

SecTrail CM offers both scheduled automatic discovery and instant manual discovery:

Automatic Discovery (Scheduled)

You can create discovery tasks that run automatically at specified intervals (daily or weekly). This way, new certificates in your infrastructure are continuously discovered and your inventory stays up-to-date.

Manual Discovery (Instant)

You can perform one-time quick scans without creating scheduled tasks. Useful when you add a new server or need urgent verification.

Get Started

- **User Guide: Discovery** - CA integration and configuration steps

Certificate Inventory

Certificate Inventory allows you to view, manage, and organize all your certificates from a central location.

Overview

Certificate Inventory features:

- Centralized certificate catalog
- Advanced search and filtering
- Tagging and grouping
- Detailed certificate information
- Visualization and reporting

Certificate Inventory Sources

Certificate Inventory collects and manages certificates from different sources in one central location. Your system automatically performs certificate discovery from the following sources:

Network Scanning

Certificates discovered through automatic scanning in your infrastructure:

- TLS/SSL certificates accessible via open ports
- Web servers, API gateways, load balancers
- Regular scans on specified IP ranges or domains
- Automatic discovery on specific port ranges (443, 8443, etc.)

Certificate Transparency Logs Scanning (CT Logs)

Certificates discovered from public certificate logs:

- CT log scanning for domains belonging to your organization
- Detection of incorrectly or unauthorized issued certificates
- Monitoring all certificates issued by public CAs

Certificates Signed Through Application

Certificates created and signed on the platform:

- Certificates created with Certificate Signing Request (CSR)
- Certificates signed through integrated CAs
- Self-signed certificates
- Internal CA certificates

Imported Certificates

Certificates manually added to the system:

- Certificates uploaded in PEM, DER, PFX/P12 formats
- Certificate chains transferred from external systems
- Certificates obtained from third-party CAs

Discovered from Integration Systems

Certificates automatically discovered through integrated systems:

- **F5 BIG-IP** - **Citrix NetScaler** - **FortiWeb** - **FortiGate** - **FortiManager**
- **NGINX / NGINX Plus** - **Palo Alto Networks** - **PaloAlto Panorama**
- **Apache** - **IIS** - **Apache Tomcat**
- **Windows TrustStore** - **Java Keystore (JKS)**
- **IBM DataPower** - **HashiCorp Vault**

> **ADDING INTEGRATION**
>
> Visit the Integrations page to add a new integration and follow step-by-step installation instructions.

Discovered Certificates List

> **WHAT ARE DISCOVERED CERTIFICATES?**
>
> This is a detailed list of all certificates found in your infrastructure as a result of Certificate Discovery operations. This list is updated after each discovery, and new certificates are automatically added.

Key Features

The Discovered Certificates list offers powerful features that simplify certificate management:

Feature	Description
Detailed Filtering	Ability to search separately for each column
Customizable View	Select the columns you want to see
Bulk Operations	Perform the same operation on multiple certificates simultaneously
Export	Export selected certificates in different formats
Quick Access	Instant access to critical information like last seen time, port, type

Provided Information

In the certificate inventory, basic information for each certificate is presented in list view. When you click on a certificate, you can access all the details of the certificate.

Information Displayed in List View

Information	Description
Last Seen	When the certificate was last seen
Server	Server address where the certificate is located
Port	Port number on which the certificate is running
Type	Discovery method (Network Scanning, CT Logs, Import, Integration, Manual)
Subject	Certificate owner information (CN, OU, O)
Not Before	Certificate validity start date
Not After	Certificate validity end date

Detailed View

SecTrail CM parses certificates and stores all information. In detailed view, you can access all fields in the X.509 standard (Subject, Issuer, Serial Number, Public Key, Extensions, Fingerprint, Certificate Chain, etc.) along with discovery source, related systems, and usage history.

Bulk Operation Capabilities

Bulk operations that can be performed from the list:

- [OK] **Change Status** - Bulk update status of selected certificates
- **Export** - Export selected certificates (CSV, Excel, PDF)
- **Delete** - Clean up certificates no longer in use
- **Create Signing Request** - Generate signing request (CSR) for renewal

Get Started

- **User Guide: Inventory** - CA integration and configuration steps

Certificate Monitoring

SecTrail CM monitors your certificates 24/7 continuously and prevents service interruptions by detecting issues in advance.

> **WHY IS CERTIFICATE MONITORING IMPORTANT?**
>
> An expired certificate can cause critical services to crash, resulting in revenue loss and reputation damage. With proactive monitoring, you can detect and prevent issues in advance.

Overview

SecTrail CM's certificate monitoring system continuously checks the health of your certificates and creates automatic alarms for critical situations.

Key Features

- ⏱ **24/7 Monitoring** - Continuous automatic certificate status checks
- **Proactive Detection** - Early warning before problems occur
- **Centralized Dashboard** - View all certificate statuses from a single screen
- **Smart Alarms** - Customizable thresholds and notifications
- **Trend Analysis** - Certificate lifecycle and usage statistics

Monitoring Metrics

SecTrail CM collects and analyzes comprehensive metrics for your certificates:

Expiration Monitoring

Track certificate expiration dates to ensure timely renewal:

- **Expiration Date** - Certificate expiration date
- **Days Until Expiration** - Number of days until expiration
- **Expiration Status** - Valid, Expiring Soon, Expired
- **Renewal Window** - Recommended renewal time

> **RENEWAL RECOMMENDATIONS**
>
> - 90+ days: Start planning
> - 30-90 days: Initiate renewal process
> - 7-30 days: Urgent renewal required
> - 0-7 days: Critical situation!

Certificate Validity

Validate technical validity of certificates:

- **Signature Verification** - Signature accuracy check
- **Key Usage** - Key usage purpose compliance
- **Extended Key Usage** - Extended key usage check
- **Basic Constraints** - Basic constraints validation

Chain Validation

Verify certificate chain integrity:

- **Chain Integrity** - Existence of all intermediate certificates
- **Root CA Trust** - Whether root CA is trusted
- **Chain Order** - Correctness of chain ordering
- **Cross-Signing** - Cross-signing status

Security Scoring

Evaluate certificate security levels:

Criterion	Evaluation
Key Size	2048+ bit RSA or 256+ bit ECC recommended
Signature Algorithm	SHA-256 or stronger recommended
TLS Version	TLS 1.2+ recommended, TLS 1.0/1.1 insecure
Cipher Suites	Use of strong cipher suites
Security Score	Overall security score from A+ to F

> **SECURITY WARNINGS**
>
> - MD5 or SHA-1 signed certificates are now considered insecure
> - 1024 bit RSA keys are insufficient
> - SSL 3.0, TLS 1.0, and TLS 1.1 protocols should no longer be used

Alarm Mechanism

SecTrail CM continuously monitors certificate statuses and creates automatic alarms for critical situations.

Alarm Types

SecTrail CM creates different alarm levels for different situations:

Alarm Level	Status	Example
Critical	Immediate action required	Certificate expired or will expire within 7 days
Warning	Attention required	Certificate will expire within 7-30 days
Info	Information	Certificate will expire within 30-90 days
OK	No issues	Certificate is valid and healthy

Alarm Triggers

The following situations create alarms:

- ⏰ **Expiration Approaching** - Based on defined threshold values
- **Security Issue** - Weak algorithm or key size

Notification Channels

> **MULTIPLE NOTIFICATION CHANNELS**
>
> You can use multiple notification channels simultaneously for certificates that have entered alarm status.

SecTrail CM supports the following notification channels:

Email Notifications

The most commonly used notification method:

- Automatic email delivery to relevant teams or users
- Direct action links
- Group or individual notifications
- Customizable email templates

SNMP Trap

For enterprise monitoring systems:

- Integration with centralized monitoring systems
- SNMPv2c and SNMPv3 support
- Customizable trap messages

Ownership Management

> **SMART ALARM ROUTING**
>
> You can use a flexible ownership model to ensure alarms reach the right people and teams.

SecTrail CM offers a two-level ownership model:

Server-based Ownership

Responsibility assignment at the server level:

Advantages:

- All certificates on a single server are routed to the same team
- Organization based on infrastructure responsibility
- Easy bulk management

Certificate-based Ownership

Define custom ownership for each certificate:

Advantages:

- Granular control and responsibility
- Domain-based organization
- Custom application ownership

Ownership Priority

Priority order in case of ownership conflict:

1. **Certificate-based Ownership**
2. **Server-based Ownership**
3. **Default Ownership**

> **BEST PRACTICE**
>
> For critical certificates, you can provide dual-layer notifications by defining both certificate-based and server-based ownership.

Reporting and Analysis

Monitoring Reports

SecTrail CM generates regular monitoring reports:

- **Daily Status Report** - Daily certificate status summary
- **Weekly Trend Analysis** - Weekly changes and trends
- **Monthly Compliance Report** - Compliance and security status
- **Custom Reports** - Customized reports based on needs

Dashboard and Visualization

- **Real-time Dashboard** - Instant certificate status
- **Expiration Timeline** - Expiration calendar view
- **Alarm History** - Historical alarms and interventions

Get Started

- **User Guide: Monitoring** - CA integration and configuration steps

Certificate Authority (CA)

SecTrail CM enables you to centrally manage your organization's Certificate Authority (CA) infrastructure.

> **WHY IS CA MANAGEMENT IMPORTANT?**
>
> Modern organizations use both internal and external CAs. Scattered CA management across different systems creates security vulnerabilities and operational complexity. SecTrail CM allows you to manage all your CAs from a single platform.

Key Features

SecTrail CM's CA management features include:

Multi-CA Management

Manage different CA providers from a single platform:

- **Local CA** - For internal certificate needs (ADCS, HashiCorp Vault)
- **External CA** - Trusted certificates for internet-facing systems (DigiCert, GlobalSign)
- **Hybrid Environments** - Ability to use multiple CAs simultaneously
- **Centralized Control** - Manage all CAs from a single interface

Certificate Request Management

Automate certificate request processes:

- **Certificate Signing Request (CSR)** - Automatic certificate signing request generation
- **Template Support** - Create standard certificate profiles
- **Bulk Operations** - Request multiple certificates simultaneously
- **Approval Processes** - Workflow-based certificate approval mechanism

Automated Lifecycle Management

Automatically manage your certificates:

Automatic Renewal Automatically renew certificates before they expire. The system automatically initiates renewal operations based on the threshold values you define.

Flexible Thresholds Ability to customize renewal scheduling. You can define different renewal policies for each certificate type or environment.

Smart Notifications Receive automatic alerts for critical events. Instant notifications for renewal failures, approaching expirations, and other important situations.

Seamless Transition Zero-downtime certificate updates. Perform certificate renewal operations in your production environments without experiencing interruptions.

Secure Key Management

Securely store your private keys:

- **Hardware Security Module (HSM) Support** - Highest security level with hardware security module integration
- **Encrypted Storage** - Comprehensive data protection with encryption at rest and in transit
- **Key Rotation** - Maintain security standards with periodic key renewal
- **Access Control** - Prevent unauthorized use with role-based key access

Centralized Monitoring and Reporting

Track all CA operations:

- **Detailed Audit Logs** - Recording every operation and historical tracking
- **Performance Metrics** - CA usage statistics and analytics
- **Alarms and Notifications** - Automatic alerts for abnormal situations

Supported CA Providers

> **EXTENSIVE CA SUPPORT**
>
> SecTrail CM integrates with industry-standard CA systems. Whether you use enterprise, public, or ACME protocol CAs - manage them all from a single platform.

Category	CA Provider	Use Case	Key Features
** Enterprise CA**	Microsoft AD CS	Enterprise Windows PKI	Windows integration, template support, auto-enrollment
	HashiCorp Vault PKI	Cloud-native & DevOps	Dynamic secrets, short-lived certificates, Kubernetes support
** External CA**	DigiCert	Public SSL/TLS certificates	OV/EV/DV certificates, CertCentral API, IoT/code signing
	GlobalSign	Internationally trusted CA	SSL/TLS, code signing, Atlas Platform integration
** ACME CA**	Let's Encrypt	Free automatic SSL	Domain validation, wildcard support, 90-day automatic renewal
	ZeroSSL	Let's Encrypt alternative	Free SSL, automatic validation
	Buypass	Free CA option	ACME protocol, Norway-based trusted CA
	Google Trust Services	GCP optimized	Optimized for Google Cloud Platform
	SSL.com	ACME commercial CA	Various certificate types, ACME support

Security and Compliance

> **SECURITY AND COMPLIANCE**
>
> SecTrail CM supports the highest security and compliance standards in certificate management.

Integration and Automation

> **API AND AUTOMATION**
>
> With SecTrail CM's powerful API, you can automate all your CA operations and integrate them into your DevOps processes.

API Features

SecTrail CM offers comprehensive API support for CA management.

Automation Scenarios

- **Automatic Certificate Request** - Generate signing request (CSR) and send to CA
- **Automatic Renewal** - Renew certificates before expiration
- **Automatic Deployment** - Automatic deployment of new certificates
- **Automatic Revocation** - Certificate revocation when necessary
- **Automatic Monitoring** - Monitor certificate statuses

Get Started

- **User Guide: CA Management** - CA integration and configuration steps

System Integrations

SecTrail CM automates certificate management by directly integrating with critical systems in your enterprise infrastructure.

> **WHY IS SYSTEM INTEGRATION IMPORTANT?**
>
> Manual certificate deployment is time-consuming, error-prone, and risky. With automatic integrations, certificate exchange processes are performed securely and quickly without human intervention.

Overview

SecTrail CM's System Integrations module automates one of the most critical stages of certificate lifecycle management: **certificate deployment and exchange** processes. The platform ensures secure certificate updates by establishing **agentless** connections to target systems.

Key Features

Feature	Description
Automatic Deployment	Renewed certificates are automatically deployed to relevant systems
Agentless Architecture	Integration without requiring agent installation on target systems
Secure Communication	Connection through secure protocols like SSH, HTTPS, WinRM
⏮ Rollback Support	Automatic rollback to previous certificate in case of error
Multi-platform	Load balancer, firewall, web server, and application server support

Supported Integrations

SecTrail CM integrates with leading load balancer, firewall, web server, and application server platforms in the industry.

Load Balancer and Application Delivery Controller (ADC)

Platform	Use Cases
F5 BIG-IP	Load balancing, SSL offload, high availability
Citrix NetScaler (ADC)	Application delivery, remote access gateway, SSL offload

Firewall and Security

Platform	Use Cases
Palo Alto Networks	SSL inspection, forward proxy, GlobalProtect
Fortinet FortiWeb	Web application firewall, OWASP protection

Web Servers

Platform	Use Cases
NGINX	Reverse proxy, API gateway, microservices
Apache HTTP Server	Traditional web server, PHP applications
IIS	Windows environments, ASP.NET, SharePoint

Application Server

Platform	Use Cases
Apache Tomcat	Java web applications, Spring Boot
Java Keystore (JKS)	Java applications, Kafka, Elasticsearch

Certificate Store

Platform	Use Cases
Windows Certificate Store	Windows servers, domain environments, Active Directory

Automatic Certificate Exchange Process

SecTrail CM fully automates the certificate exchange process and provides **error checking** and **rollback support** at each step:

Step	Stage	Operation	In Case of Error
1□	**Connection**	Secure connection to target system (SSH/WinRM/API) and access control	[!] **Operation canceled**, send notification
2□	**Backup**	Backup of existing certificate (certificate + key + config)	[!] **Stop operation**, safe exit
3□	**Deployment**	Secure transfer of new certificate files to target system	**Restore old certificate**
4□	**Configuration**	Certificate configuration update	**Restore from backup**
5□	**Service Update**	Service reload	**Restart with old certificate**
6□	**[x] Validation**	SSL/TLS connection and accessibility test	**Complete rollback**
7□	**Notification**	Success/error status reporting, audit log recording, dashboard update	[OK] **Rollback notification sent**

> **AUTOMATIC ROLLBACK GUARANTEE**
>
> If an error is detected at any step, the system automatically returns to the previous working state. The old certificate is preserved, and no service interruption occurs.

Integration Advantages

Operational Efficiency

Advantage	Description
⏱ **Time Savings**	Minutes instead of hours by automating manual operations
Error Minimization	99.9%+ success rate by eliminating human errors
24/7 Operation	Automatic certificate renewal outside business hours
Scalability	Simultaneous certificate deployment to hundreds of systems

Security

Advantage	Description
⏰ **Timely Renewal**	Eliminate expired certificate risk
Centralized Control	Single-point management of all certificates
Secure Communication	Secure protocols like SSH, TLS, WinRM
Audit Trail	Detailed recording of every operation

Get Started

- **User Guide: CA Management** - CA integration and configuration steps

Certificate Workflow

SecTrail CM's Certificate Workflow module automates the certificate lifecycle from end to end, minimizing manual intervention.

> **WHY IS WORKFLOW AUTOMATION IMPORTANT?**
>
> Manual certificate renewal and deployment processes create forgotten renewal dates, interruption risks, and operational overhead. With automatic workflows, certificates are renewed before expiration and deployed to systems seamlessly.

Overview

SecTrail CM's Workflow module manages the **automatic renewal**, **approval**, and **deployment to target systems** processes of certificates. A customizable workflow can be defined for each discovered certificate, and the entire process can be automated from end to end.

Automatic Workflow Process

SecTrail CM fully automates the certificate renewal process and records every step:

Stage	Description
Discovery and Monitoring	Certificates detected by the Certificate Discovery module are continuously monitored
⏰ **Automatic Trigger**	Workflow is initiated based on defined threshold values
Authority Selection	CA selection based on existing authority or policies and integration status check
[OK] **Approval Mechanism**	Optional manual checkpoint (recommended for production)
Certificate Request	Automatic communication with CA and certificate acquisition
Automatic Deployment	Deployment to target systems (web servers, load balancers, firewalls, cloud platforms)
[x] **Validation & Notification**	SSL/TLS tests, accessibility checks, and reporting

> **ROLLBACK SUPPORT**
>
> Error checking is performed at each step, and automatic rollback is performed if necessary.

Workflow Advantages

Operational Efficiency

Advantage	Description
⏱ **Time Savings**	Reduce labor costs by automating manual processes
Error Minimization	99.9%+ success rate by eliminating human errors
24/7 Automatic Operations	Continuous certificate management outside business hours
Scalability	Simultaneous workflow management for hundreds of certificates

Security and Compliance

Advantage	Description
⏰ **Timely Renewal**	Completely eliminate expired certificate risk
Complete Audit Trail	Detailed recording of every operation
Centralized Control	Single-point management of all workflows

Workflow Configuration

SecTrail CM allows you to create customized workflow templates for different certificate groups:

- **Renewal Thresholds**: Custom trigger times based on certificate type
- **Approval Rules**: Multi-layer approval mechanisms for critical systems
- **Deployment Targets**: System groups for automatic deployment
- **Notification Settings**: Email, SNMP Trap
- **Rollback Policies**: Automatic or manual rollback on error

Get Started

- **User Guide: Workflow** - CA integration and configuration steps

RBAC and Authorization

SecTrail CM offers a secure and flexible authorization system with enterprise-level **Role-Based Access Control (RBAC)**. Centrally manage all security layers from user management to permission control.

WHY RBAC?

Certificate management is a sensitive operation. Wrong people performing critical operations can lead to security breaches. With RBAC, you ensure that each user has only the permissions appropriate for their role.

CORE PRINCIPLES

- **Least Privilege** - Users are given only the minimum permissions they need
- **Separation of Duties** - Critical operations are distributed among different roles
- **Defense in Depth** - Multi-layered security control is provided

Key Features

Flexible User Management

SecTrail CM supports multiple user sources to meet different enterprise needs:

Active Directory (AD) / LDAP Integration

Use your existing enterprise identity infrastructure:

- **Automatic Synchronization** - User information is automatically updated
- **Group-based Management** - Map AD groups directly to roles
- **Centralized User Management** - User addition/removal is done in AD

Local User Accounts

Independent user management:

- For external consultants and temporary users
- Alternative for users without AD access
- Customizable password policies
- Manual user creation and management

Hybrid Management

You can use both methods simultaneously. For example, employees can log in with AD while external consultants can use local accounts.

Role-Based Access Control (RBAC)

Powerful and flexible role management system:

Hierarchical Role Structure

- **System Roles** - Immutable predefined roles

- **Custom Roles** - Create roles specific to your organization
- **Role Inheritance** - Roles inheriting permissions from each other

Granular Permission Control

Separate permission definition for each operation (CRUD + Execute model):

Permission	Description	Example
Create	Add new resource	Create new certificate request
Read	View information	View certificate details
Update	Modify existing resource	Update certificate information
Delete	Remove resource	Delete certificate or CA
Execute	Trigger operation	Certificate renewal, deployment

Organization and Group Management

User Groups

Organize users:

- **Department-based** - IT, DevOps, Security, Network teams
- **Project-based** - Teams for specific projects
- **Region/Location-based** - Istanbul, Ankara, Izmir offices
- **Bulk Role Assignment** - Automatic role distribution to groups

Dynamic Membership

Automatic group membership management:

- **AD Group Synchronization** - Active Directory groups are automatically synchronized
- **Rule-based Assignment** - Automatic group membership based on user attributes
- **Attribute Filtering** - Filtering based on attributes like department, title, location

Detailed Audit and Monitoring

Record all authorization operations and meet compliance requirements:

User Activity Log

Monitor all user interactions:

- [OK] Who logged into the system when?
- [OK] What operations were performed?
- [OK] Which resources were accessed?
- [OK] Failed login attempts
- [OK] IP address and user agent information

Role and Permission Changes

Track authorization changes:

- **Role Assignment/Removal** - Who assigned/removed which role to whom, when?
- **Permission Changes** - Which permissions were added/removed?
- **Group Membership Changes** - Complete history of group memberships
- **Change Author Information** - The person who made each change is recorded

Compliance Reports

Audit and compliance reports:

- **User Access Rights** - Report of each user's permissions
- **Active/Inactive User List** - User analysis by usage status
- **Last Login Times** - User activity tracking
- **Permission Change History** - Changes made within a specific date range
- **Privileged User Report** - List of highly authorized users

---

Predefined Roles

SecTrail CM offers ready-made roles for quick setup:

Role	Description	Basic Permissions	Use Case
Admin	System administrator with all permissions	- All modules: full access - User management - System settings - Role definition	For system administrators and IT leaders
API	System user for API access	- Certificates: read, execute - Integrations: execute - API: full access	For automation and integration systems

> **CUSTOM ROLE DEFINITION**
>
> These roles meet basic needs. You can create new roles based on your organization's special requirements or customize by cloning existing roles.

Use Cases

Scenario 1: Department-based Access

Situation: IT department manages all certificates while DevOps team only sees and can renew certificates for their own projects.

Solution:

- IT team is assigned the `Certificate Manager` role
- A custom `DevOps Certificate Operator` role is created for DevOps team
- Access is restricted with project-based tags

```
Roles:
├── IT Team -> Certificate Manager (all certificates)
└── DevOps Team -> DevOps Certificate Operator (only tag:project=devops)
```

[OK] Scenario 2: Approval Mechanism

Situation: Junior employees can create certificate requests but cannot deploy certificates to production environment without manager approval.

Solution:

- Juniors get the `Certificate Requester` role (create, read permissions)
- Managers get the `Certificate Approver` role (execute, deploy permissions)
- Approval mechanism is set up with workflow system

```
Workflow:
1. Junior -> Creates certificate request (create)
2. Manager -> Reviews and approves request (approve)
3. System -> Deploys approved certificate (execute)
```

Scenario 3: External Consultant Access

Situation: Temporary consultant workers can be given limited-time and read-only access to specific certificates.

Solution:

- Local user account is created (outside AD)
- `External Auditor` role is assigned (read-only permissions)
- Account expiration date is set
- Access is restricted to specific certificate groups

```
Consultant Profile:
├── User Type: Local (outside AD)
├── Role: Certificate Viewer (read-only)
├── Access Duration: 90 days
└── Restriction: Only "Production-Web" certificates
```

Scenario 4: Multi-Tenant Structure

Situation: Different companies or business units can use the same platform but cannot access each other's data.

Solution:

- Separate organization is defined for each company/unit
- Organization-based data isolation is provided
- Users access only their organization's data

```
Organization Structure:
├── Company A
│ ├── Users: user1@companyA.com, user2@companyA.com
│ └── Certificates: *.companyA.com
```

```
├── Company B
│ ├── Users: user1@companyB.com, user2@companyB.com
│ └── Certificates: *.companyB.com
└── Company C
 ├── Users: user1@companyC.com
 └── Certificates: *.companyC.com
```

MORE INFORMATION

Review the User Guide: RBAC Management page for user management and role configuration.

Introduction

SecTrail CM offers two main integration categories to automate every phase of the certificate lifecycle: **Certificate Authority (CA)** integrations and **System Integrations**.

Integration Types

Certificate Authority (CA) Integrations

CA integrations automate certificate **acquisition** and **renewal** processes. SecTrail CM works seamlessly with both public and private certificate authorities, fully automating certificate requests, approval processes, and certificate acquisition.

Key Features:

- Automatic certificate request and approval process
- Automatic renewal
- Multi-CA support
- Template-based request management
- API-based secure communication

Supported CA Types:

CA Type	Integrations
Public CA	DigiCert, GlobalSign
Private CA	Microsoft ADCS, HashiCorp Vault
ACME	Let's Encrypt, ZeroSSL

System Integrations

System integrations automate the **deployment** and **management** of certificates obtained from CAs to target systems. They establish secure connections to load balancers, firewalls, web servers, and application servers using an agent-less architecture to automatically perform certificate exchanges.

Key Features:

- Agent-less architecture
- Secure protocols (SSH, WinRM, HTTPS API)
- Automatic rollback support
- Post-deployment validation
- Detailed audit logs

Supported System Categories:

Category	Integrations
Load Balancer	F5 BIG-IP, Citrix NetScaler
Firewall	Palo Alto, PaloAlto Panorama, Fortinet FortiWeb, FortiGate, FortiManager
Web Server	NGINX, Apache, IIS
App Server	Tomcat, Java Keystore
Certificate Store	Windows Trust Store

GlobalSign

SecTrail CM integrates with the GlobalSign ManagedSSL service to centrally manage ordering, renewal, and revocation of SSL/TLS certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	SOAP API (HTTPS)	GlobalSign ManagedSSL API is used
API Endpoint	`https://system.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl`	ManagedSSL SOAP service
Authentication	Basic Authentication	Authentication with Username and Password
User Permission	ManagedSSL API Access	Certificate order, query, and management permission

Automatic Operations

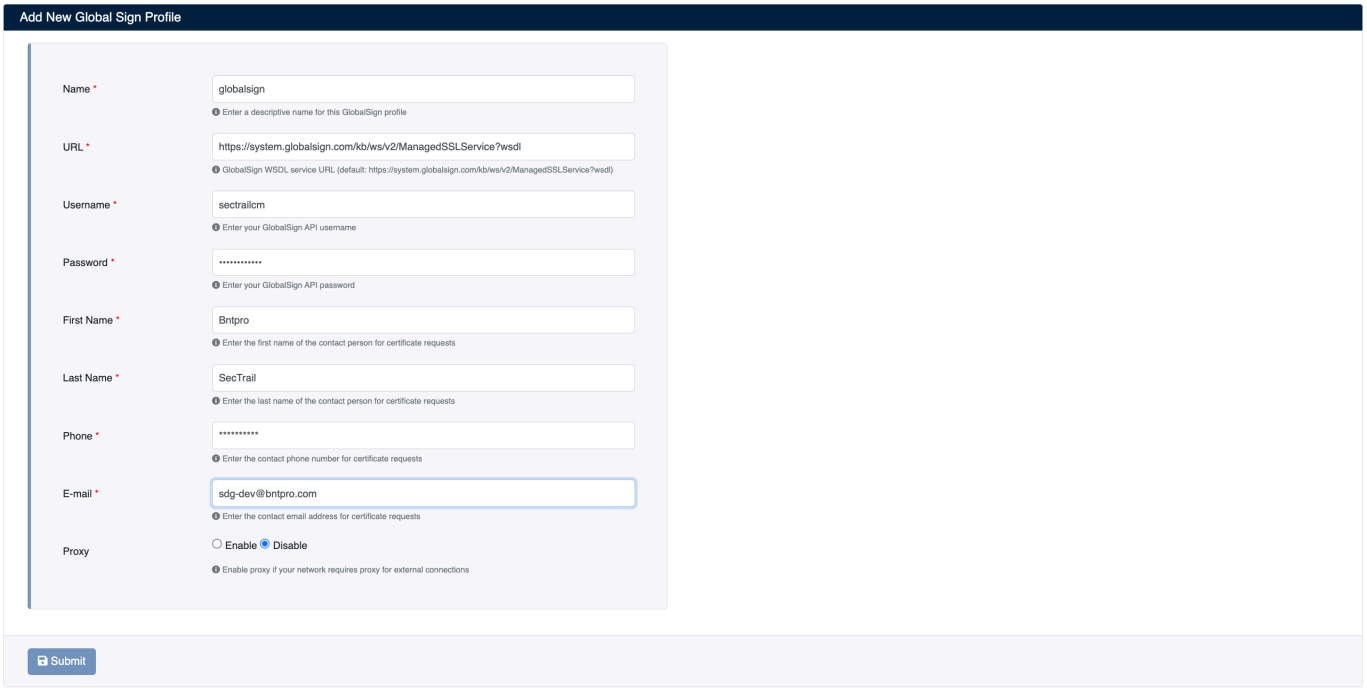
SecTrail CM automatically performs the following operations on GlobalSign:

1. **Certificate Order**: Creating a new SSL/TLS certificate request
2. **Order Query**: Viewing the status of existing certificate orders
3. **Certificate Renewal**: Renewing certificates about to expire
4. **Certificate Revocation**: Revoking certificates that are no longer used or compromised

Configuration Steps

1. Add GlobalSign Profile

Navigate to **Certificate Authorities (CA) > GlobalSign > Accounts** and click the **Add New Global Sign Profile** button:



Enter the following information:

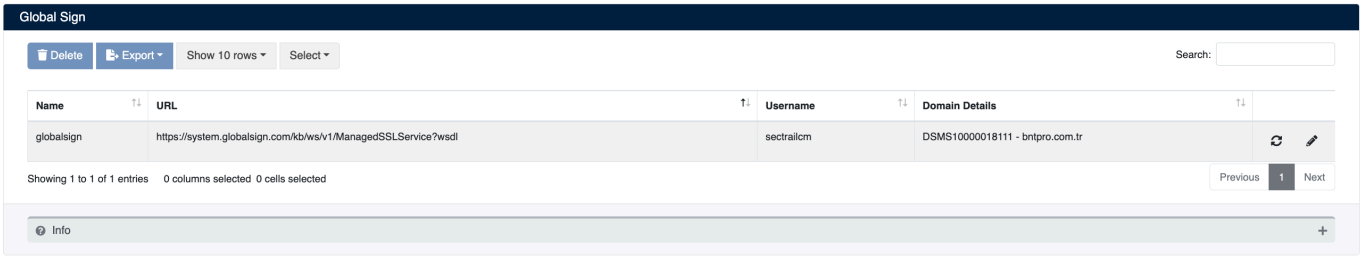
- **Name**: Give a descriptive name for the profile
- **URL**: GlobalSign ManagedSSL API endpoint address
- `https://system.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl`
- **Username**: Your GlobalSign API username
- **Password**: Your GlobalSign API password
- **Proxy**: Proxy usage (Enable/Disable). After enabling the proxy, complete your proxy configuration from **Settings -> Proxy** settings.

Click **Submit** button to save the profile.

> **CONTACT INFORMATION**
>
> GlobalSign will use the specified contact information for certificate operations. Ensure this information is accurate and up-to-date.

2. View GlobalSign Accounts

After adding a profile, it will be displayed in the **Certificate Authorities (CA) > GlobalSign > Accounts** list:



The list screen displays the following information:

- **Name**: Profile name

- **URL**: API endpoint address
- **Username**: Username
- **Domain Details**: Associated domain information

Account Operations

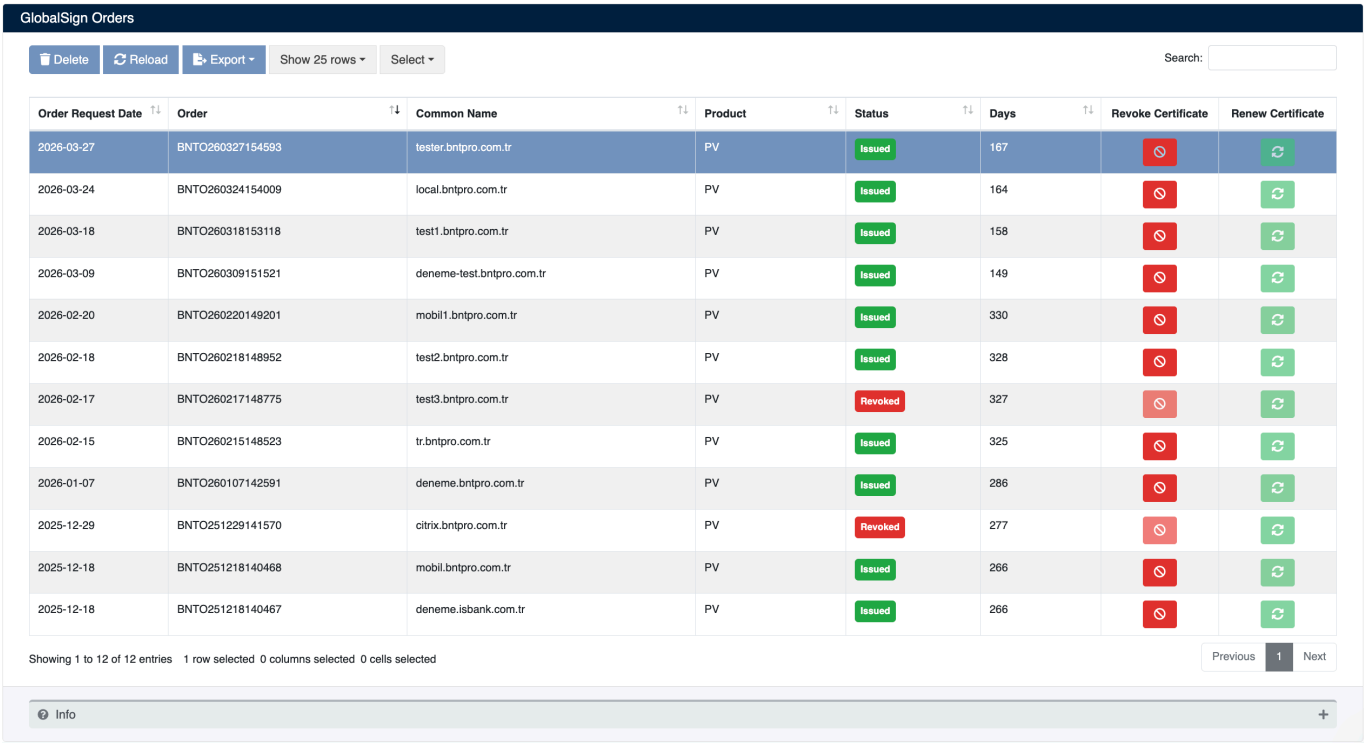
The following operations can be performed for each profile:

- **Refresh** (): Refresh profile information
- **Edit** (): Edit profile settings
- **Delete** (): Delete profile

View Certificate Orders

After GlobalSign integration, you can view all your certificate orders:

Navigate to **Certificate Authorities (CA) > GlobalSign > Orders**:



Order Information

Field	Description
Order Request Date	Certificate request date
Order	GlobalSign order number
Common Name	Domain name where the certificate will be used
Product	Certificate product type
Status	Certificate status (Issued, Pending, etc.)
Days	Remaining validity period (days)

Certificate Statuses

- **Issued** : Certificate successfully issued and active
- **Pending** : Order is being processed
- **Revoked** : Certificate revoked
- **Expired** : Certificate expired

Certificate Management

Certificate Renewal (Renew)

To renew certificates about to expire:

1. Navigate to **Certificate Authorities (CA) > GlobalSign > Orders**
2. Find the certificate you want to renew
3. Click **Renew Certificate** button (green icon)
4. Confirm the renewal

> **RENEWAL TIMING**
>
> It is recommended to start renewing certificates at least 30 days before the expiration date.

Certificate Revocation (Revoke)

To revoke compromised or no longer used certificates:

1. Navigate to **Certificate Authorities (CA) > GlobalSign > Orders**
2. Find the certificate you want to revoke
3. Click **Revoke Certificate** button (red icon)
4. Confirm the revocation

> **REVOCATION PROCESS**
>
> Once a certificate is revoked, this action cannot be undone. A revoked certificate can no longer be used.

DigiCert

SecTrail CM integrates with the DigiCert API service to centrally manage ordering, renewal, and revocation of SSL/TLS certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	REST API (HTTPS)	DigiCert REST API is used
API Endpoint	`https://www.digicert.com/services/v2/`	DigiCert API v2 service
Authentication	API Key Authentication	Authentication with API Key
User Permission	DigiCert API Access	Certificate order, query, and management permission

Automatic Operations

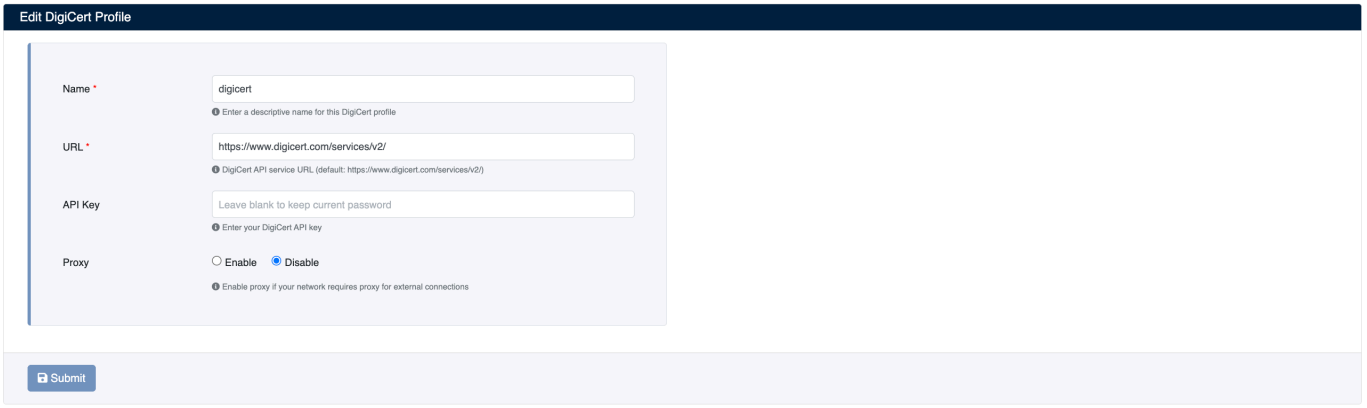
SecTrail CM automatically performs the following operations on DigiCert:

1. **Certificate Order**: Creating a new SSL/TLS certificate request
2. **Order Query**: Viewing the status of existing certificate orders
3. **Certificate Renewal**: Renewing certificates about to expire
4. **Certificate Revocation**: Revoking certificates that are no longer used or compromised
5. **Certificate Download**: Automatic downloading of issued certificates

Configuration Steps

1. Add DigiCert Profile

Navigate to **Certificate Authorities (CA) > DigiCert > Accounts** and click the **Add New DigiCert Profile** button:



Enter the following information:

- **Name**: Give a descriptive name for the profile

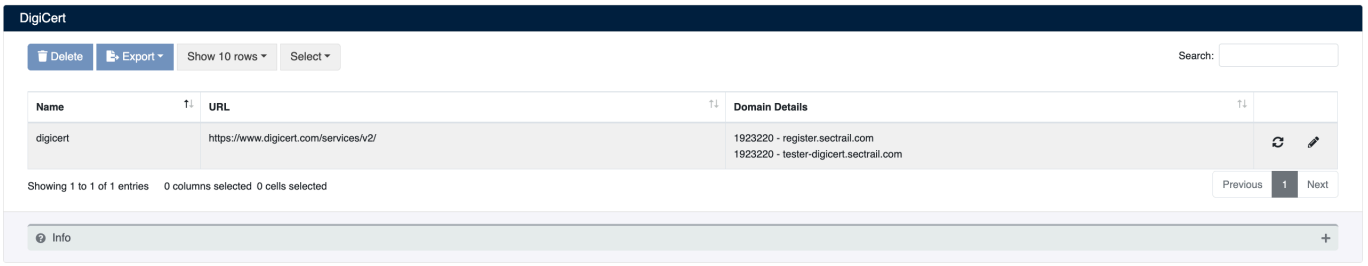
- **URL**: DigiCert API endpoint address
- `https://www.digicert.com/services/v2/`
- **API Key**: Your DigiCert API key
- **Proxy**: Proxy usage (Enable/Disable). After enabling the proxy, complete your proxy configuration from **Settings -> Proxy** settings.

Click **Submit** button to save the profile.

> **API KEY**
>
> You can create your DigiCert API key from the DigiCert account management panel. Ensure that the API key has sufficient permissions.

2. View DigiCert Accounts

After adding a profile, it will be displayed in the **Certificate Authorities (CA) > DigiCert > Accounts** list:



The list screen displays the following information:

- **Name**: Profile name
- **URL**: API endpoint address
- **Domain Details**: Associated domain information

Account Operations

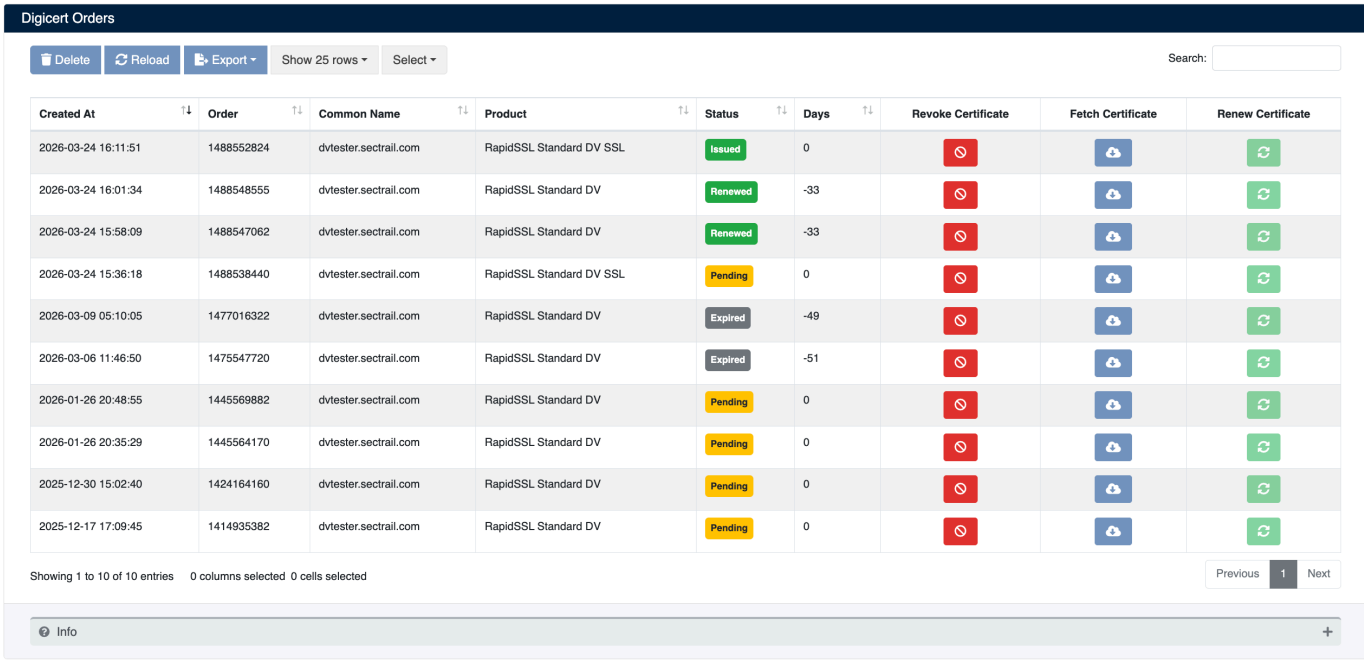
The following operations can be performed for each profile:

- **Refresh**: Refresh profile information
- **Edit**: Edit profile settings
- **Delete**: Delete profile

View Certificate Orders

After DigiCert integration, you can view all your certificate orders:

Navigate to **Certificate Authorities (CA) > DigiCert > Orders**:



Order Information

Field	Description
Created At	Certificate request date and time
Order	DigiCert order number
Common Name	Domain name where the certificate will be used
Product	Certificate product type (e.g., RapidSSL Standard DV)
Status	Certificate status (Issued, Expired, Renewed, Revoked)
Days	Remaining/elapsed validity period (in days)

Certificate Statuses

- **Renewed**: Certificate renewed and active
- **Expired**: Certificate expired (negative day value)
- **Revoked**: Certificate revoked
- **Issued**: Certificate successfully issued and active

Certificate Management

Download Certificate (Fetch)

To download issued certificates:

1. Navigate to **Certificate Authorities (CA) > DigiCert > Orders**
2. Find the certificate you want to download
3. Click **Fetch Certificate** button
4. Certificate is automatically downloaded and added to the system

AUTOMATIC DOWNLOAD

Certificates issued by DigiCert can be automatically downloaded to the system. This feature eliminates the need for manual downloading.

Certificate Renewal (Renew)

To renew certificates about to expire:

1. Navigate to **Certificate Authorities (CA) > DigiCert > Orders**
2. Find the certificate you want to renew
3. Click **Renew Certificate** button
4. Confirm the renewal

RENEWAL TIMING

It is recommended to start renewing certificates at least 30 days before the expiration date. Negative values in the "Days" column indicate expired certificates.

Certificate Revocation (Revoke)

To revoke compromised or no longer used certificates:

1. Navigate to **Certificate Authorities (CA) > DigiCert > Orders**
2. Find the certificate you want to revoke
3. Click **Revoke Certificate** button
4. Confirm the revocation

REVOCATION PROCESS

Once a certificate is revoked, this action cannot be undone. A revoked certificate can no longer be used.

Microsoft ADCS

SecTrail CM integrates with Microsoft Active Directory Certificate Services (ADCS) to enable automatic requesting and management of enterprise SSL/TLS certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	HTTPS	Certificate Enrollment Web Service is used
Port	`443` (default)	Standard HTTPS port
Authentication	NTLM / Kerberos authentication	Windows authentication
User Permission	Certificate request and enrollment	Certificate request and enrollment permission

Automatic Operations

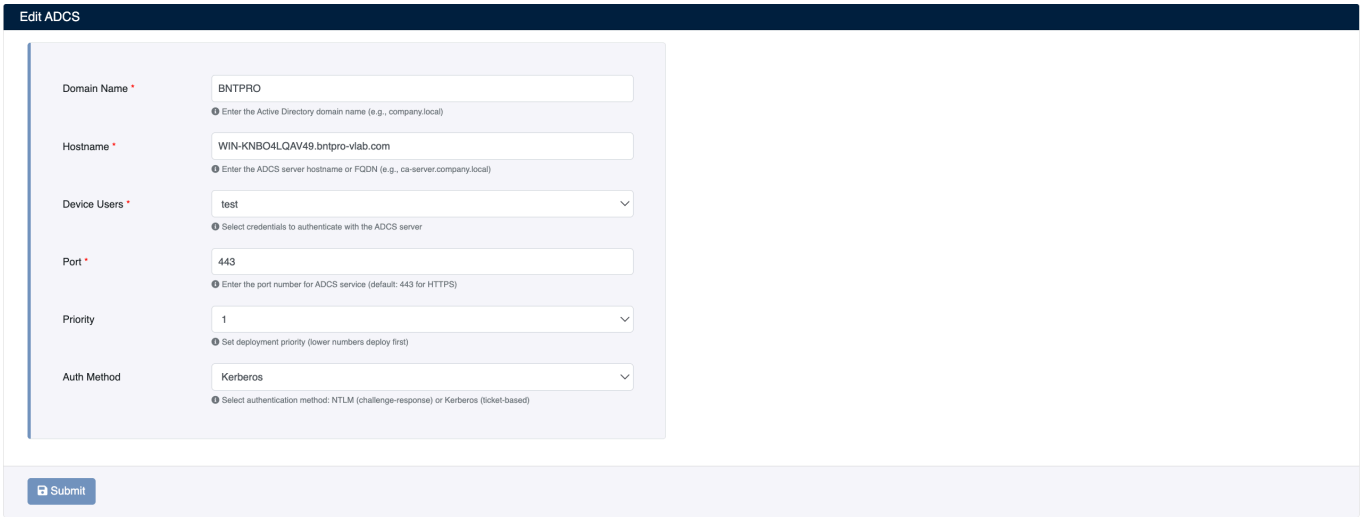
SecTrail CM automatically performs the following operations on Microsoft ADCS:

1. **Certificate Request**: CSR submission
2. **Certificate Enrollment**: Certificate issuance through ADCS
3. **Template Management**: Using different certificate templates
4. **Automatic Approval**: Automatic approval for configured templates
5. **Pending Order Tracking**: Tracking certificates awaiting CA manager approval

Configuration Steps

1. Add ADCS Service

Navigate to **Certificate Authorities (CA) > ADCS > Accounts** and click the **Add New ADCS Service** button:



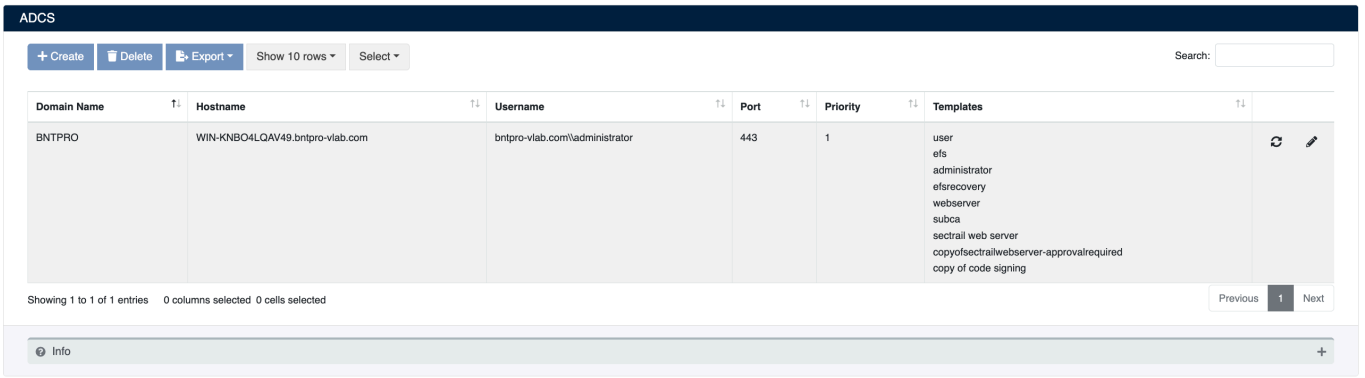
Enter the following information:

- **Domain Name**: Active Directory domain name
- **Hostname**: Hostname of the ADCS server
- **Username**: Username for ADCS access. You can create a user from **Automation > Device Users** and select it here.
- **Port**: ADCS Web Enrollment service port (default: 443)
- **Priority**: Service priority level (between 1-10)
- **Auth Method**: Authentication method (NTLM / Kerberos)

Click **Submit** button to save the service.

2. View ADCS Services

After adding a service, it will be displayed in the **Certificate Authorities (CA) > ADCS > Accounts** list:



The list screen displays the following information:

Domain Name: The Active Directory domain name that SecTrail CM connects to when submitting certificate requests. All ADCS requests are routed to the ADCS server within this domain.

Hostname: The network address of the ADCS server.

Username: The account name used to authenticate against the ADCS server.

Port: The port number the ADCS Web Enrollment service listens on (default: 443).

Priority: Determines which server takes precedence when multiple ADCS services are configured (1–10, lower value means higher priority).

Templates: The list of certificate templates fetched from this ADCS server, available for use during certificate signing.

Service Operations

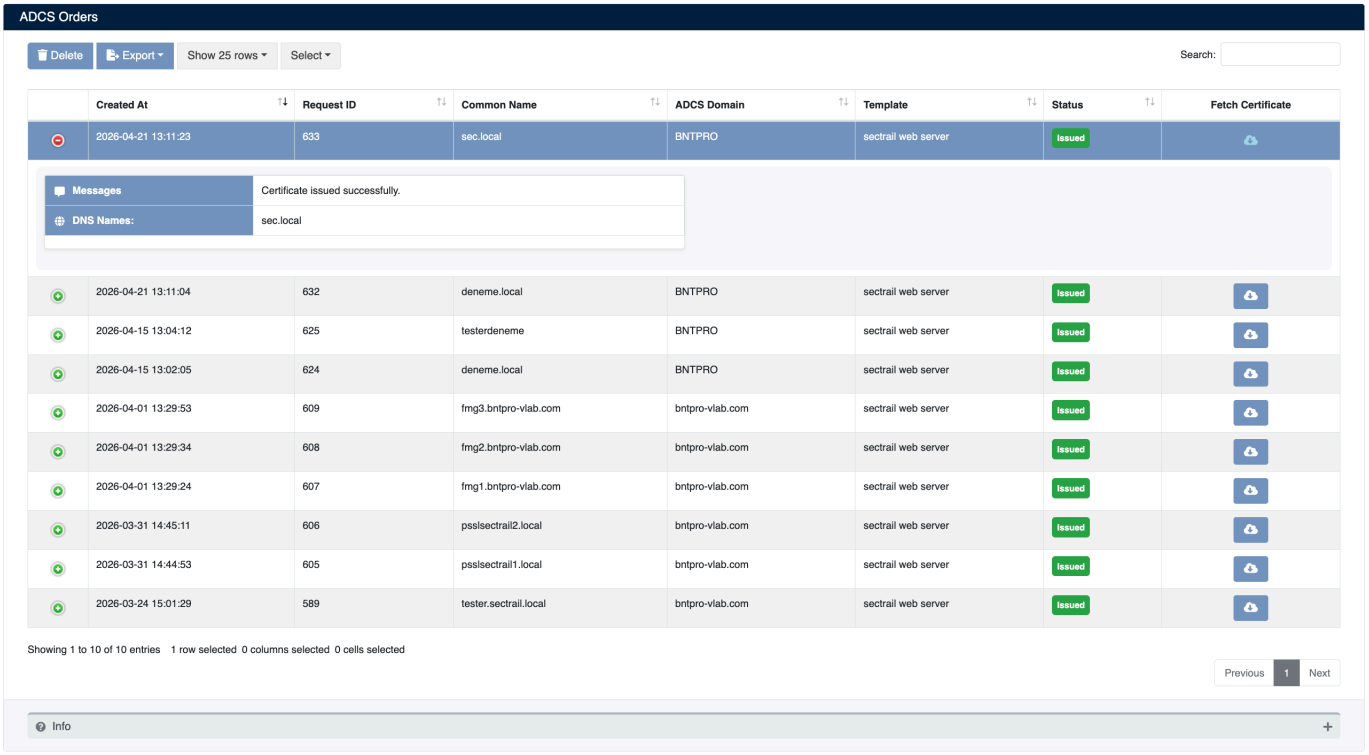
The following operations can be performed for each service:

- **Refresh**: Re-fetches service information and the template list from the ADCS server
- **Edit**: Edit service connection settings
- **Delete**: Delete service

Orders

After submitting a certificate request to ADCS, you can track all pending and completed orders from:

Certificate Authorities (CA) > ADCS > Orders



About Approval-Based Templates

Some ADCS certificate templates require **CA manager approval** before issuance. When a certificate is requested using one of these templates, the request is not issued immediately — it is queued and must be manually approved by a CA administrator on the ADCS server.

> **TRACKING PENDING REQUESTS**
>
> If you submitted a certificate request using an approval-required template and the certificate has not been issued yet, navigate to **Certificate Authorities (CA) > ADCS > Orders** to check its status. Once the CA manager approves the request on the ADCS side, you can use the **Fetch** action to retrieve the issued certificate into SecTrail CM.

Order Fields

Field	Description
Created At	Date and time the request was submitted to the ADCS server
Request ID	The request ID returned by ADCS after submission
Common Name	The domain name for which the certificate will be issued
ADCS Domain	The Active Directory domain name the request was routed to
Template	The ADCS certificate template used for signing
Status	The current status of the order (Issued, Pending, Denied)
Fetch Certificate	Action button used to import the issued certificate into the SecTrail CM inventory

Order Statuses

- **Issued** : Certificate has been approved and issued — use **Fetch** to retrieve it
- **Pending** : Awaiting CA manager approval on the ADCS server
- **Denied** : Request was rejected by the CA manager

Order Operations

- **Fetch**: Retrieve the issued certificate into SecTrail CM inventory
- **Delete**: Remove the order record

> **APPROVAL-BASED WORKFLOW**
>
> If your organization uses approval-required ADCS templates, coordinate with your CA administrator to approve pending requests. After approval, return to **Certificate Authorities (CA) > ADCS > Orders** and use **Fetch** to import the certificate.

> **CERTIFICATE SIGNING**
>
> With ADCS integration, you can perform certificate signing with your desired template. Template selection determines the certificate's validity period, purpose, and security level.

ACME - Automatic Certificate Management

SecTrail CM integrates with all Certificate Authority systems that support the ACME (Automatic Certificate Management Environment) protocol, enabling automatic ordering, renewal, and management of SSL/TLS certificates.

Supported ACME Providers

SecTrail CM is compatible with the following Certificate Authorities that support the ACME protocol:

- **Let's Encrypt** - Most popular ACME provider for free DV certificates
- **Let's Encrypt Staging** - Test server for test and development environments
- **ZeroSSL** - ACME service providing free SSL certificates
- **Buypass** - Norway-based free Certificate Authority
- **Buypass Staging** - Buypass test environment
- **SSL.com RSA** - SSL.com commercial certificates with RSA algorithm
- **SSL.com ECC** - SSL.com certificates with ECC (Elliptic Curve) algorithm
- **Google Trust Services** - Google's enterprise ACME service
- **Google Trust Services Staging** - Google test environment
- **DigiCert** - DigiCert ACME service (enterprise)

> **ACME PROTOCOL**
>
> ACME protocol is an open standard (RFC 8555) that enables automation of the certificate lifecycle. This documentation will explain integration steps using **Let's Encrypt** as an example.

Connection Requirements

Requirement	Detail	Description
Protocol	ACME v2 (HTTPS)	RFC 8555 standard
Authentication	Email	ACME account registration
Validation Methods	DNS-01, HTTP-01	Domain ownership validation
DNS-01 Port	53 (DNS)	Required for Domain Delegation (optional)
HTTP-01 Port	80 (HTTP)	Required for HTTP validation (optional)
DNS Integration	PowerDNS, Akamai	Recommended for DNS-01 automation

Automatic Operations

SecTrail CM automatically performs the following operations through the ACME protocol:

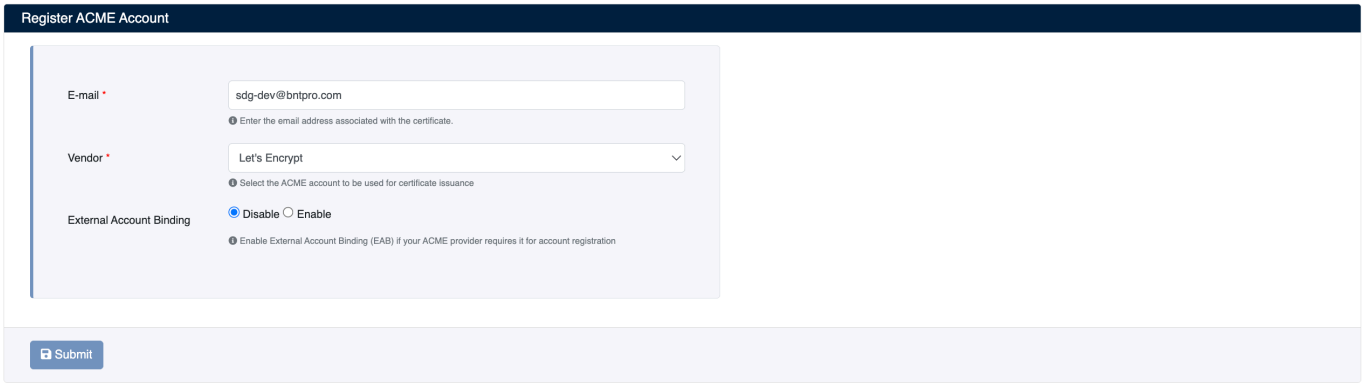
1. **ACME Account Registration**: Creating an ACME account for certificate orders

2. **Certificate Order**: Creating a new SSL/TLS certificate request
3. **Domain Validation**: Domain validation via DNS-01 or HTTP-01 challenge
4. **Automatic DNS Record Management**: Automatic creation and deletion of DNS validation records
5. **Certificate Issuance**: Automatic retrieval of the certificate
6. **Certificate Renewal**: Automatic renewal of certificates about to expire
7. **Certificate Deployment**: Automatic addition of issued certificates to the system

Configuration Steps

1. Create ACME Account

Navigate to **Certificate Authorities (CA) > ACME > Accounts** and click the **Register** button:



Enter the following information:

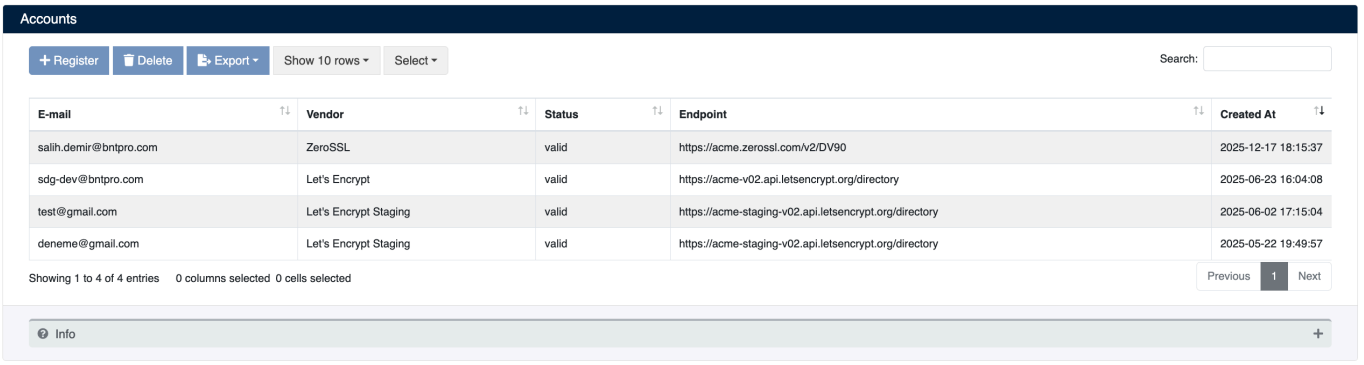
- **E-mail**: Email address for ACME account
- **Vendor**: ACME provider selection
- Let's Encrypt
- Let's Encrypt Staging
- ZeroSSL
- Buypass
- Buypass Staging
- SSL.com RSA
- SSL.com ECC
- Google Trust Services
- Google Trust Services Staging
- DigiCert
- **Use External Account Binding**: Required for some providers (default: Disable)

Click **Submit** button to create the ACME account.

> **ACCOUNT REGISTRATION**
>
> When an ACME account is created, a key pair is automatically generated and registration is performed. Account information is securely stored.

2. View ACME Accounts

After adding an account, it will be displayed in the **Certificate Authorities (CA) > ACME > Accounts** list:



The list screen displays the following information:

- **E-mail**: ACME account email address
- **Vendor**: ACME provider being used
- **Status**: Account status (valid/invalid)
- **Endpoint**: ACME directory endpoint URL
- **Created At**: Account creation date

Account Operations

The following operations can be performed for each account:

- **Delete**: Delete the account

> **ACCOUNT DELETION**
>
> When an ACME account is deleted, all orders created with this account become invisible. However, issued certificates remain in the system.

3. Validation Methods

Two different validation methods are used when signing certificates with the ACME protocol:

DNS-01 Validation (DNS Validation)

You must use DNS validation method to sign wildcard certificates.

There are two different methods for DNS validation:

Method 1: Domain Delegation (Recommended)

Requirements:

- SecTrail CM application must have **port 53 (DNS)** open to the internet
- The `_acme-challenge` subdomain of the domain to be signed must be delegated to the SecTrail CM server

Configuration:

Create the following NS record in your domain DNS:

```
_acme-challenge.domainname NS 3600 sectrailcm.server.address
```

Advantages:

- Fully automatic process
- No manual intervention required
- Ideal for continuous certificate renewal

Method 2: Manual TXT Record

Configuration:

For each certificate request, you must manually create a TXT record in your domain DNS:

```
_acme-challenge.domainname TXT 3600 TOKEN_VALUE
```

Disadvantages:

- Requires manual intervention for each certificate request
- Token value changes for each order
- Not suitable for automatic renewal

> **MANUAL TXT RECORD**
>
> This method is not recommended as it requires manual intervention. Domain Delegation or External DNS integration should be used for automatic certificate renewal processes.

Method 3: External DNS Integration (Recommended)

Supported DNS Providers:

From the **Certificate Authorities (CA) > External DNS** section, you can configure one of the following DNS providers:

- **PowerDNS** - Open source DNS server
- **Akamai** - Enterprise DNS management

Configuration:

1. Navigate to **Certificate Authorities (CA) > External DNS**
2. Select your DNS provider
3. Enter API credentials
4. Test and save

Advantages:

- Fully automatic DNS record management
- TXT records are automatically created and deleted
- Ideal for wildcard and multi-domain certificates
- Full automation of certificate renewal

> **DNS INTEGRATION**

With PowerDNS and Akamai integrations, DNS validation records are fully automatically managed. No manual intervention is required, and certificate renewal processes run uninterrupted.

HTTP-01 Validation (HTTP Validation)

Use Case: Can only be used for single domain certificates. **Not supported** for wildcard certificates.

Requirements:

1. **Port 80 Access:** The domain to be signed must respond to HTTP requests on port 80
2. **Public IP:** The domain's public IP address must be able to receive requests
3. **Web Server:** There must be a web server configuration for the domain

If Using F5 Load Balancer:

- The domain's public IP must route requests to F5
- You must know which virtual server it lands on
- Access to the `/.well-known/acme-challenge/` path must be provided via port 80

ACME Challenge Process:

1. ACME server sends an HTTP GET request to `http://domainname/.well-known/acme-challenge/TOKEN`
2. Your web server must respond to this request with the validation token
3. Once the token is validated, the certificate is issued

HTTP-01 LIMITATIONS

- **Cannot be used for wildcard certificates**
- Must be accessible via port 80 (not HTTPS)
- Separate validation required for each domain
- May require load balancer or firewall configuration

VALIDATION METHOD SELECTION

- **For Wildcard Certificates:** DNS-01 validation must be used (mandatory)
- **For Single Domain:** HTTP-01 or DNS-01 can be used
- **For Automatic Renewal:** DNS-01 with External DNS is recommended
- **For Manual Process:** HTTP-01 can be used

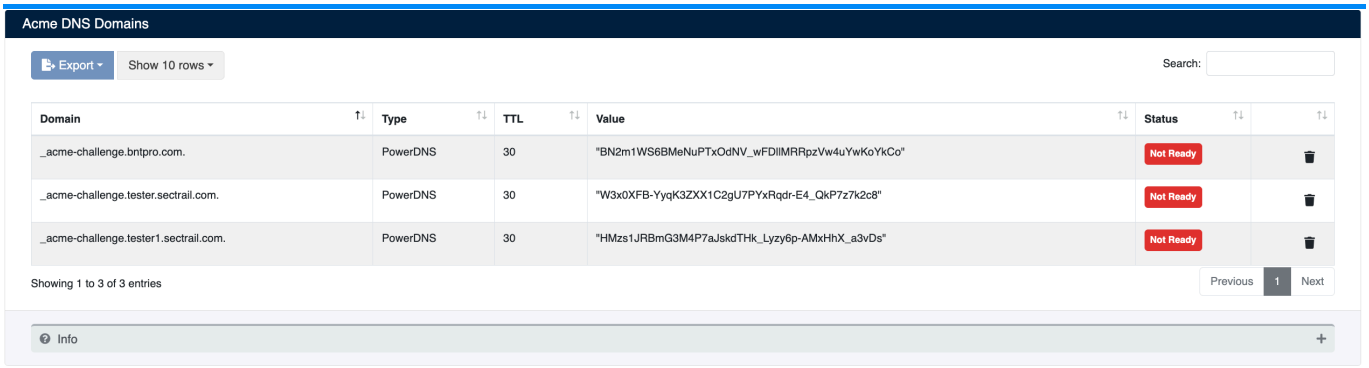
4. DNS Integration Configuration

External DNS integration must be configured to use DNS-01 validation.

DNS Challenge Records

When an ACME certificate order is created, TXT records are automatically created for DNS validation:

You can view challenge records in the **Certificate Authorities (CA) > ACME > Acme DNS Domains** section:



DNS Record Information

- **Domain**: Domain where the challenge record will be created (_acme-challenge.example.com)
- **Type**: DNS record type (PowerDNS, Akamai, etc.)
- **TTL**: Time to Live value (seconds)
- **Value**: ACME challenge token value
- **Status**: Record status (Not Ready, Ready, Valid)

> **AUTOMATIC DNS MANAGEMENT**
>
> DNS validation records are automatically added when a certificate order is created and automatically deleted after validation is complete. No manual intervention required.

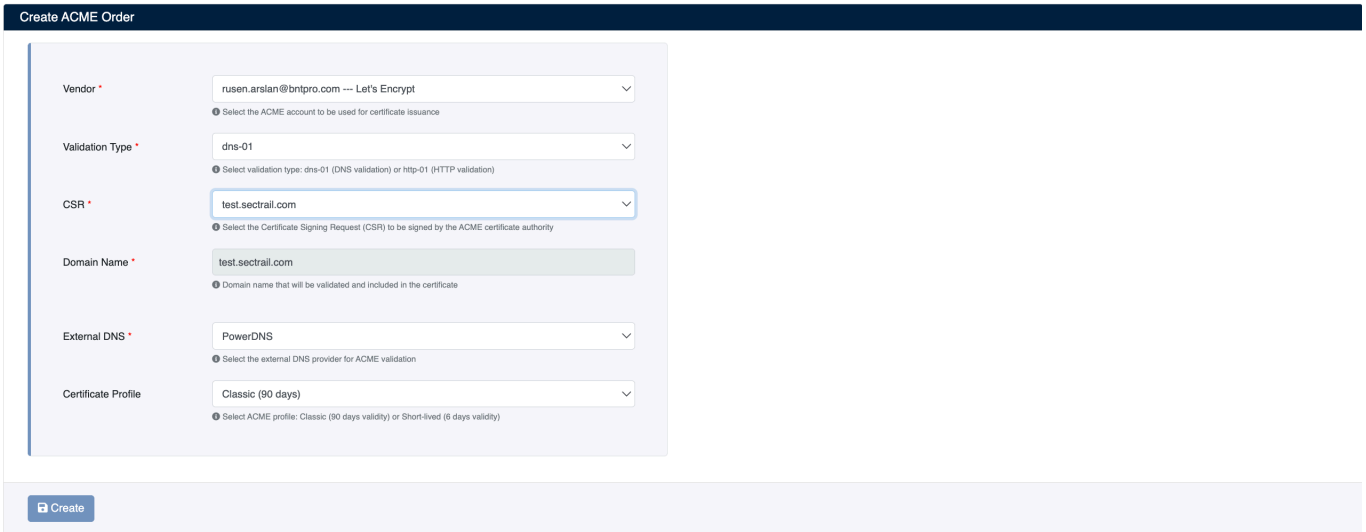
DNS Record Statuses

- **Not Ready**: DNS record created, waiting for propagation
- **Ready**: DNS record propagated, validation can be initiated
- **Valid**: Validation successful, certificate issued

Create Certificate Order

To create a new certificate order via ACME:

Navigate to **Certificate Authorities (CA) > ACME > Orders** and click the **Create ACME Order** button:



Order Information

Enter the following information:

- **Vendor**: ACME account selection (email --- vendor format)
- **Validation Type**: Validation method selection
- `dns-01`: DNS validation (mandatory for wildcard certificates, recommended for single domain)
- `http-01`: HTTP challenge (only for single domain certificates)
- **CSR**: Certificate Signing Request selection
- Select from previously created CSRs
- CSRs can be created from the **Integration** section
- **Domain Name**: Domain names for the certificate
- **External DNS**: DNS provider selection for DNS validation (only for dns-01)
- PowerDNS, Akamai, Cloudflare, Route53, etc.

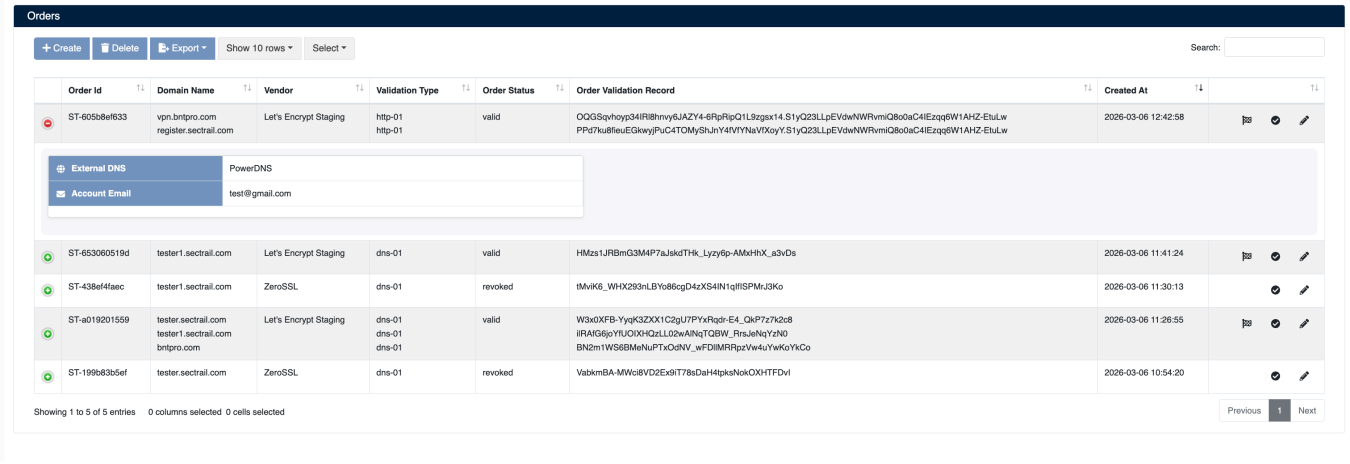
Click **Submit** button to create the order.

> **CSR (CERTIFICATE SIGNING REQUEST)**
>
> Before creating an order, you need to create a CSR from the **Certificates > CSR** section. CSR contains the required domain names, organization information, and public key for the certificate.

View Certificate Orders

To view your ACME certificate orders:

Navigate to **Certificate Authorities (CA) > ACME > Orders**:



Order Information

- **Order Id**: SecTrail order ID
- **External DNS**: DNS provider being used
- **Domain Name**: Certificate domain names
- **Vendor**: ACME provider
- **Account Email**: ACME account email

- **Validation Type**: Validation method (dns-01 or http-01)
- **Order Status**: Order status (valid, processing, invalid)
- **Order Validation Record**: ACME challenge token values
- **Created At**: Order creation date

Order Operations

The following operations can be performed for each order:

- **Refresh Order**: Update order status
- **Finalize Order**: Retrieve certificate when validation is complete
- **Download Certificate**: Download issued certificate
- **Delete Order**: Delete order

Order Statuses

- **pending**: Order created, waiting for validation
- **ready**: Validation successful, ready to finalize
- **processing**: Certificate is being issued
- **valid**: Certificate issued successfully
- **invalid**: Validation failed

Certificate Lifecycle

1. Order Creation

1. Create CSR (**Certificates > CSR**)
2. Select ACME account
3. Select validation type and External DNS
4. Create order

2. DNS Challenge (Validation)

After order creation, automatically:

1. DNS validation records are created (`_acme-challenge.example.com`)
2. DNS propagation is awaited (typically 30-60 seconds)
3. ACME server validates domain ownership
4. When validation is successful, order status becomes "ready"

3. Certificate Retrieval (Finalization)

After successful validation:

1. Click **Finalize Order** button
2. Certificate is automatically issued
3. Order status becomes "valid"
4. DNS validation records are automatically deleted

4. Certificate Download

1. Click **Download Certificate** button
2. Certificate is automatically added to the system
3. Can be viewed from the **Certificates** section

> **AUTOMATIC OPERATIONS**
>
> DNS validation record creation, validation, and certificate retrieval operations are fully automatic. No manual intervention required.

Certificate Renewal

ACME certificates can be automatically renewed:

1. Select the certificate about to expire from the **Certificates** section
2. Click **Renew** button
3. A new ACME order is automatically created
4. Validation and finalization occur automatically

> **LET'S ENCRYPT VALIDITY PERIODS**
>
> Let's Encrypt certificates are valid for 90 days.

HashiCorp Vault

SecTrail CM integrates with HashiCorp Vault to enable automatic requesting and management of enterprise SSL/TLS certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	HTTPS	Vault API is used
Port	Used Port	Standard Vault API port
Authentication	Token Authentication	Authentication with Vault token
User Permission	PKI Secret Engine Read/Write	Certificate request and enrollment permission

Automatic Operations

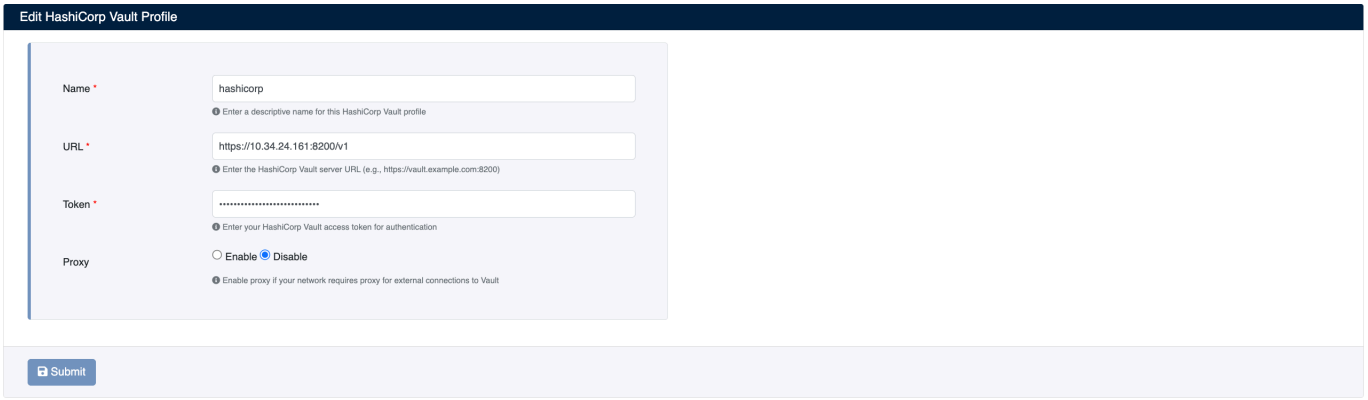
SecTrail CM automatically performs the following operations on HashiCorp Vault:

1. **Certificate Request**: CSR (Certificate Signing Request) submission
2. **Certificate Enrollment**: Certificate issuance through Vault PKI Engine
3. **Role Management**: Using different certificate roles
4. **Automatic Approval**: Automatic approval for configured roles

Configuration Steps

1. Add HashiCorp Vault Profile

Navigate to **Certificate Authorities (CA) > Hashicorp** and click the **Create** button:



Enter the following information:

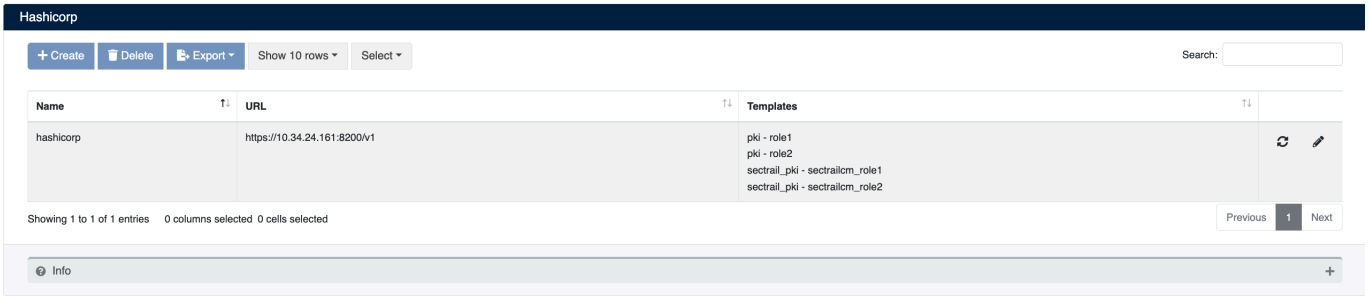
- **Name**: Profile name
- **URL**: Vault server URL
- **Token**: Vault API token

- **Proxy**: Proxy usage (Enable/Disable). After enabling the proxy, complete your proxy configuration from **Settings -> Proxy** settings.

Click **Submit** button to save the profile.

2. View HashiCorp Vault Profiles

After adding a profile, it will be displayed in the **Certificate Authorities (CA) > Hashicorp** list:



The list screen displays the following information:

- **Name**: Profile name
- **URL**: Vault server address
- **Templates**: Available certificate roles (PKI roles)

Profile Operations

The following operations can be performed for each profile:

- **Refresh**: Refresh profile information and role list
- **Edit**: Edit profile settings
- **Delete**: Delete profile

> **CERTIFICATE SIGNING**
>
> With HashiCorp Vault integration, you can perform certificate signing with your desired role. Role selection determines the certificate's validity period, purpose, and security level.

F5 BIG-IP

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to F5 BIG-IP devices.

Connection Requirements

Requirement	Detail	Description
Protocol	iControl REST API (HTTPS)	F5 BIG-IP's native REST API is used
Port	`443`	Standard HTTPS port
Authentication	Basic Authentication	Authentication via Username and Password
User Permission	tmsh + Administrator	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on F5 BIG-IP:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key
2. **Virtual Server Update**: Configuring relevant virtual servers to use the new certificate
3. **Configuration Sync**: Automatic synchronization to peer devices in HA environments

Configuration Steps

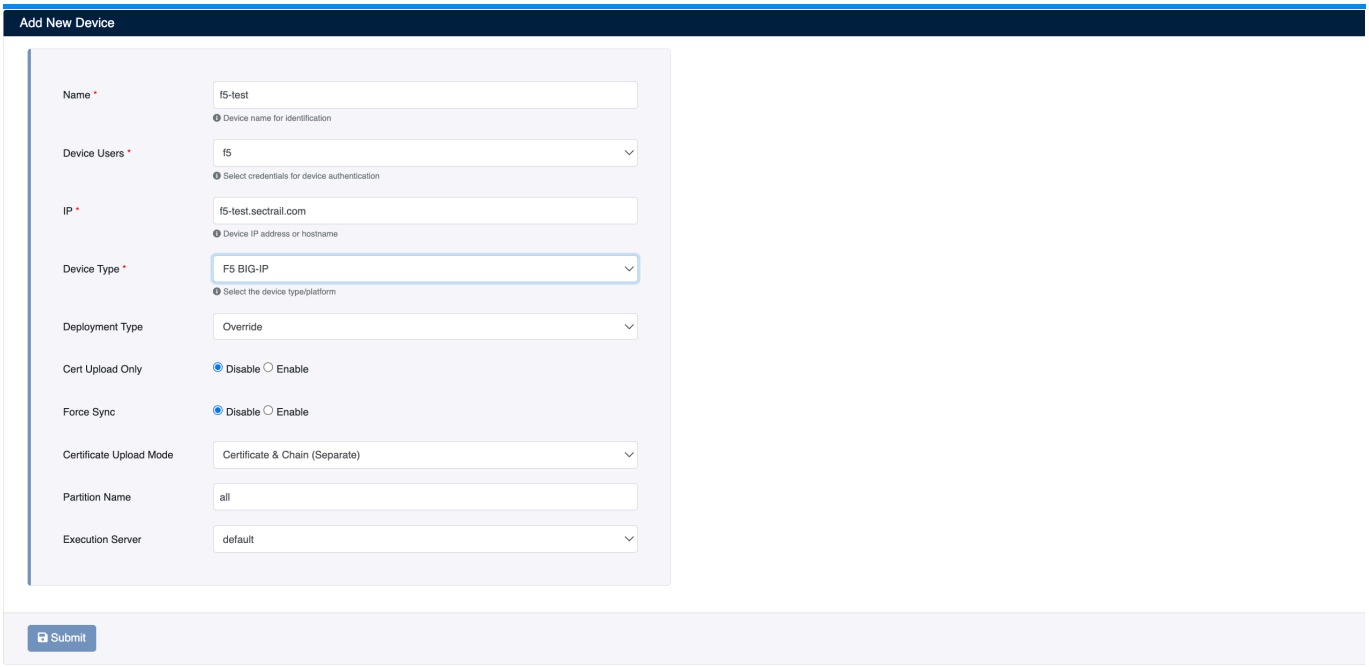
1. Creating F5 BIG-IP User

Navigate to **Automation > Device Users** and create a user for F5.

> **USER PERMISSIONS**
>
> Ensure the user has tmsh (Traffic Management Shell) permissions.

2. Adding F5 Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:



- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the IP address of the F5 BIG-IP device
- **Device Type**: Select `F5 BIG-IP` from the dropdown menu
- **Deployment Type**: Select **Generative** or **Override** mode
- **Cert Upload Only**: Should only certificate be uploaded? (Disabled/Enabled)
- **Force Sync**: Should automatic synchronization to standby device be active? (Disabled/Enabled)
- **Partition Name**: Can be left as `all` by default

Deployment Type Options

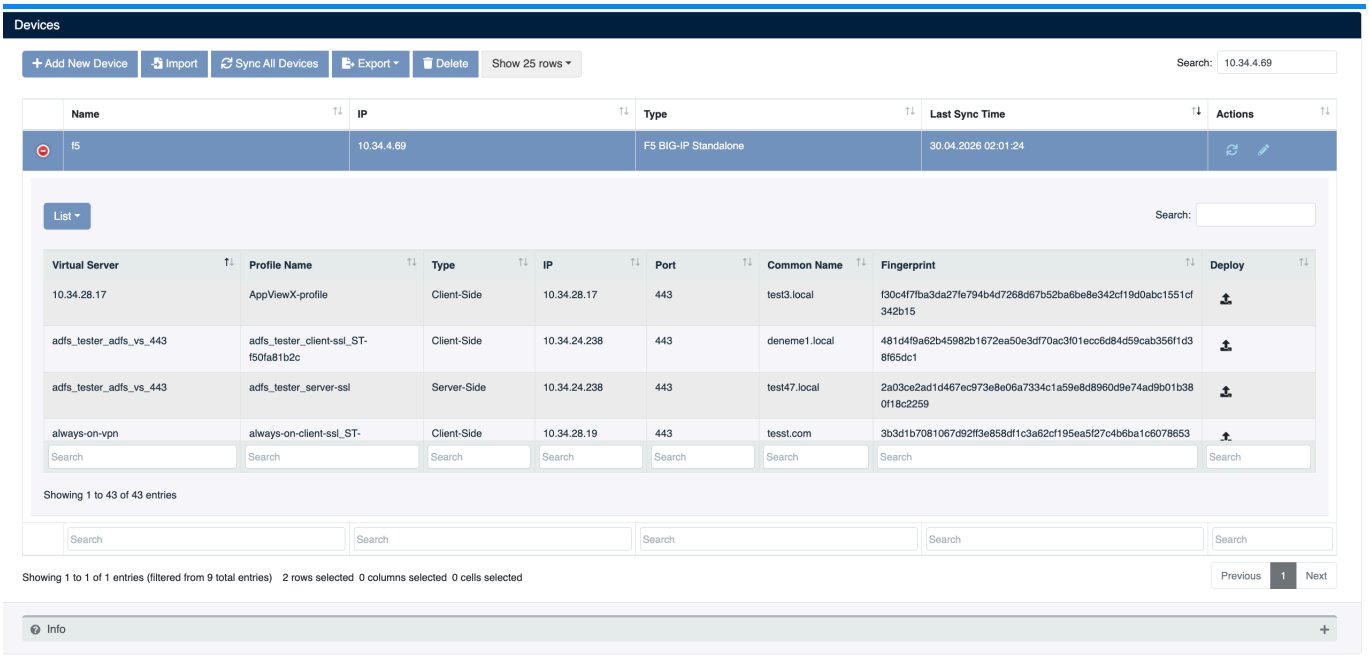
- **Generative**: SecTrail CM creates a new Client SSL Profile and automatically updates the Virtual Server
- **Override**: Directly modifies the existing SSL Profile

> **FORCE SYNC**
>
> In HA (High Availability) environments, you can enable **Force Sync** to ensure automatic synchronization to the standby device.

> **AUTOMATIC DISCOVERY**
>
> After the F5 device is added to SecTrail CM, the IP addresses and ports of all Virtual Servers defined on the device are automatically included in the discovery period and scanned regularly.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



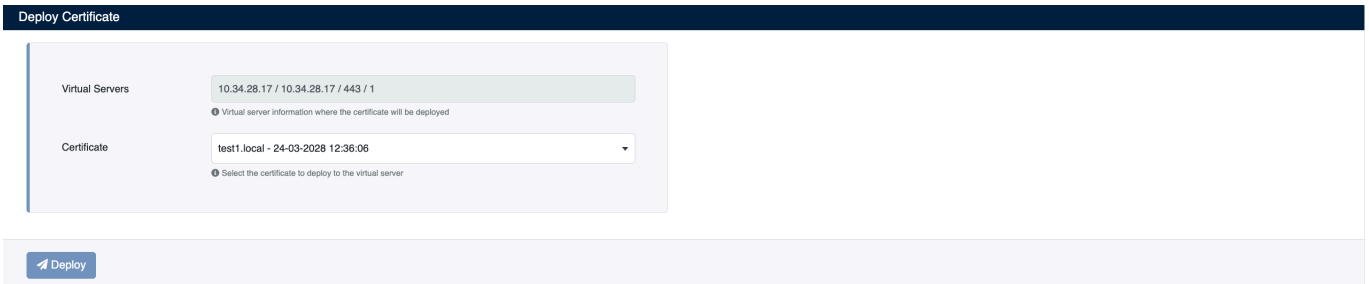
- **Virtual Server**: Virtual Server names defined on the F5 device
- **Profile Name**: SSL profile names
- **Type**: Client-Side or Server-Side SSL profile type
- **Destination Address** and **Port**: IP and port that the Virtual Server listens on
- **Common Name**: Common Name value of the current certificate
- **Fingerprint**: Certificate fingerprint
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your F5 device from **Automation > Devices**
2. In the device details, find the **Virtual Server** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Server information is displayed
- **Certificate**: Select the certificate you want to deploy from the dropdown menu



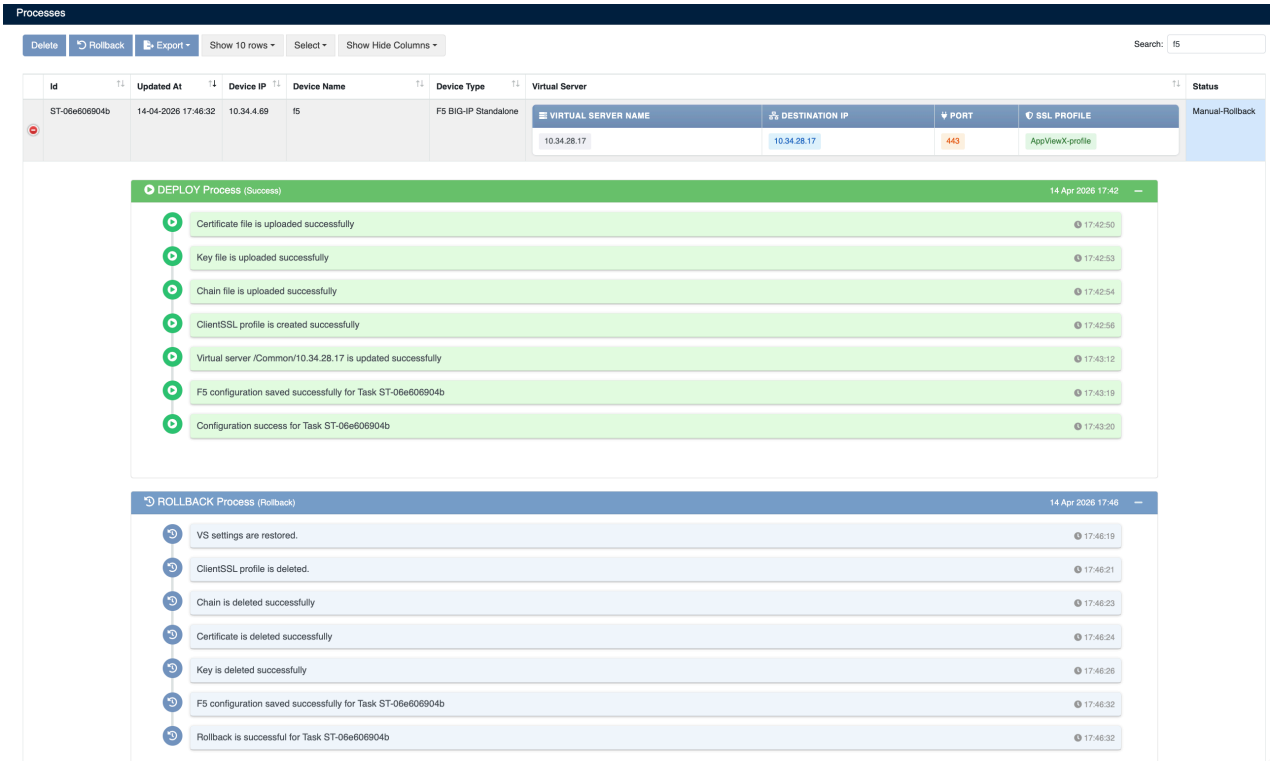
Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

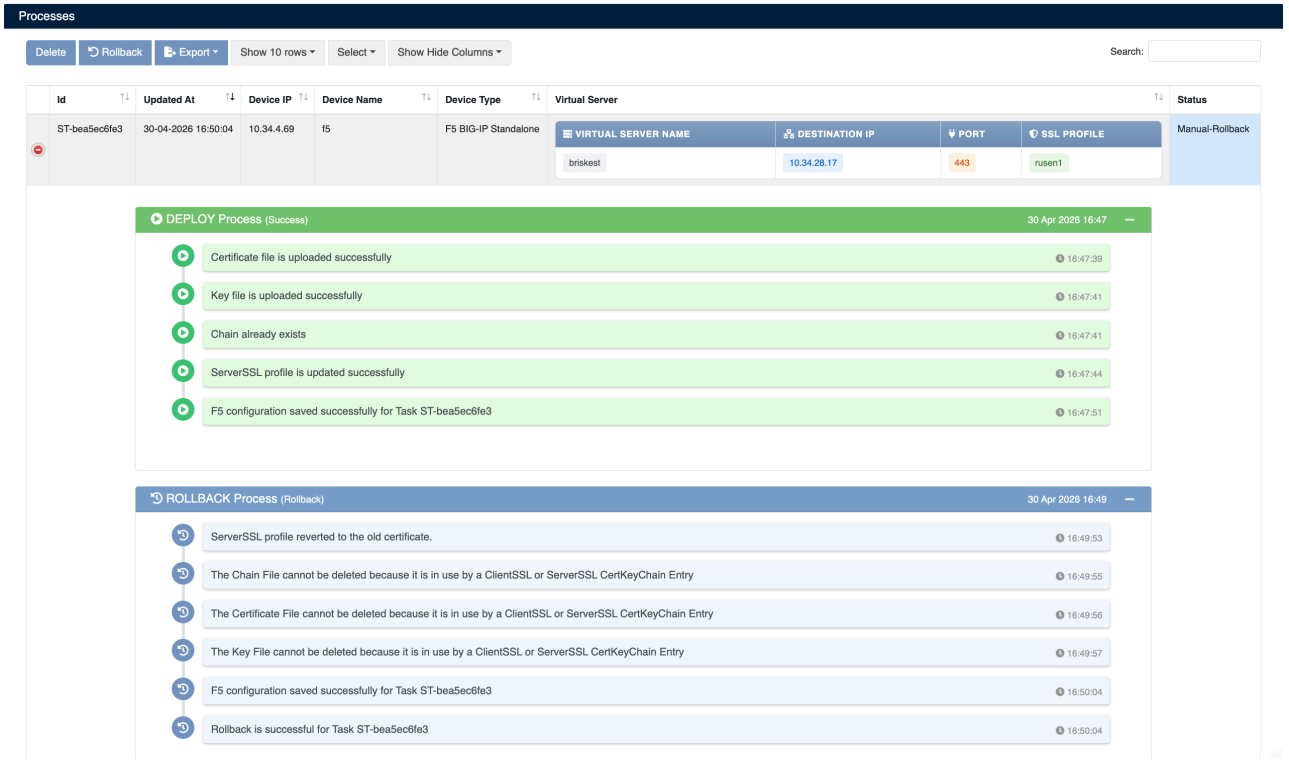
Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:

Generative Mode:



Override Mode:



Operation Details

Step	Generative Mode	Override Mode
1	Certificate, key, and chain files are uploaded to F5 BIG-IP device	Certificate, key, and chain files are uploaded to F5 BIG-IP device
2	A new Client SSL profile is created using the existing Client SSL profile as parent	Existing Client SSL profile is directly updated (no new profile created)
3	The created new profile is assigned to the Virtual Server	Certificate in the profile is updated without changing VS configuration

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Generative Mode Rollback	Override Mode Rollback
1	VS's previous profile settings are restored	Certificate references in the profile are reverted to the old certificate
2	Profile created during deployment is removed	Newly uploaded certificate, key, and chain files are deleted
3	Certificate, key, and chain files are deleted from F5 device	-

Citrix NetScaler

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to Citrix NetScaler Application Delivery Controller (ADC) devices.

Connection Requirements

Requirement	Detail	Description
Protocol	NITRO REST API (HTTPS)	NetScaler's native REST API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Basic Authentication	Authentication via Username and Password
User Permission	nsroot or superuser role	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on Citrix NetScaler:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key
2. **CertKey Creation**: Creating and managing certificate-key pairs
3. **Virtual Server Binding**: Binding certificates to SSL Virtual Servers
4. **Configuration Save**: Making configuration persistent

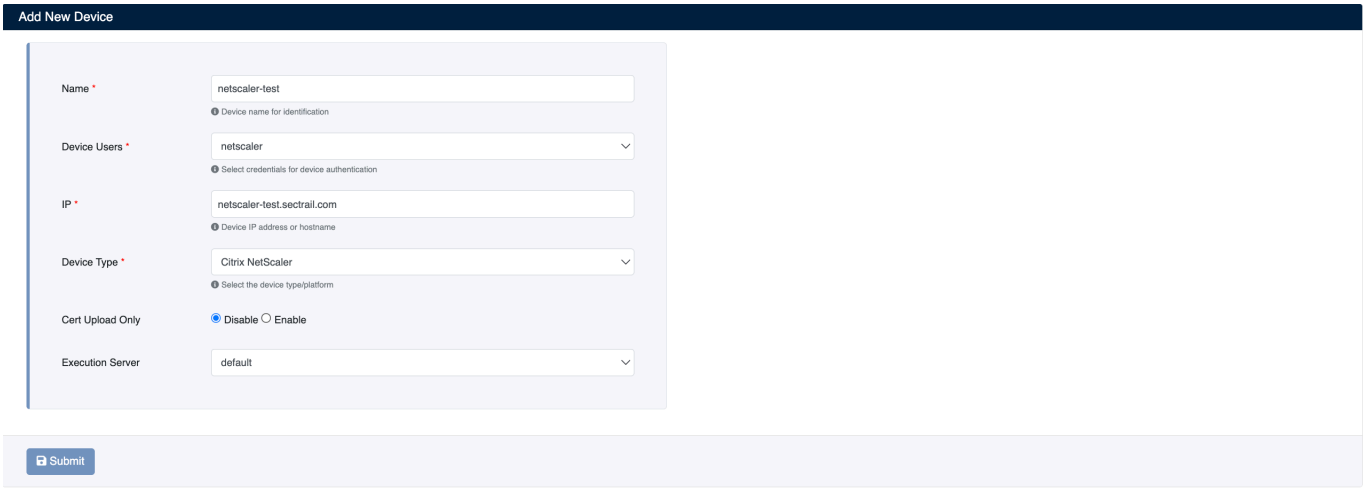
Configuration Steps

1. Creating NetScaler User

Navigate to **Automation > Device Users** and create a user for F5.

2. Adding NetScaler Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

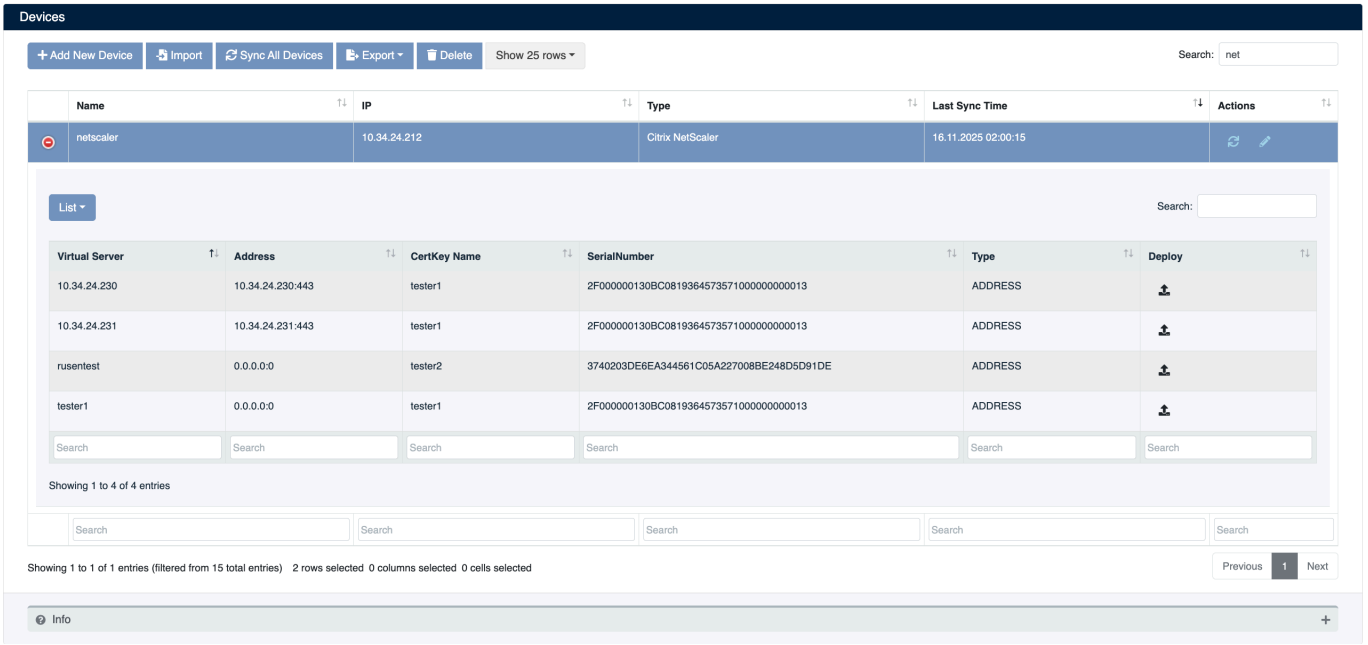


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the NSIP address of the NetScaler device
- **Device Type**: Select `Citrix NetScaler` from the dropdown menu
- **Cert Upload Only**: Should only certificate be uploaded? (Disabled/Enabled)

> **AUTOMATIC DISCOVERY**
>
> After the NetScaler device is added to SecTrail CM, the IP addresses and ports of all Virtual Servers defined on the device are automatically included in the discovery period and scanned regularly.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



- **Virtual Server**: Virtual Server names defined on the NetScaler device
- **Address**: IP address and port of the Virtual Server
- **CertKey Name**: Current certificate-key pair names
- **SerialNumber**: Certificate serial number
- **Type**: Shows the address type
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your NetScaler device from **Automation > Devices**
2. In the device details, find the **Virtual Server** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row

4. In the **Deploy Certificate** window that opens:

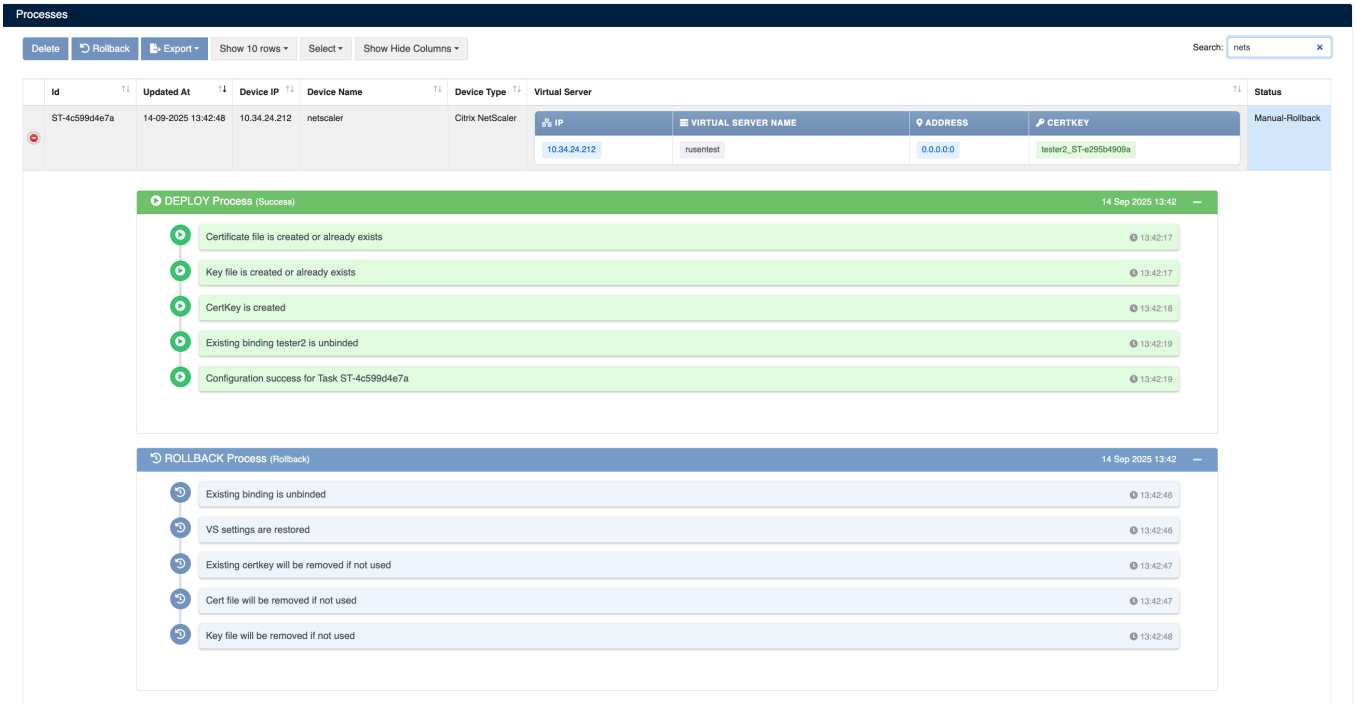
- **Virtual Servers**: Target Virtual Server information is displayed (IP, port, CertKey name)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate and key file are uploaded to the system
2	Certificate-key pair is created
3	Existing certificate binding is removed
4	New certificate is bound to virtual server

AUTOMATIC CLEANUP

SecTrail CM automatically cleans up unused old certificate and key files after deployment.

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

AUTOMATIC ROLLBACK

If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Old certificate-key pair is preserved
2	Virtual Server's previous binding settings are restored
3	Newly uploaded certificate and key files are deleted
4	Certkey created during deployment is removed

Palo Alto Networks

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to Palo Alto Networks firewall devices.

Connection Requirements

Requirement	Detail	Description
Protocol	XML API (HTTPS)	Palo Alto's native XML API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Username and Password	Authentication via Username and Password
User Permission	Admin or Certificate Manager role	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on Palo Alto Networks firewall:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key
2. **Certificate Import**: Importing certificate and key to the device
3. **SSL Profile Update**: Updating SSL decryption profiles
4. **Configuration Commit**: Committing and making configuration persistent

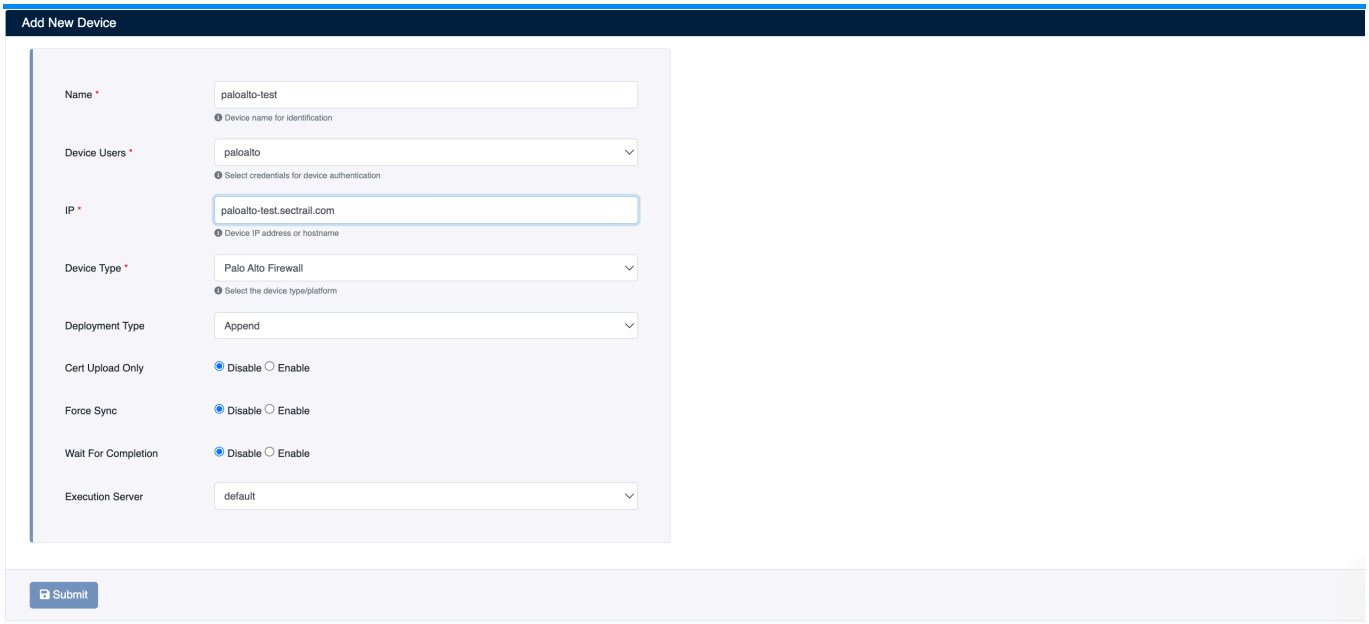
Configuration Steps

1. Creating Palo Alto User

Navigate to **Automation > Device Users** and create a user for Palo Alto.

2. Adding Palo Alto Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

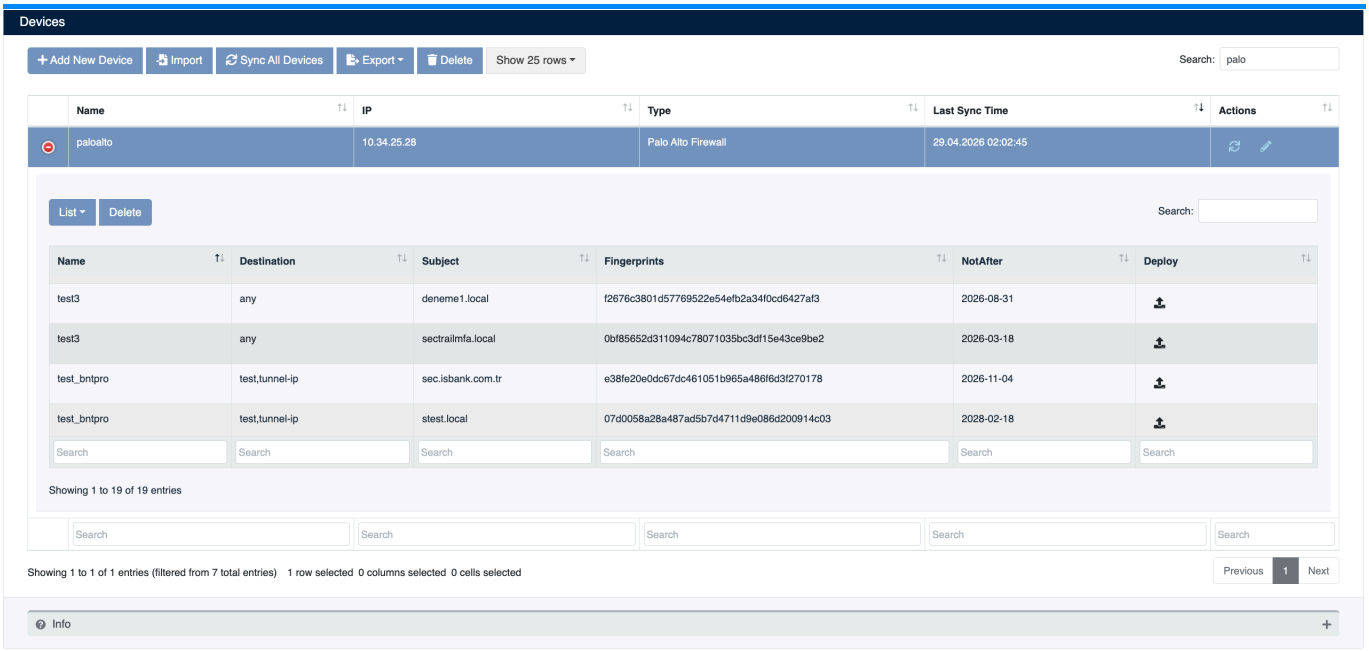


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the management IP address of the Palo Alto device
- **Device Type**: Select `Palo Alto Firewall` from the dropdown menu
- **Deployment Type**: Select deployment type
- **Append**: Adds new certificate to existing decryption rule (existing certificates are preserved)
- **Override**: Replaces existing certificate with new one (old certificate is deleted)
- **Cert Upload Only**: Should only certificate be uploaded? (Disabled/Enabled)
- **Force Sync**: Should changes be automatically committed? (Disabled/Enabled)
- **Wait For Completion**: Should commit operation completion be awaited? (Disabled/Enabled)

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the Palo Alto device is added to SecTrail CM, all certificates defined on the device are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



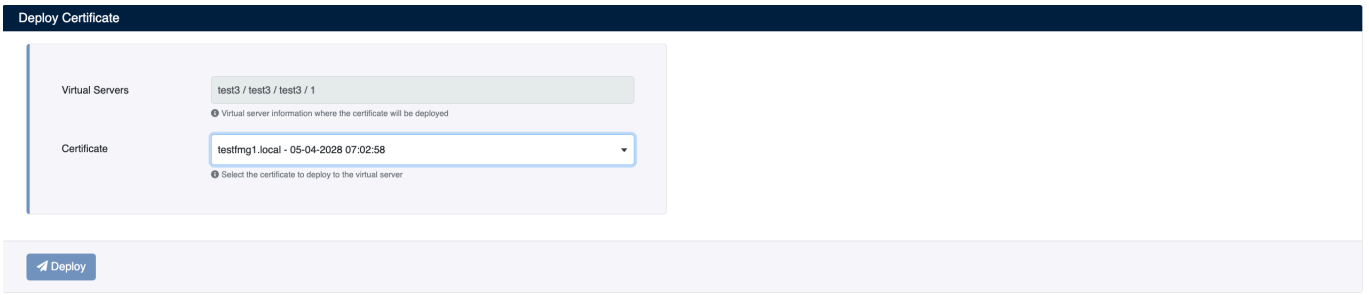
- **Name**: Certificate names defined on the device
- **Destination**: Certificate usage area (any, tunnel-ip, etc.)
- **Subject**: Certificate subject information
- **Fingerprints**: Certificate fingerprint
- **NotAfter**: Certificate expiration date
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your Palo Alto device from **Automation > Devices**
2. In the device details, find the **Virtual Server** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Server information is displayed (Name/Destination/Subject format)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

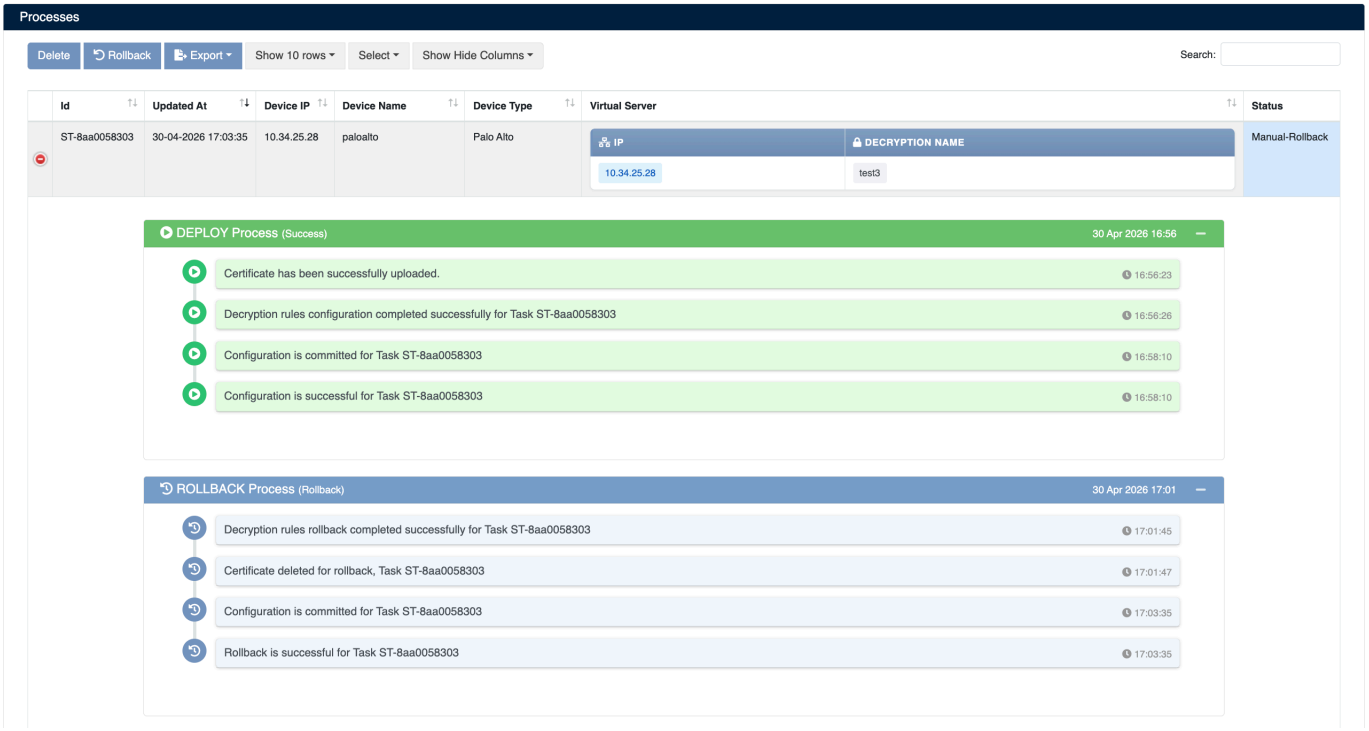


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate is successfully updated
2	Decryption rules are configured
3	Configuration is committed
4	Configuration is successfully completed

> **COMMIT**
>
> When **Force Sync** is enabled, SecTrail CM automatically commits configuration changes after deployment and makes them persistent.

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Newly uploaded certificate is deleted
2	Previous configuration is restored
3	Decryption rules are reverted to their previous state
4	Rollback operation is successfully completed

PaloAlto Panorama

SecTrail CM enables automatic deployment and renewal of SSL certificates to all managed firewall devices by establishing **agentless** connections to the Palo Alto Panorama central management platform.

Connection Requirements

Requirement	Detail	Description
Protocol	XML API (HTTPS)	Panorama's native XML API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Username and Password	Authentication via Username and Password
User Permission	Admin or Certificate Manager role	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on Palo Alto Panorama:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key
2. **Certificate Import**: Importing certificate and key to devices managed through Panorama
3. **SSL Profile Update**: Updating SSL decryption profiles
4. **Configuration Commit**: Committing and making configuration persistent

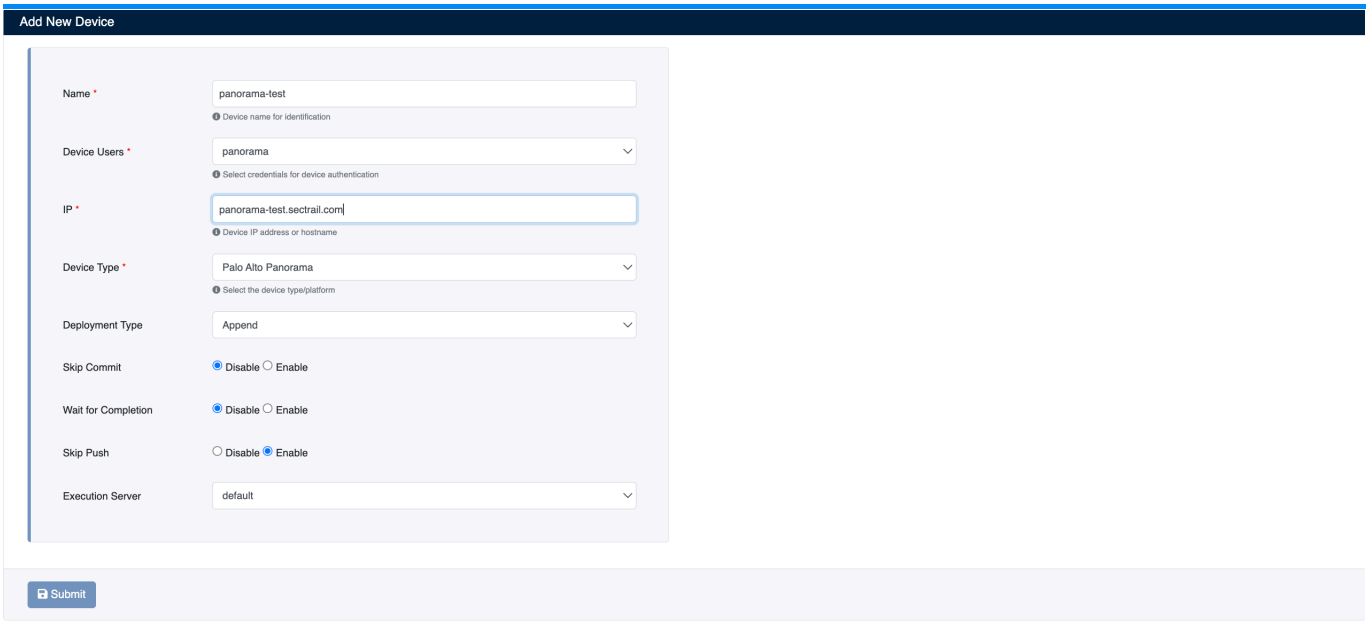
Configuration Steps

1. Creating Panorama User

Navigate to **Automation > Device Users** and create a user for Panorama.

2. Adding Panorama Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

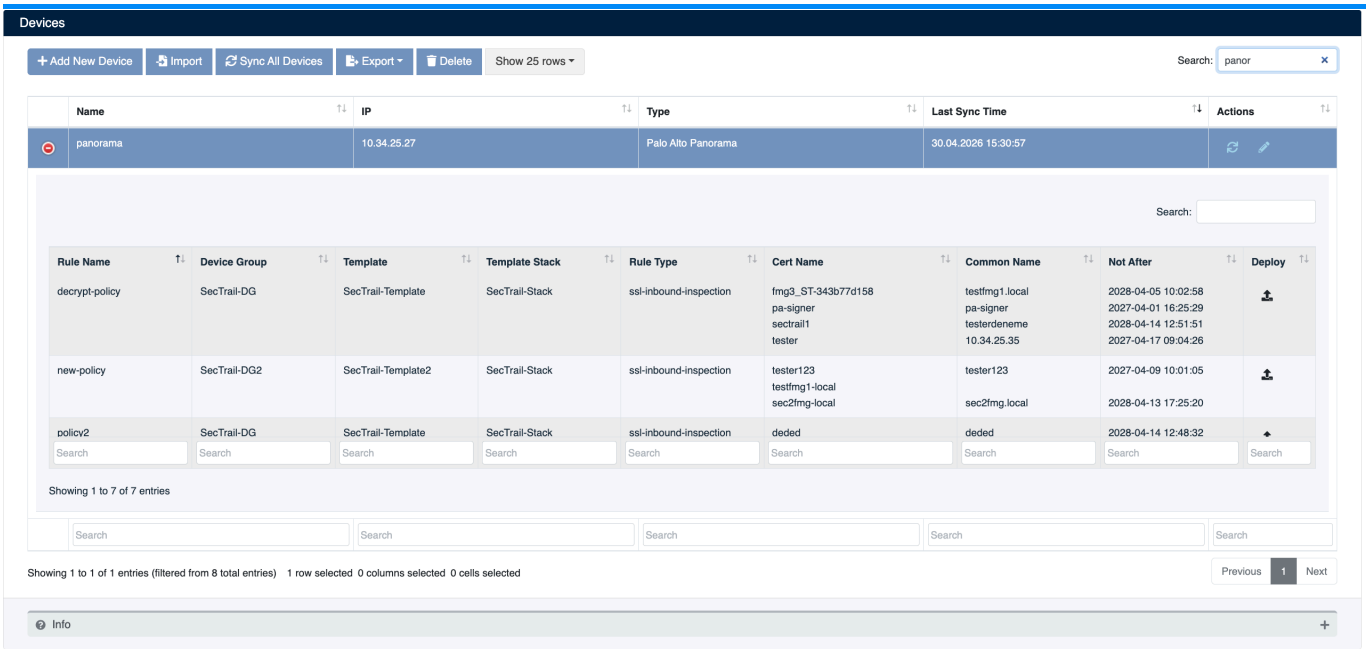


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the Panorama management IP address
- **Device Type**: Select `Panorama` from the dropdown menu
- **Deployment Type**: Select deployment type
- **Append**: Adds new certificate to existing decryption rule (existing certificates are preserved)
- **Replace**: Replaces existing certificate with new one (old certificate is deleted)
- **Skip Commit**: Should changes be committed? (Disabled/Enabled)
- **Skip Push**: Should the certificate be pushed to the target device? (Disabled/Enabled)

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the Panorama device is added to SecTrail CM, all certificates on devices managed by Panorama are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



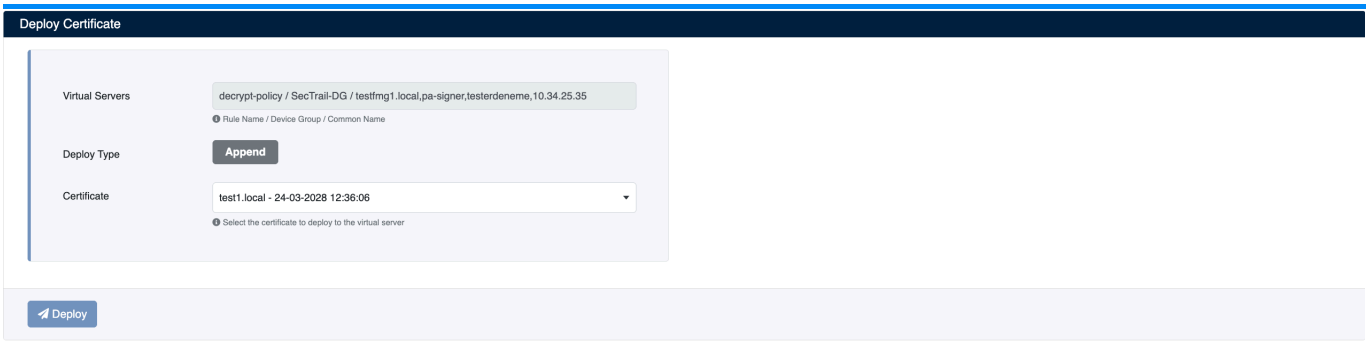
- **Rule Name**: Name of the rule defined on Panorama
- **Device Group**: Device group the certificate belongs to
- **Template**: Panorama template name the certificate is associated with
- **Template Stack**: Template stack name the certificate belongs to
- **Rule Type**: Type of the rule (e.g. decryption rule)
- **Cert Name**: Name of the certificate defined on the device
- **Common Name**: Common Name (CN) information of the certificate
- **Not After**: Certificate expiration date
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your Panorama device from **Automation > Devices**
2. In the device details, find the **Virtual Server** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Server information is displayed (Name/Destination/Subject format)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

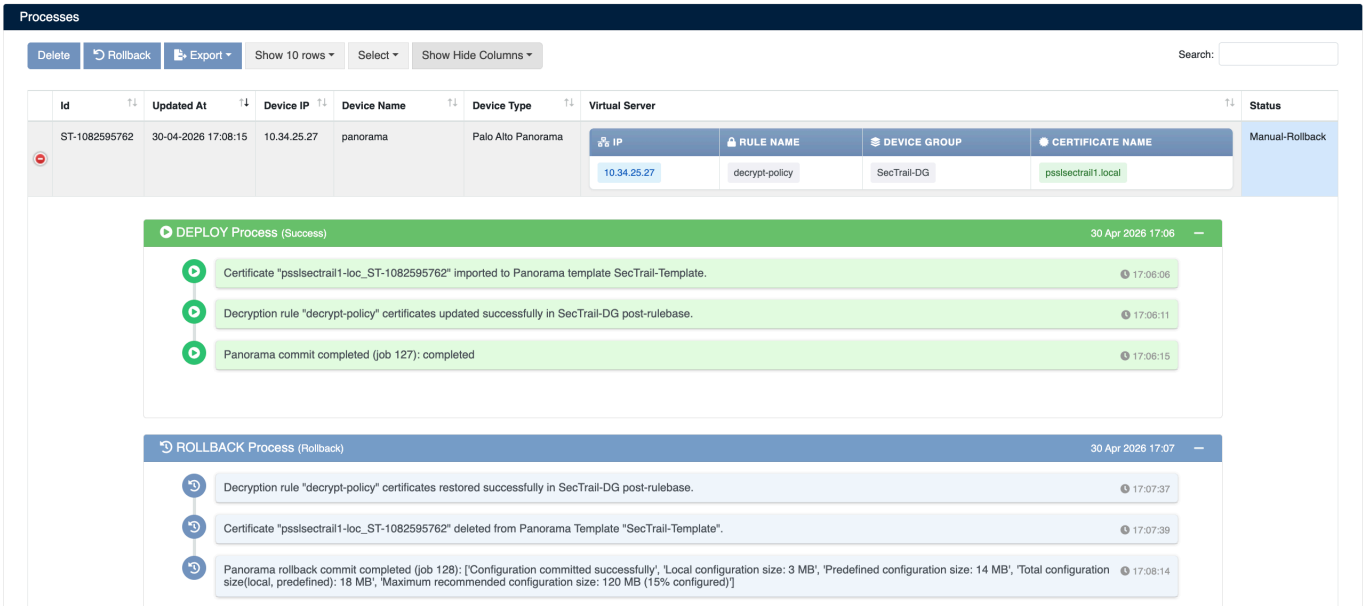


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate is successfully updated
2	Decryption rules are configured
3	Configuration is committed
4	Configuration is successfully completed

> **COMMIT**
>
> When **Skip Commit** is disabled, SecTrail CM commits the configuration changes after deployment and makes them persistent.

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Newly uploaded certificate is deleted
2	Previous configuration is restored
3	Decryption rules are reverted to their previous state
4	Rollback operation is successfully completed

FortiWeb

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to Fortinet FortiWeb Web Application Firewall (WAF) devices.

Connection Requirements

Requirement	Detail	Description
Protocol	REST API (HTTPS)	FortiWeb's native REST API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Basic Authentication	Authentication via Username and Password
User Permission	Administrator or Certificate Manager	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on FortiWeb:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key
2. **Certificate Chain Creation**: Creating chain with Intermediate CA certificates
3. **Server Policy Update**: Updating certificate references in server policy
4. **SNI Members Update**: SNI-based certificate assignments
5. **Configuration Apply**: Activating the configuration

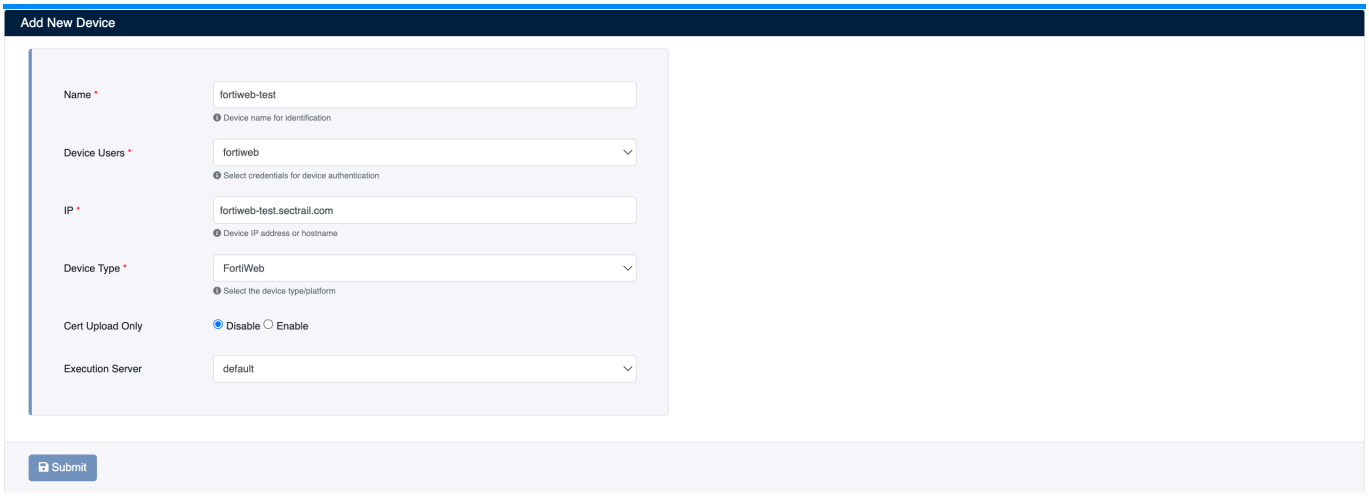
Configuration Steps

1. Creating FortiWeb User

Navigate to **Automation > Device Users** and create a user for FortiWeb.

2. Adding FortiWeb Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

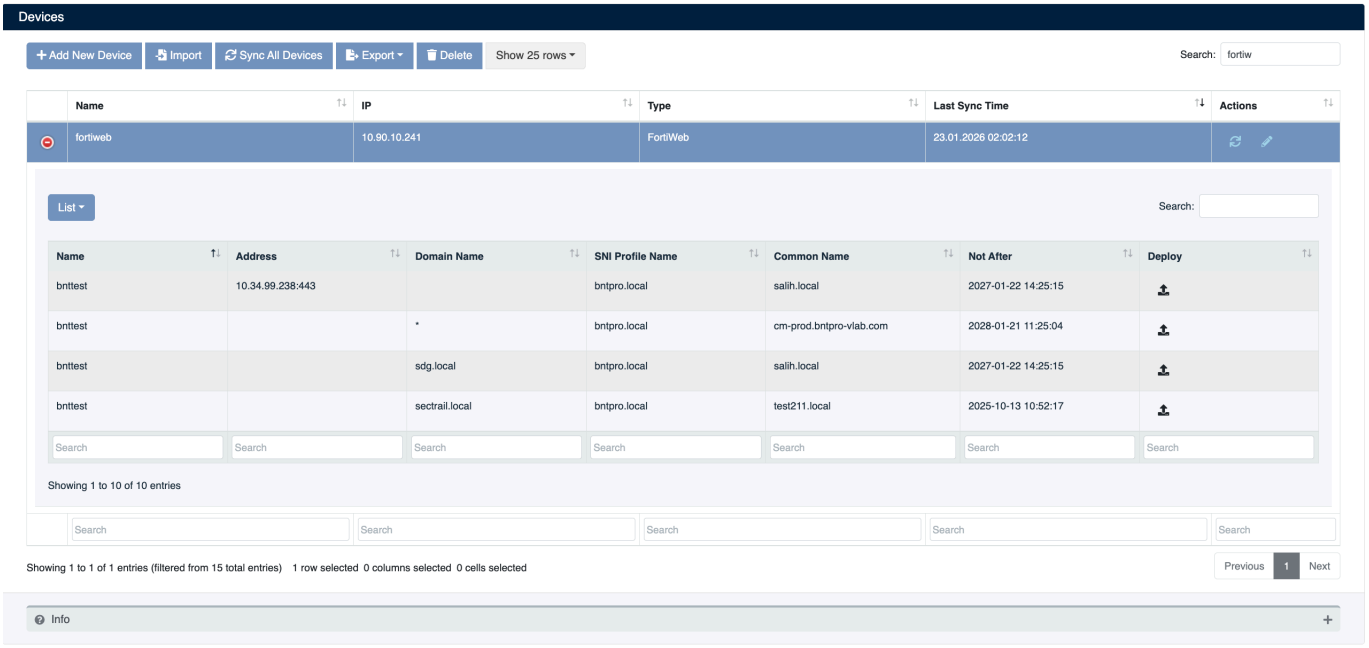


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the management IP address of the FortiWeb device
- **Device Type**: Select `FortiWeb` from the dropdown menu
- **Cert Upload Only**: Should only certificate be uploaded? (Disabled/Enabled)

> **AUTOMATIC DISCOVERY**
>
> After the FortiWeb device is added to SecTrail CM, the IP addresses and ports of all Server Policies and SNIs defined on the device are automatically included in the discovery period and scanned regularly.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



- **Server Policy**: Server Policy names defined on the FortiWeb device
- **Type**: Shows policy type (Server-Policy or SNI)

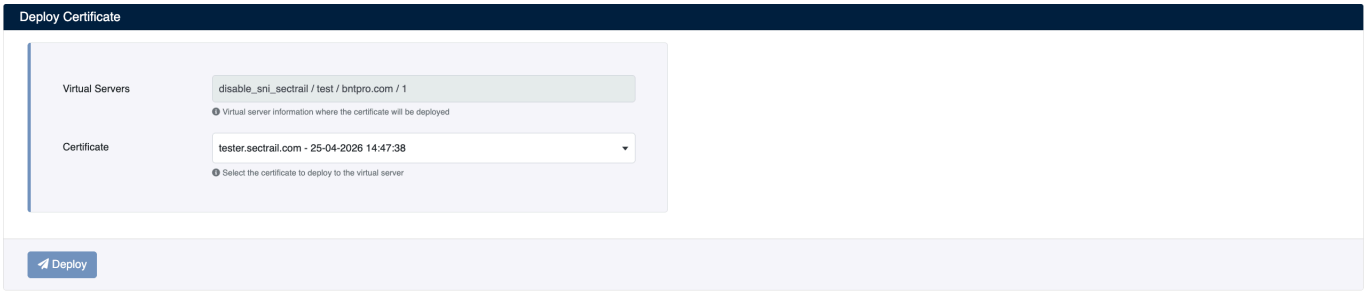
- **SNI**: Server Name Indication name (for SNI types)
- **Domain Name**: Associated domain name of the SNI profile
- **Address**: IP address and port of the virtual server
- **Common Name**: Common Name value of the certificate
- **Not After**: Certificate expiration date
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Server Policy and Certificate Selection

1. Select your FortiWeb device from **Automation > Devices**
2. In the device details, find the **Server Policy** or **SNI** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Server Policy/SNI**: Target policy information is displayed
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

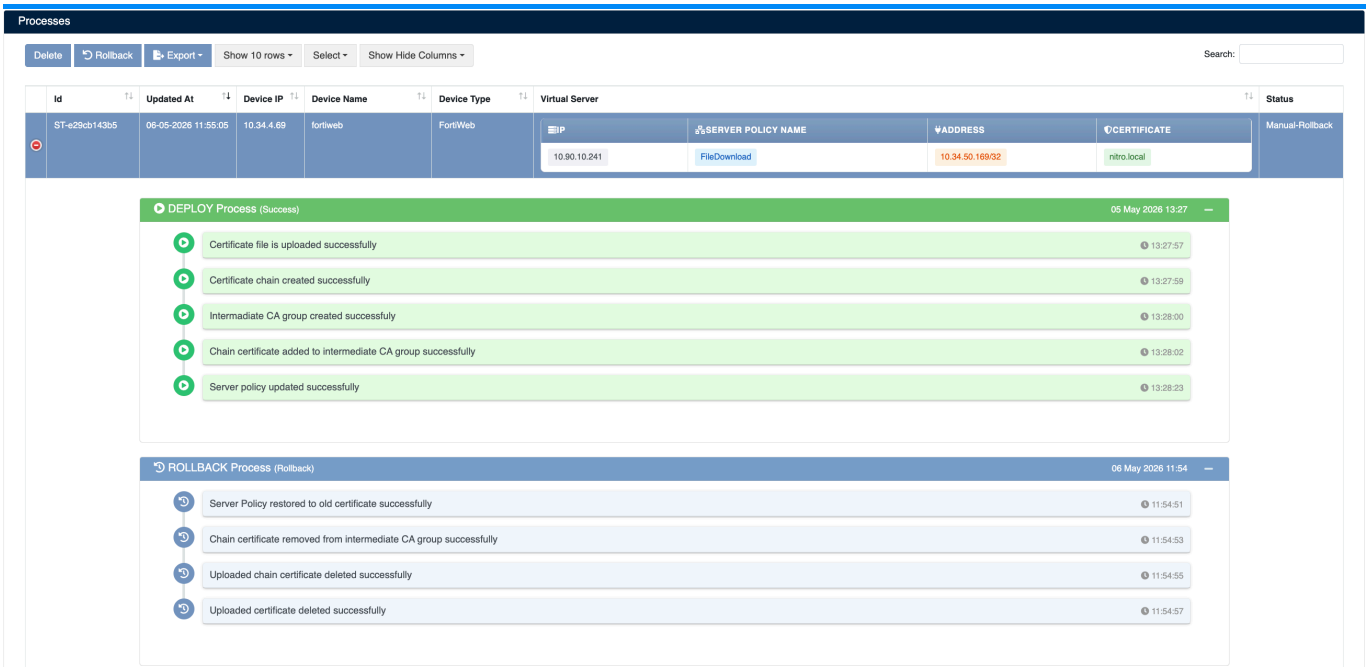


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

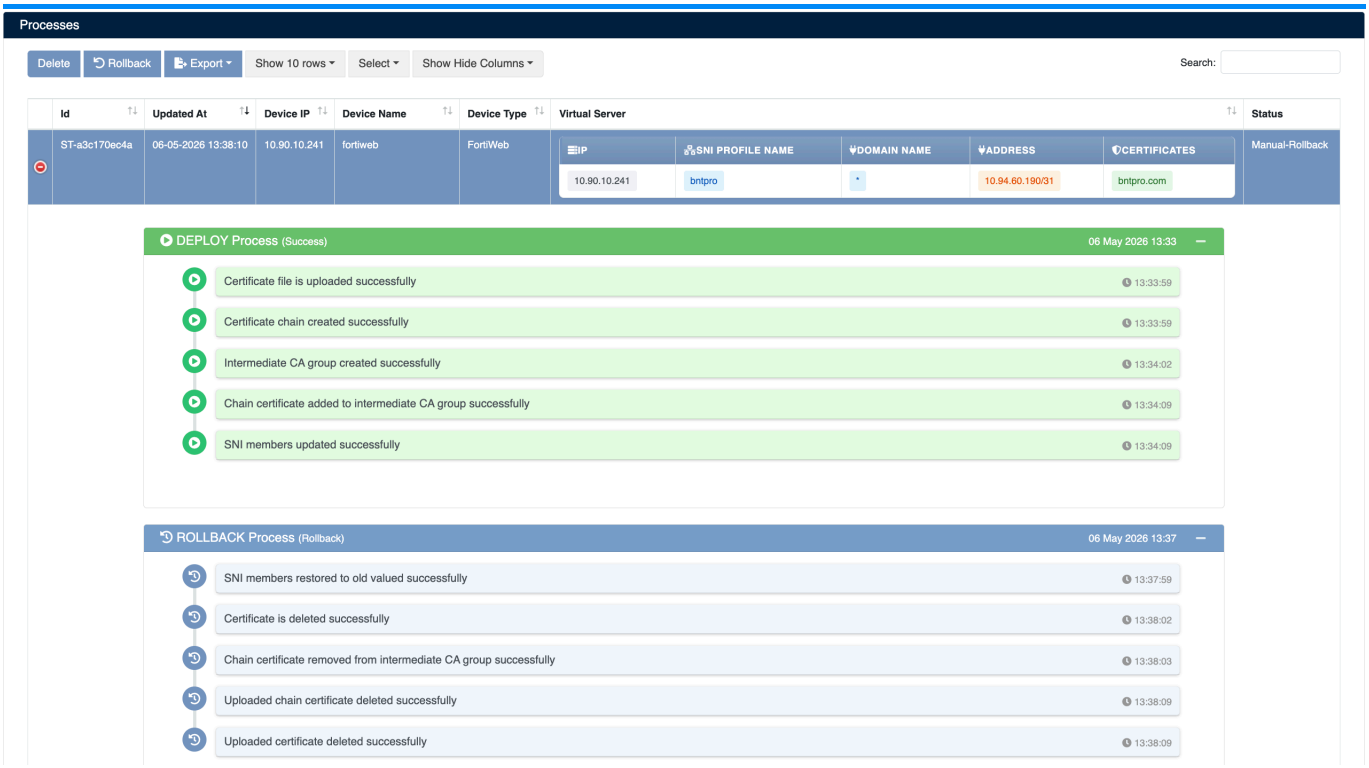
The following steps are performed during deployment:

Step	Operation Description
1	Certificate file is uploaded to the device
2	Certificate chain is created
3	Intermediate CA group is created
4	Chain certificate is added to CA group
5	Server policy is updated with new certificate

> **SERVER POLICY OPERATIONS**
>
> FortiWeb integration supports **Server Policy**-based certificate updates. During deployment, the certificate reference in the relevant server policy is automatically updated.

SNI (Server Name Indication) Management

FortiWeb supports SNI-based certificate management. SNI deployment operations:



SNI Operation Details

Step	Operation Description
1	Certificate file is uploaded to the device
2	Certificate chain is created
3	Intermediate CA group is created
4	Chain certificate is added to CA group
5	SNI member certificate is updated

> **SNI OVERRIDE OPERATIONS**
>
> In SNI member updates, existing certificate references are overridden with the new certificate. This simplifies domain-based certificate management.

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**

2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Server Policy Rollback	SNI Rollback
1	Server policy is reverted to old certificate	SNI member is reverted to old certificate
2	Chain certificate is removed from CA group	Chain certificate is removed from CA group
3	Uploaded chain certificate is deleted	Uploaded chain certificate is deleted
4	Uploaded certificate is deleted	Uploaded certificate is deleted

FortiGate

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to FortiGate firewall devices.

Connection Requirements

Requirement	Detail	Description
Protocol	REST API (HTTPS)	FortiGate's native REST API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Username and Password	Authentication via Username and Password
User Permission	Admin or Certificate Manager role	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on FortiGate:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key to the device
2. **SSL Profile Update**: Updating SSL inspection profiles
3. **Policy Update**: Updating firewall policies to use the new profile
4. **Configuration Commit**: Making configuration persistent

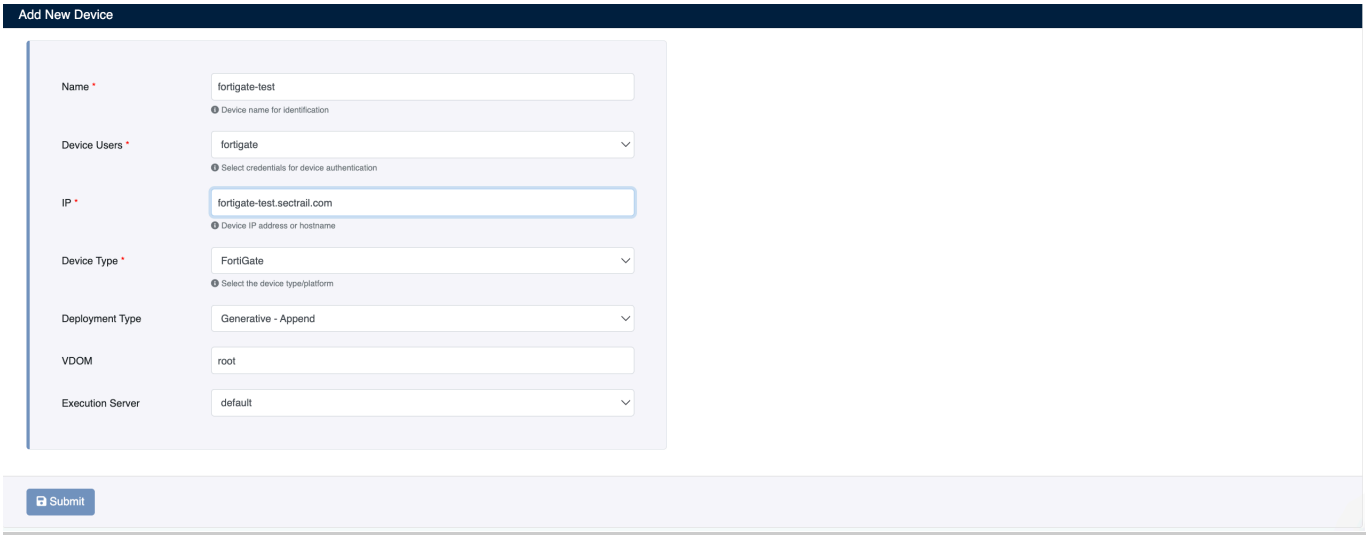
Configuration Steps

1. Creating FortiGate User

Navigate to **Automation > Device Users** and create a user for FortiGate.

2. Adding FortiGate Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

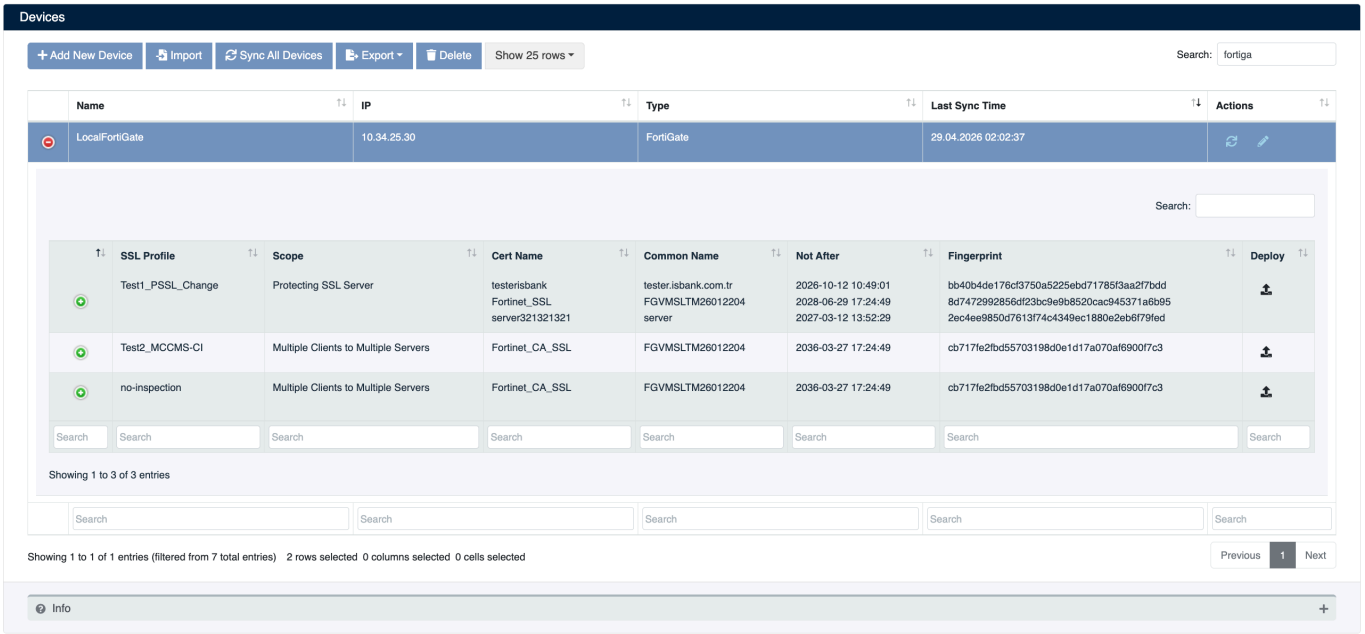


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the FortiGate device IP address or hostname
- **Device Type**: Select `FortiGate` from the dropdown menu
- **Deployment Type**: Select deployment type
- **Generative - Append**: Creates a new SSL profile, adds the new certificate to it, and associates it with matching policies
- **Generative - Replace**: Creates a new SSL profile, replaces the certificate within it, and associates it with matching policies
- **Override - Append**: Adds the new certificate to the existing SSL profile
- **Override - Replace**: Removes the current certificate from the existing SSL profile and adds the new one
- **VDOM**: FortiGate VDOM name (e.g. `root`)
- **Execution Server**: Server to use for executing deployment operations

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the FortiGate device is added to SecTrail CM, all certificates defined on the device are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



- **SSL Profile**: SSL inspection profile name associated with the certificate
- **Scope**: Scope of the SSL profile (e.g. Protecting SSL Server, Multiple Clients to Multiple Servers)
- **Cert Name**: Name of the certificate defined on the device
- **Common Name**: Common Name (CN) information of the certificate

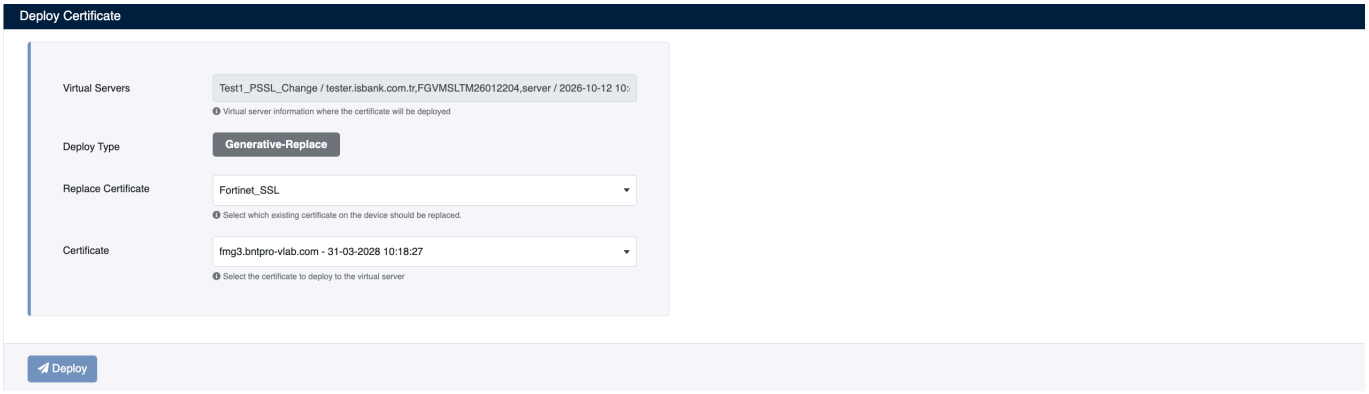
- **Not After**: Certificate expiration date
- **Fingerprint**: Certificate fingerprint
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: SSL Profile and Certificate Selection

1. Select your FortiGate device from **Automation > Devices**
2. In the device details, find the SSL profile where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target virtual server information is displayed (SSL Profile / Common Name / Installation Target / Not After format)
- **Deploy Type**: Displays the configured deployment type (e.g. Generative-Replace)
- **Replace Certificate**: Select the existing certificate on the device to be replaced
- **Certificate**: Select the new certificate to deploy from the dropdown menu

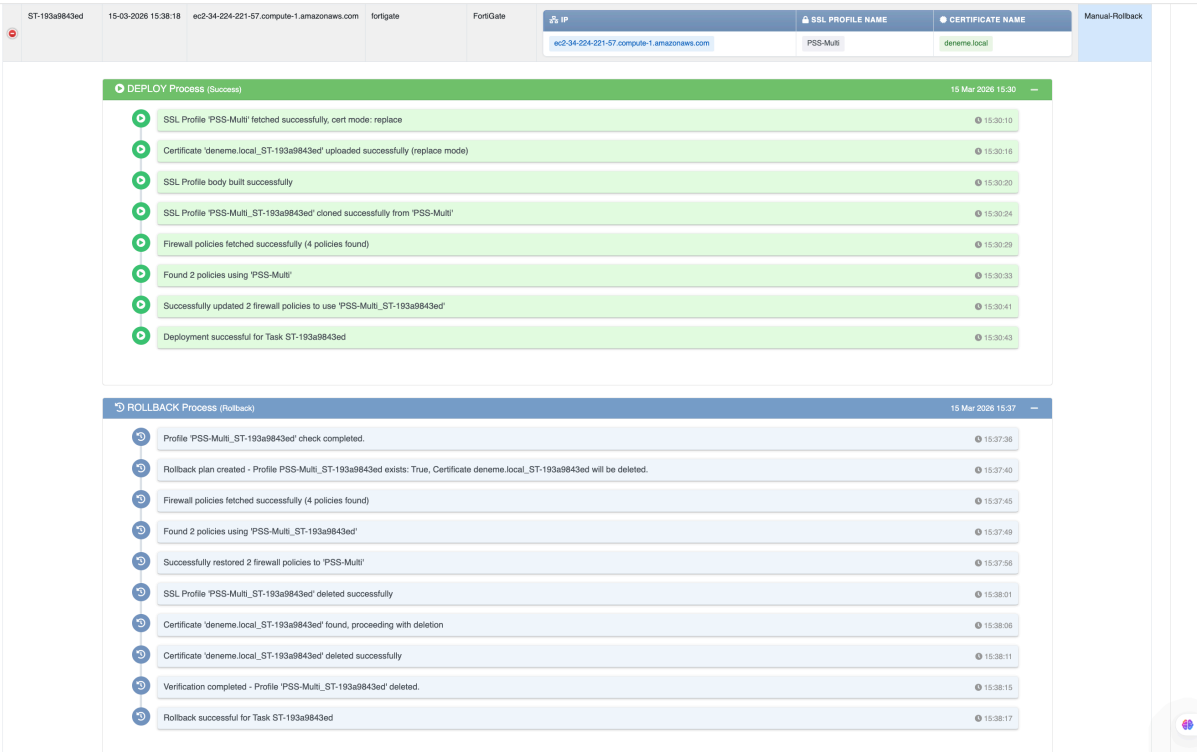


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	SSL profile is fetched and cert mode is determined
2	Certificate is uploaded to the device
3	SSL profile body is built
4	SSL profile is stored successfully
5	Firewall policies are fetched
6	Matching policies are updated to use the new profile
7	Deployment completed successfully

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback

3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Rollback plan is created and certificate to be deleted is identified
2	Firewall policies are fetched
3	Matching policies are reverted to the previous profile
4	New SSL profile is deleted
5	Certificate is deleted from the device
6	Rollback completed successfully

FortiManager

SecTrail CM enables automatic deployment and renewal of SSL certificates to all managed FortiGate devices by establishing **agentless** connections to the FortiManager central management platform.

Connection Requirements

Requirement	Detail	Description
Protocol	REST API (HTTPS)	FortiManager's native REST API is used
Port	`443`	Standard HTTPS port or custom management port
Authentication	Username and Password	Authentication via Username and Password
User Permission	Admin or Certificate Manager role	Certificate upload and configuration permission

Automated Operations

SecTrail CM automatically performs the following operations on FortiManager:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate and private key to ADOM local store
2. **Certificate Import**: Distributing certificate and key to managed devices via FortiManager
3. **SSL Profile Update**: Updating SSL inspection profiles
4. **Policy Install**: Installing updated policies to target devices
5. **Configuration Commit**: Committing workspace and making configuration persistent

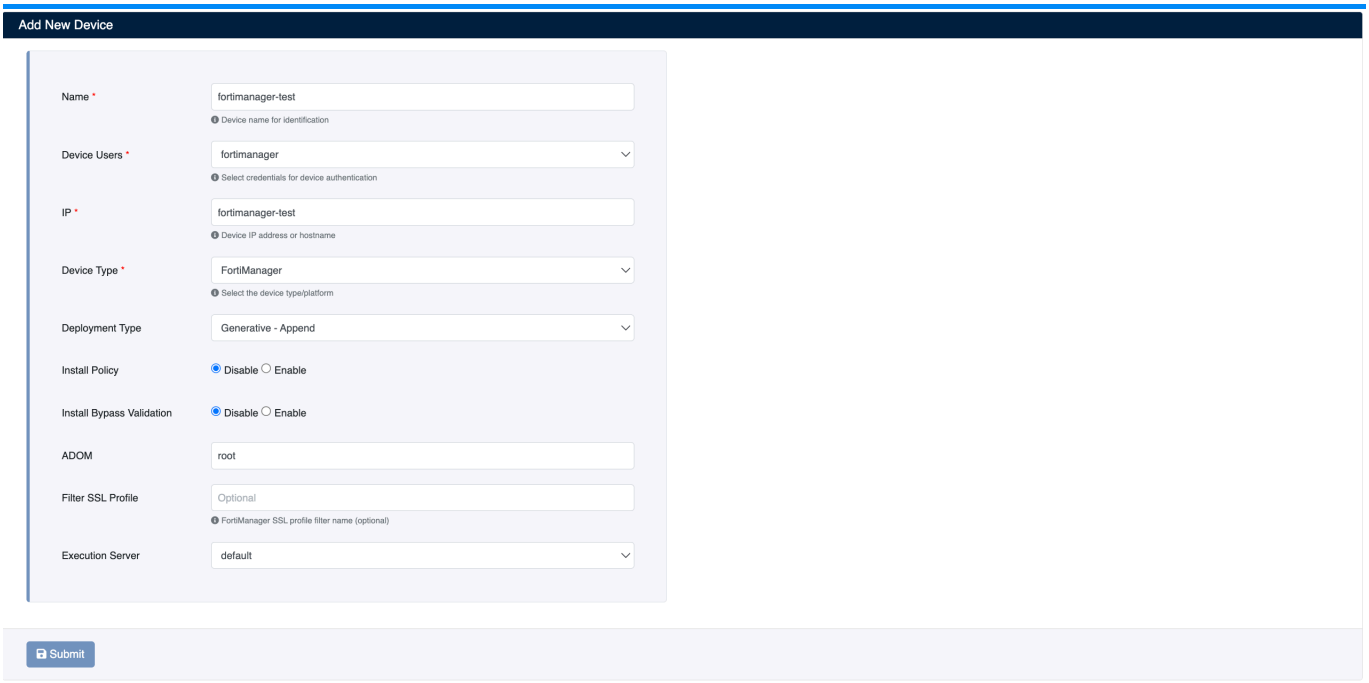
Configuration Steps

1. Creating FortiManager User

Navigate to **Automation > Device Users** and create a user for FortiManager.

2. Adding FortiManager Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

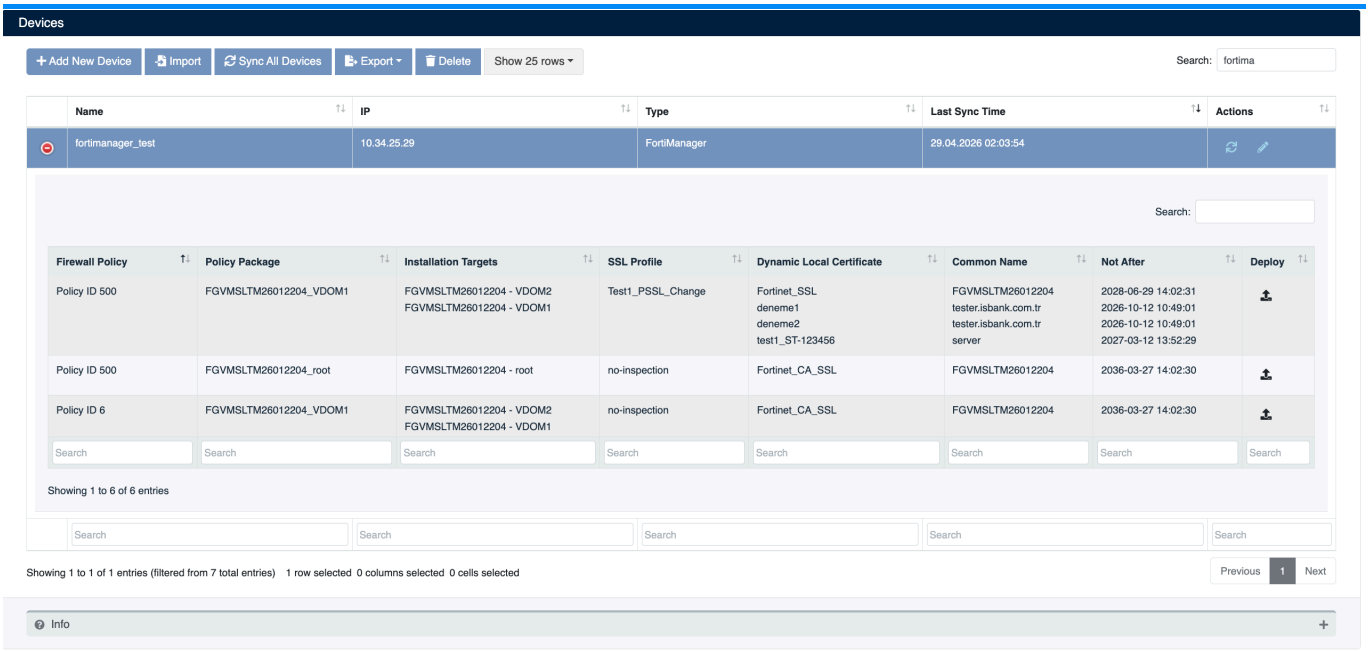


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the FortiManager management IP address or hostname
- **Device Type**: Select `FortiManager` from the dropdown menu
- **Deployment Type**: Select deployment type
- **Generative - Append**: Creates a new SSL profile, adds the new certificate to it, and associates it with matching policies
- **Generative - Replace**: Creates a new SSL profile, replaces the certificate within it, and associates it with matching policies
- **Override - Append**: Adds the new certificate to the existing SSL profile
- **Override - Replace**: Removes the current certificate from the existing SSL profile and adds the new one
- **Install Policy**: Should updated policies be installed to devices? (Disabled/Enabled)
- **Install Bypass Validation**: Should validation be bypassed during policy installation? (Disabled/Enabled)
- **ADOM**: FortiManager ADOM name (e.g. `root`)
- **Filter SSL Profile**: FortiManager SSL profile filter name (optional)
- **Execution Server**: Server to use for executing deployment operations

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the FortiManager device is added to SecTrail CM, all certificates on devices managed by FortiManager are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



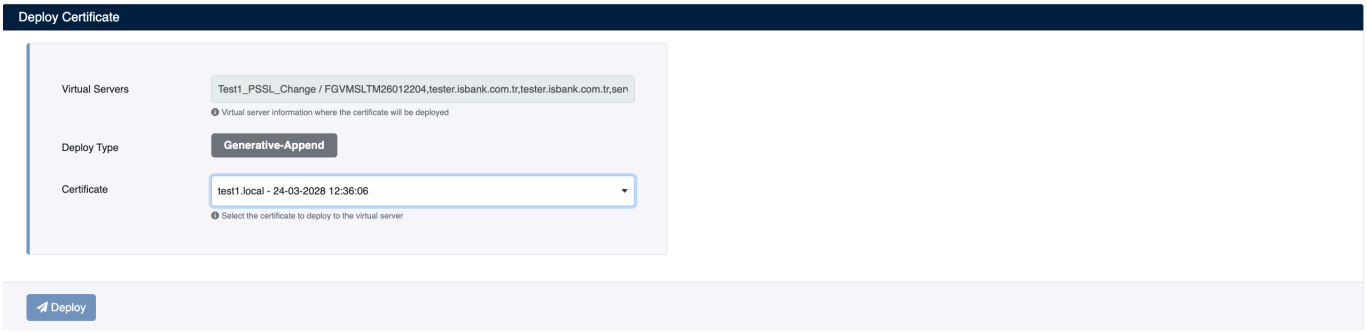
- **Firewall Policy**: Name of the firewall policy associated with the certificate
- **Policy Package**: Policy package the rule belongs to
- **Installation Targets**: Target FortiGate devices the policy will be installed to
- **SSL Profile**: SSL inspection profile name associated with the certificate
- **Dynamic Local Certificate**: Dynamic local certificate mappings on managed devices
- **Common Name**: Common Name (CN) information of the certificate
- **Not After**: Certificate expiration date
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your FortiManager device from **Automation > Devices**
2. In the device details, find the policy where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target virtual server information is displayed (SSL Profile / Installation Targets / Common Name format)
- **Deploy Type**: Displays the configured deployment type (e.g. Generative-Append)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu



Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:

Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Workspace mode is enabled, ADOM is locked
2	Certificate uploaded to ADOM local store
3	Certificate distributed to managed devices
4	Dynamic Certificate Object created in ADOM
5	Dynamic Certificate Mapping assigned to devices
6	SSL profile fetched and cloned
7	SSL Profile payload prepared and applied
8	Firewall policies updated to use new profile
9	ADOM workspace committed and policy installed
10	ADOM workspace unlocked successfully

> **COMMIT**
>
> SecTrail CM locks the ADOM workspace before deployment, commits all changes after the operation is complete, and unlocks the workspace. If **Install Policy** is enabled, the updated policy is also pushed to the target FortiGate devices.

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Workspace mode is enabled, ADOM is locked
2	SSL profiles fetched from ADOM
3	Firewall policies reverted to base profile
4	SSL Profile deleted successfully
5	Dynamic mappings deleted from managed devices
6	Dynamic Certificate Object deleted
7	Certificate deleted from ADOM and device databases
8	ADOM workspace committed successfully
9	ADOM workspace unlocked successfully

IIS (Internet Information Services)

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to Windows IIS (Internet Information Services) web servers.

Connection Requirements

Requirement	Detail	Description
Protocol	WinRM (Windows Remote Management)	Uses Windows Remote Management protocol
Port	`5986` / `5985`	HTTPS port recommended for secure connection
Transport	NTLM / Kerberos / CredSSP	Windows authentication mechanisms
Authentication	Domain account / Local Administrator	Windows user credentials

Automated Operations

SecTrail CM automatically performs the following operations on Windows IIS:

1. **Certificate Store Import**: Secure transfer of certificate and private key to Windows Certificate Store
2. **IIS Binding Update**: Updating Virtual Server (Web Site) SSL bindings
3. **Configuration Backup**: Backing up configuration before changes
4. **SSL Validation**: HTTPS connection testing and validation

Configuration Steps

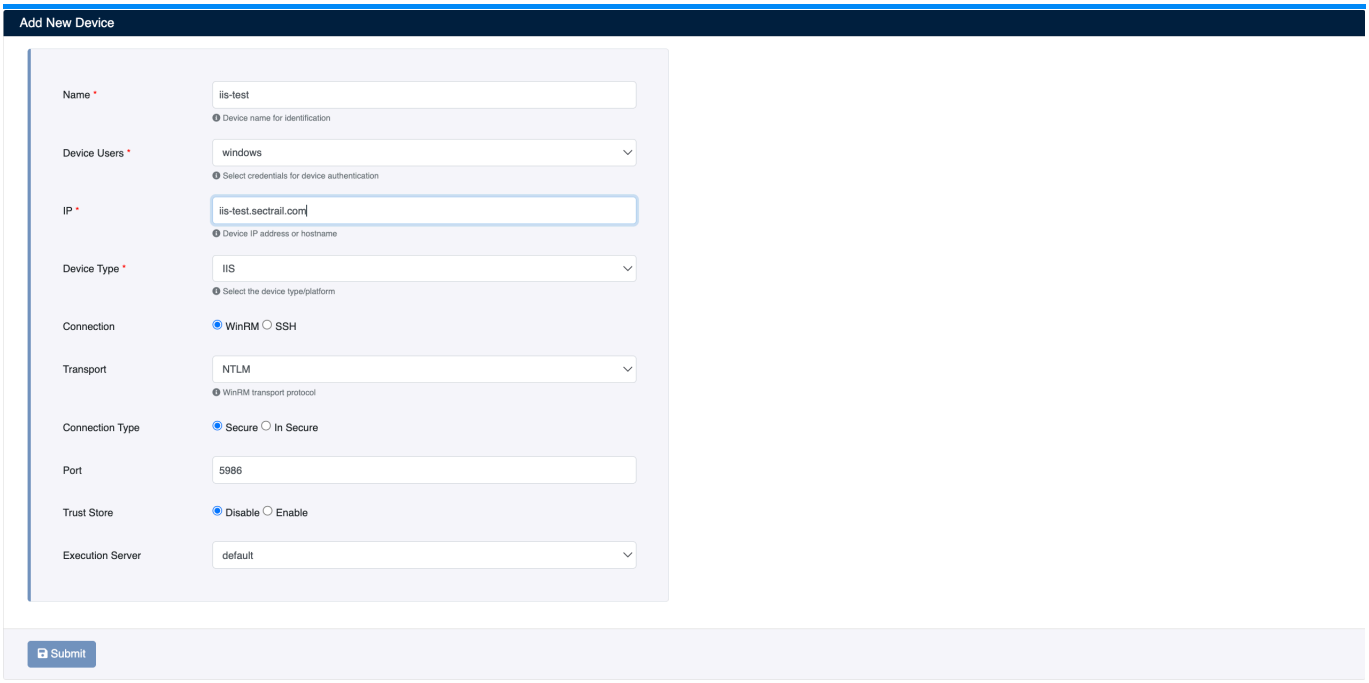
1. Creating IIS User

Navigate to **Automation > Device Users** and create a user for IIS:

- Windows domain user
- Or local administrator

2. Adding IIS Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

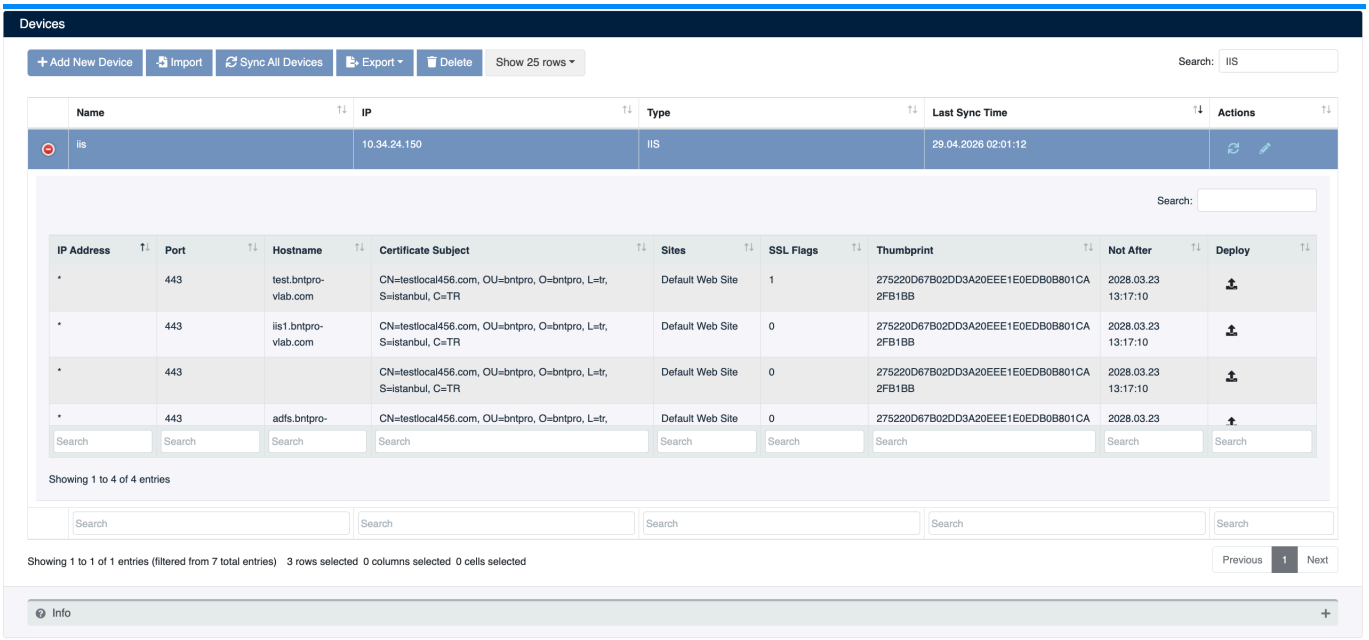


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the Windows user created in Step 1
- **IP**: Enter the IP address of the Windows IIS server
- **Device Type**: Select `IIS` from the dropdown menu
- **Connection**: Select either `WinRM` or `SSH`
- **Transport**: Select either NTLM or Kerberos
- **Connection Type**: Select `Secure` for secure connection
- **Port**: WinRM port (default: `5986` HTTPS or `5985` HTTP)
- **Trust Store**: Include Trust Store? `Disabled` or `Enabled`

> **AUTOMATIC DISCOVERY**
>
> After the IIS device is added to SecTrail CM, the IP addresses and ports of all Web Sites defined on the device are automatically included in the discovery period and scanned regularly.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



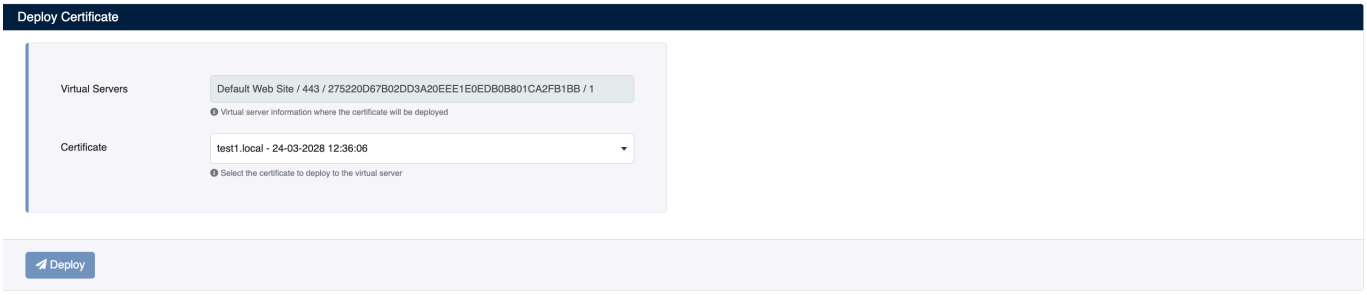
- **IP Address**: IP address of the IIS server
- **Port**: HTTPS port (443)
- **Hostname**: Hostname information of the IIS website
- **Certificate Subject**: Subject (CN) information of the current certificate
- **Sites**: IIS site name (Default Web Site or custom site name)
- **SSL Flags**: SSL flag value (0: no SNI, 1: SNI present)
- **Thumbprint**: Thumbprint value of the current certificate
- **Not After**: Certificate expiration date
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your IIS device from **Automation > Devices**
2. In the device details, find the **Virtual Server** (Web Site binding) where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Server information is displayed (Hostname, IP, Port)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

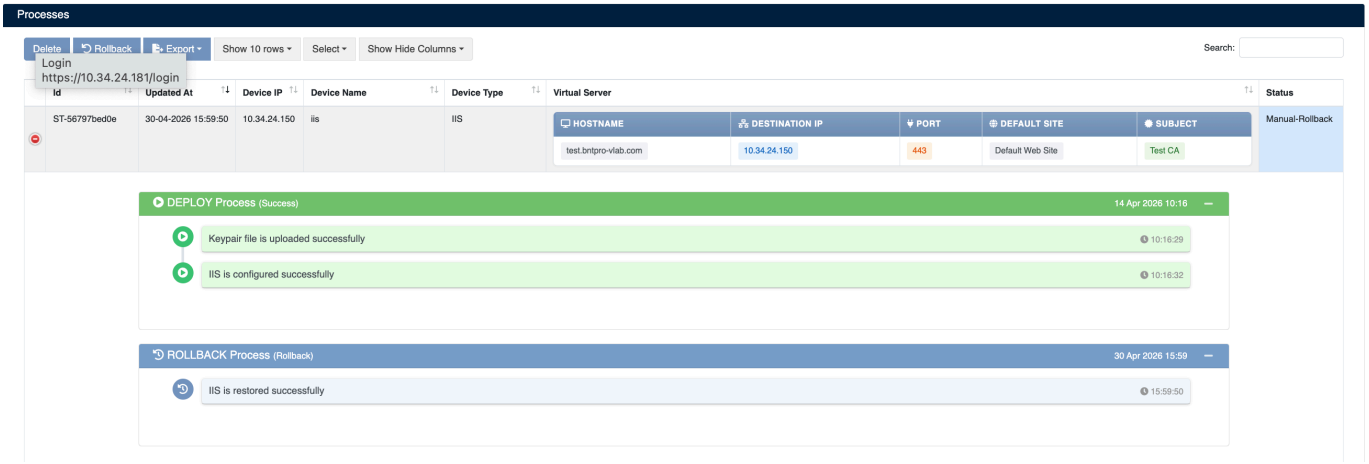


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate is imported to Windows Certificate Store in PFX format
2	IIS website SSL binding configuration is updated

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	IIS website SSL binding is reverted to its previous state
2	Old certificate binding is restored

Apache HTTP Server

SecTrail CM establishes **agent-less** connections to Apache HTTP Servers to enable automatic deployment and renewal of SSL certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	SSH (Secure Shell)	Secure remote connection protocol
Port	`22`	Standard SSH port or custom port
Authentication	SSH Key or Password	Authentication with SSH key or password
User Permission	Configuration read/write permission	Access and edit permission for Apache config files

Automatic Operations

SecTrail CM automatically performs the following operations on Apache HTTP Server:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate, private key, and chain file
2. **Configuration Update**: Updating Apache VirtualHost SSL directives
3. **Configuration Test**: Syntax check and validation
4. **Service Reload**: Seamless reloading of Apache service

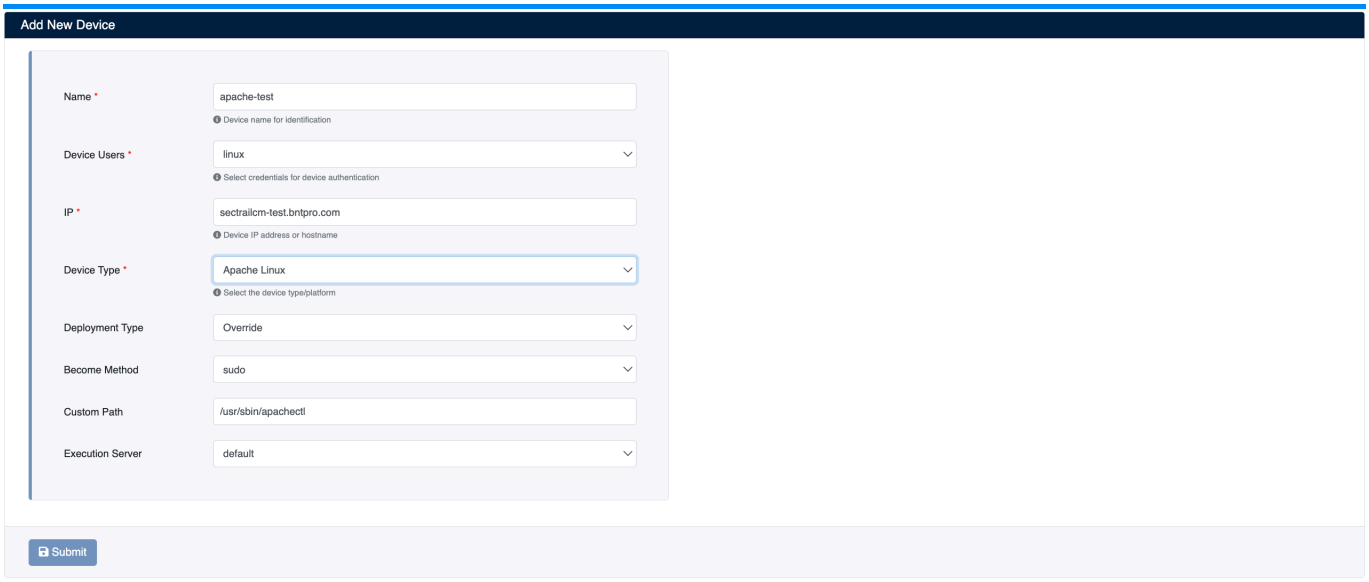
Configuration Steps

1. Create Apache Linux User

Navigate to **Automation > Device Users** and create a user for Apache.

2. Add Apache Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

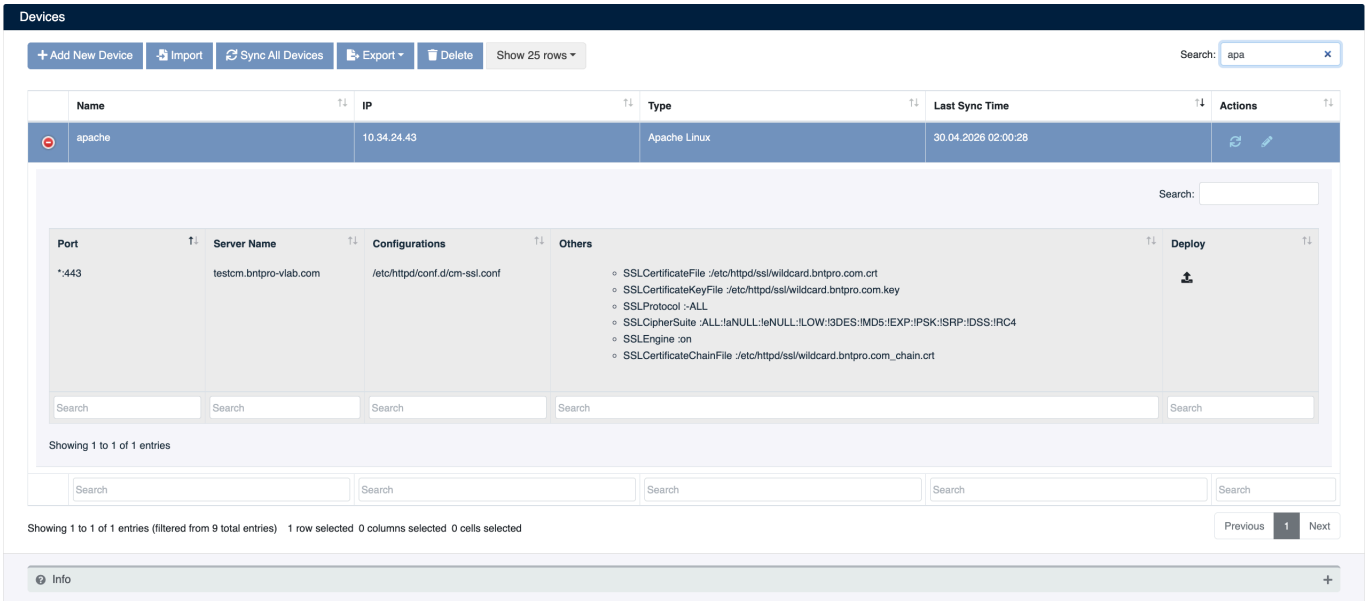


- **Name**: Give a descriptive name for the device
- **Device Users**: Select the user you created in Step 1
- **IP**: Enter the IP address of the Apache server
- **Device Type**: Select `Apache Linux` from the dropdown menu
- **Become Method**: Select privilege escalation method
- **Custom Path**: Enter the path to the Apache binary file (e.g., `/usr/sbin/apachectl`)

> **AUTOMATIC DISCOVERY**
>
> After the Apache device is added to SecTrail CM, IP addresses and ports of all Virtual Hosts defined on the device are automatically included in the discovery period and regularly scanned.

3. View Device Information

After adding a device, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



- **Port**: Ports Apache is listening on (e.g., `*:443`, `*:444`)

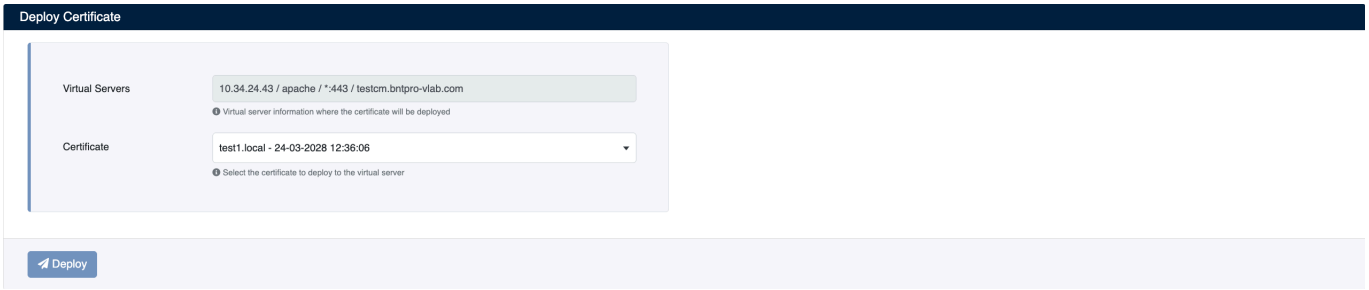
- **Server Name**: VirtualHost server name or `*` (all hosts)
- **Configurations**: Apache configuration file path (e.g., `/etc/httpd/conf.d/cm-ssl.conf`)
- **Others**: Current SSL configuration details
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Host and Certificate Selection

1. Select your Apache device from the **Automation > Devices** section
2. In the device details, find the **Virtual Host** you want to deploy a certificate to
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Host information is displayed (IP, port, server name)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

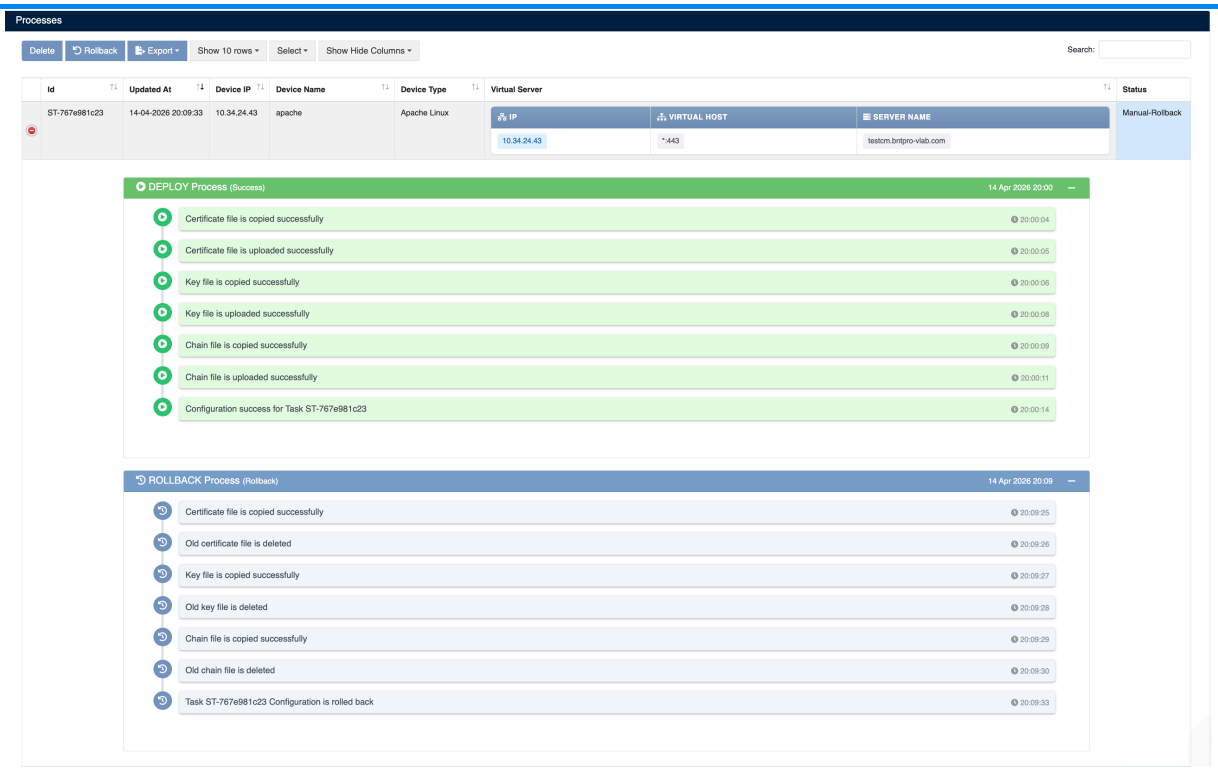


Step 2: Start Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from the **Automation > Processes** section:



Process Details

The following steps are performed during deployment:

Step	Process Description
1	Certificate, key, and chain files are uploaded to the server
2	Current certificate files are backed up
3	New certificate configuration is applied
4	Apache service is reloaded

Rollback Process

If problems occur after certificate deployment, the **Manual Rollback** feature can be used.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs during any step of the deployment process, the system automatically performs the rollback operation and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the process you want to roll back
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	New configuration is removed
2	Backed up certificate files are restored
3	Newly uploaded certificate, key, and chain files are deleted
4	Apache service is reloaded

NGINX

SecTrail CM establishes **agent-less** connections to NGINX web servers to enable automatic deployment and renewal of SSL certificates.

Connection Requirements

Requirement	Detail	Description
Protocol	SSH (Secure Shell)	Secure remote connection protocol
Port	`22`	Standard SSH port or custom port
Authentication	SSH Key or Password	Authentication with SSH key or password
User Permission	Configuration read/write permission	Access and edit permission for NGINX config files

Automatic Operations

SecTrail CM automatically performs the following operations on NGINX:

1. **Certificate and Key Upload**: Secure transfer of SSL certificate, private key, and chain file
2. **Configuration Update**: Updating NGINX Server Block SSL directives
3. **Configuration Test**: Syntax check and validation
4. **Service Reload**: Seamless reloading of NGINX service

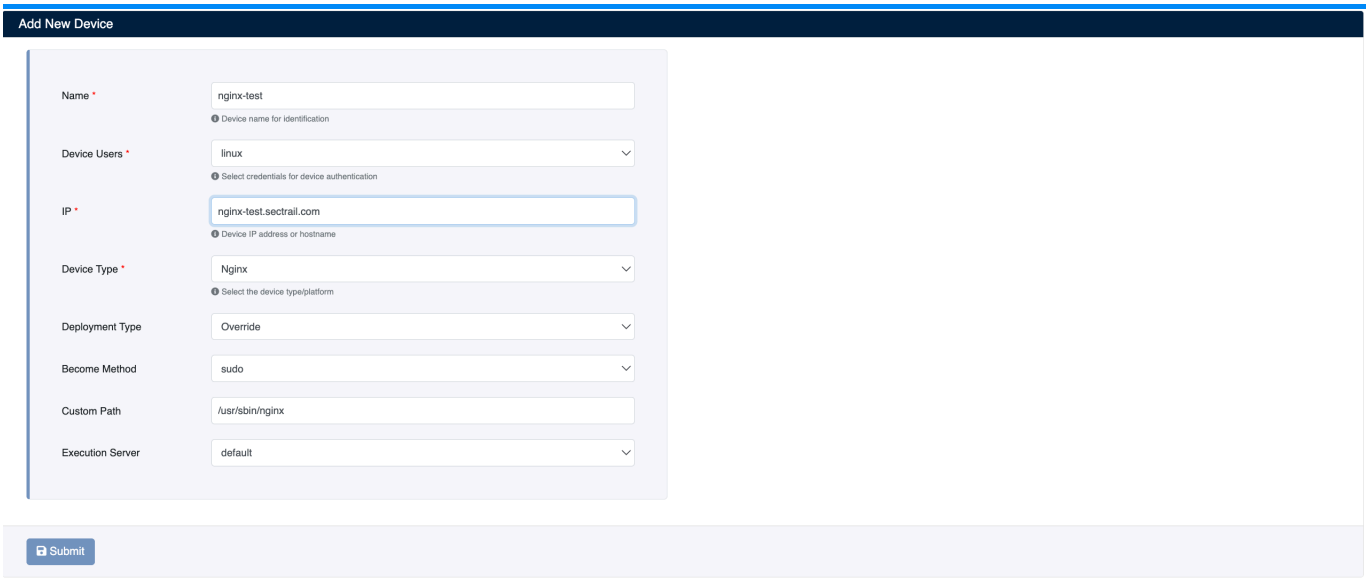
Configuration Steps

1. Create NGINX Linux User

Navigate to **Automation > Device Users** and create a user for NGINX.

2. Add NGINX Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

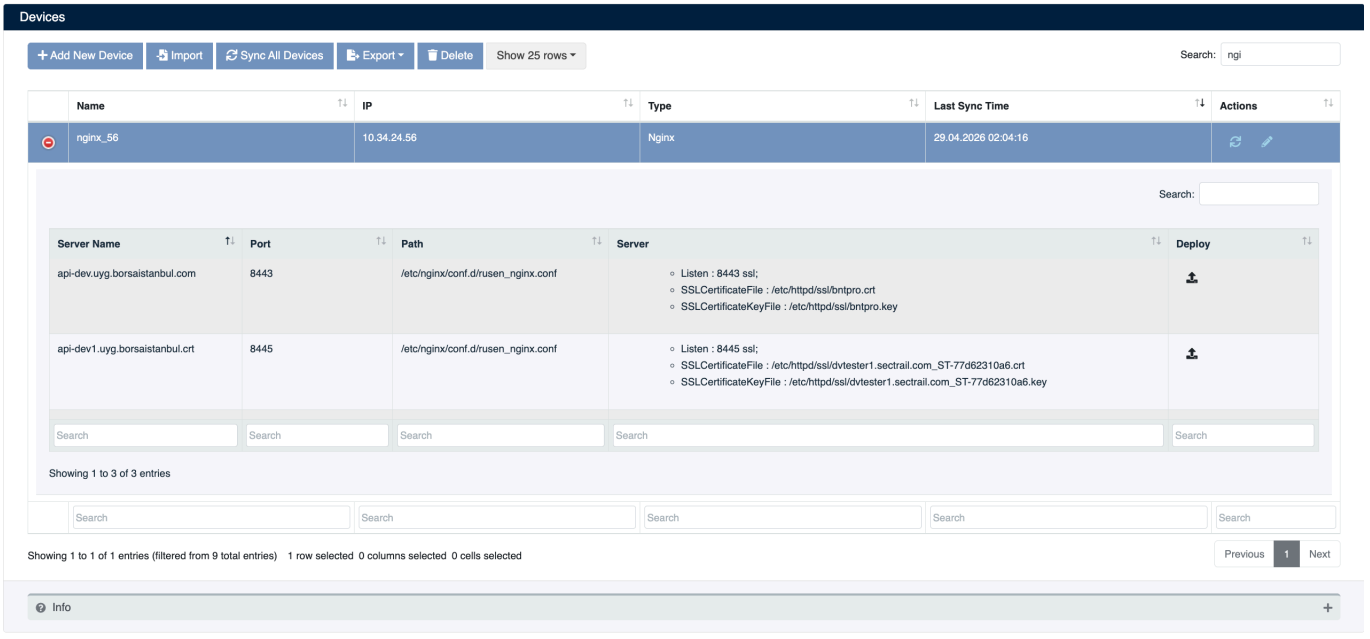


- **Name**: Give a descriptive name for the device
- **Device Users**: Select the user you created in Step 1
- **IP**: Enter the IP address of the NGINX server
- **Device Type**: Select `Nginx` from the dropdown menu
- **Become Method**: Select privilege escalation method (e.g., `sudo`)
- **Custom Path**: Enter the path to the NGINX binary file (e.g., `/usr/sbin/nginx`)

> **AUTOMATIC DISCOVERY**
>
> After the NGINX device is added to SecTrail CM, IP addresses and ports of all Server Blocks defined on the device are automatically included in the discovery period and regularly scanned.

3. View Device Information

After adding a device, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



- **Server Name**: Server block server name (e.g., `sectrailcm-test.borsaistanbul.com`)

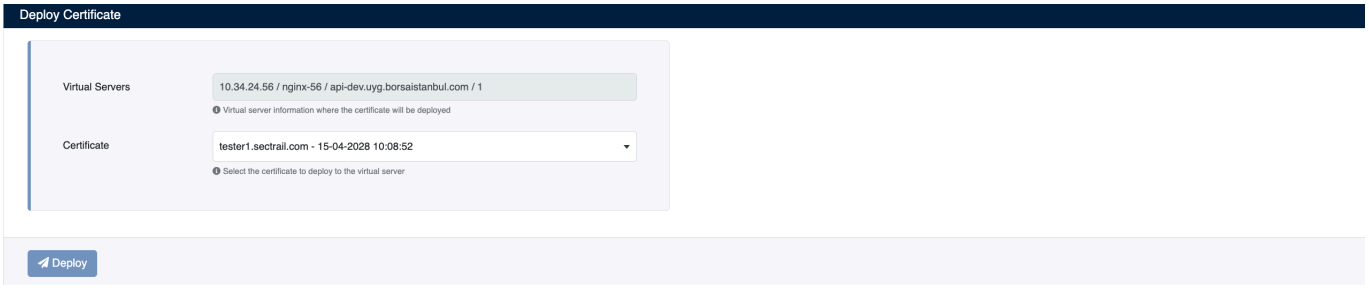
- **Port**: Ports NGINX is listening on (e.g., `8443`)
- **Path**: NGINX configuration file path (e.g., `/etc/nginx/conf.d/domain_nginx.conf`)
- **Server**: SSL configuration details
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Server Block and Certificate Selection

1. Select your NGINX device from the **Automation > Devices** section
2. In the device details, find the **Server Block** you want to deploy a certificate to
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Server Block information is displayed (IP, port, server name)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

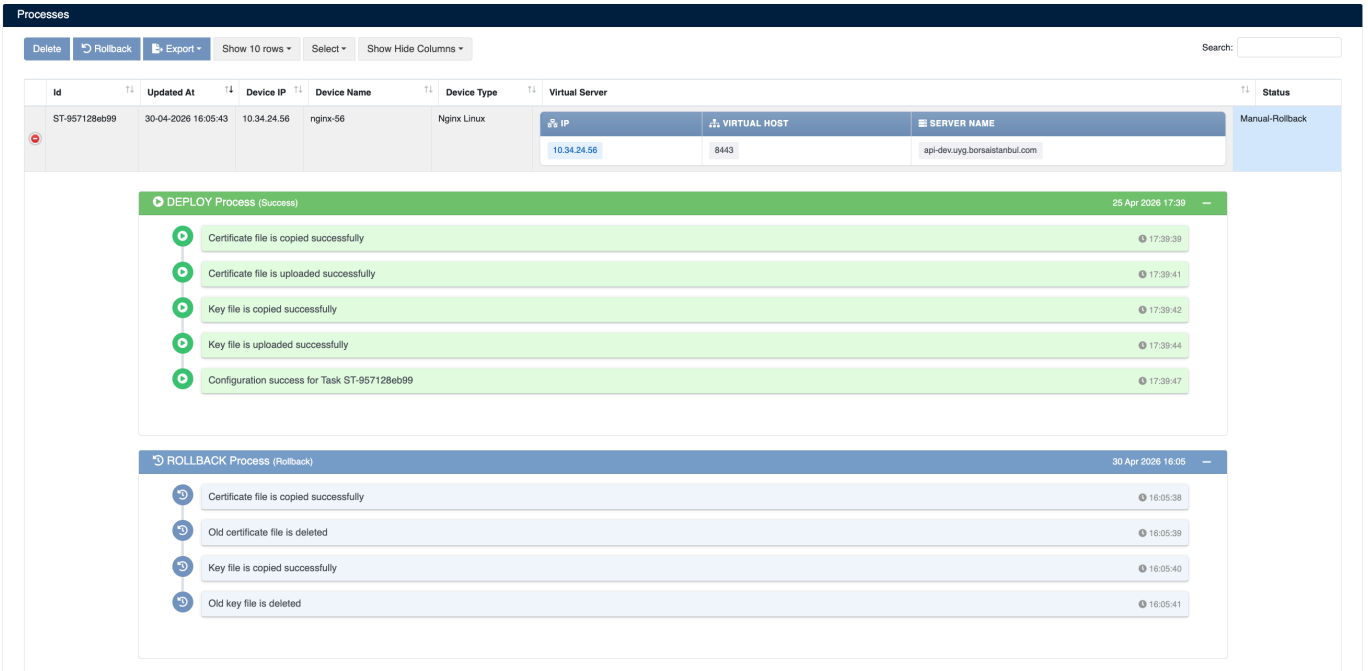


Step 2: Start Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from the **Automation > Processes** section:



Process Details

The following steps are performed during deployment:

Step	Process Description
1	Certificate, key, and chain files are uploaded to the server
2	Current certificate files are backed up
3	New certificate configuration is applied
4	NGINX service is reloaded

Rollback Process

If problems occur after certificate deployment, the **Manual Rollback** feature can be used.

> **AUTOMATIC ROLLBACK**
>
> If an error occurs during any step of the deployment process, the system automatically performs the rollback operation and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the process you want to roll back
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	New configuration is removed
2	Backed up certificate files are restored
3	Newly uploaded certificate, key, and chain files are deleted
4	NGINX service is reloaded

Apache Tomcat

SecTrail CM enables automatic deployment and renewal of SSL certificates by establishing **agentless** connections to Apache Tomcat application servers.

Connection Requirements

Requirement	Detail	Description
Protocol	SSH (Secure Shell)	Secure remote connection protocol
Port	`22` (default)	Standard SSH port or custom port
Authentication	SSH Key or Password	Authentication via SSH key or password
User Permission	Keystore and restart permission	Java keystore creation and Tomcat restart permission

Automated Operations

SecTrail CM automatically performs the following operations on Apache Tomcat:

1. **Keystore Management**: Creating and updating Java KeyStore (JKS/PKCS12)
2. **Certificate Import**: Adding SSL certificate and private key to keystore
3. **Configuration Update**: Updating Tomcat server.xml SSL connector settings
4. **Service Refresh**: Restarting Tomcat service

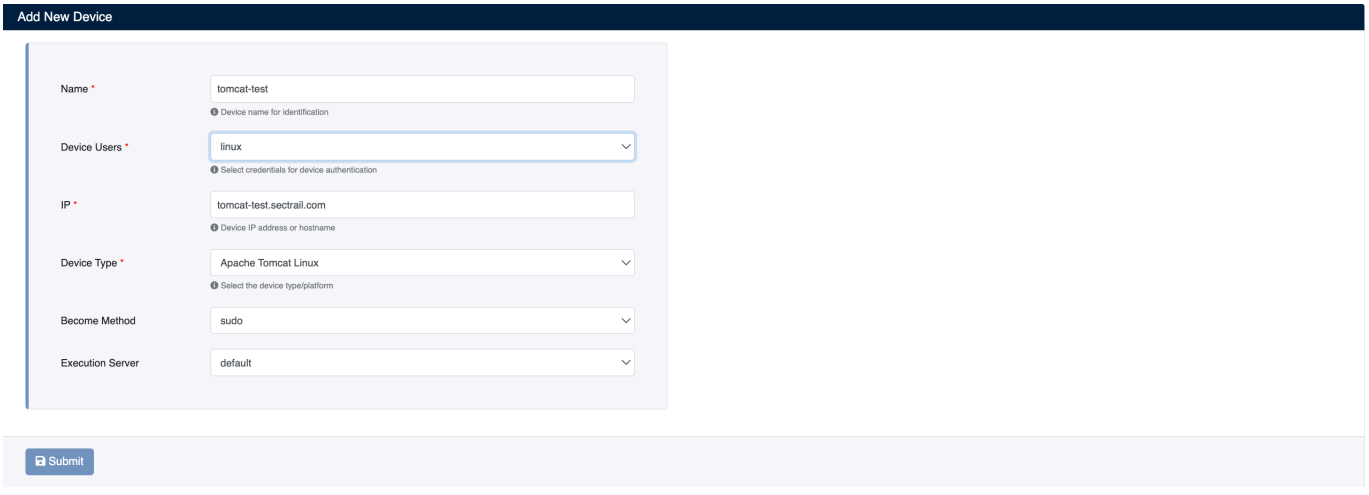
Configuration Steps

1. Creating Tomcat Linux User

Navigate to **Automation > Device Users** and create a user for Tomcat.

2. Adding Tomcat Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

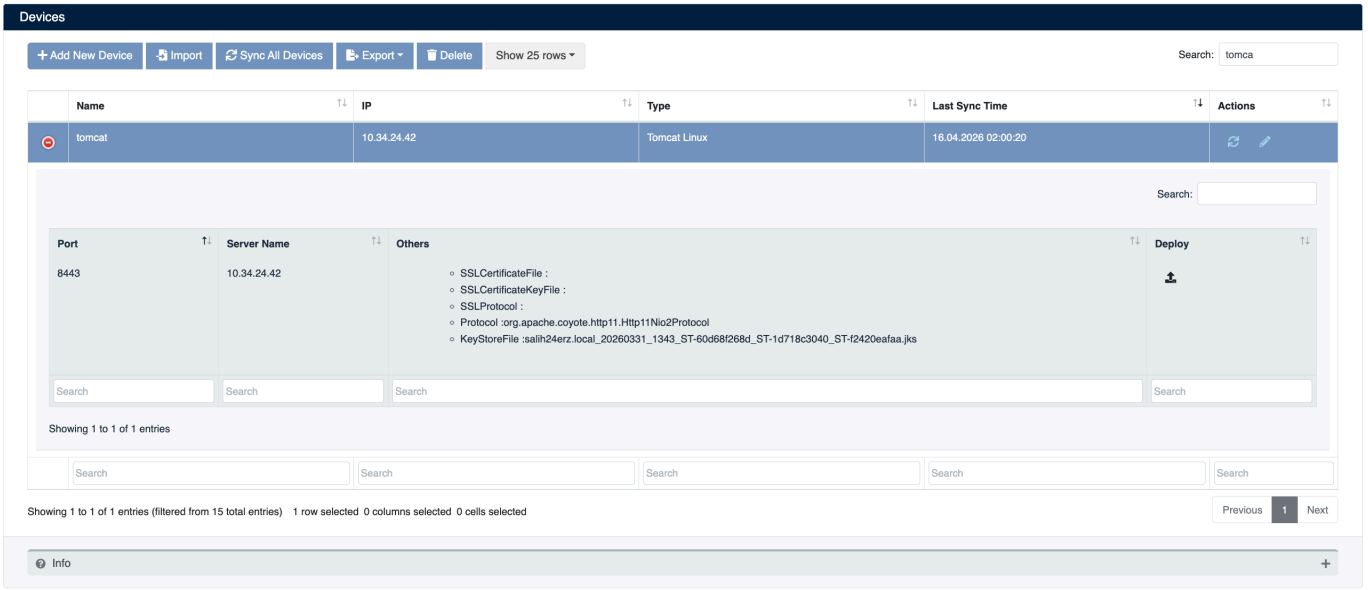


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the IP address of the Tomcat server
- **Device Type**: Select `Apache Tomcat Linux` from the dropdown menu
- **Become Method**: Select privilege escalation method (e.g., `sudo`)

> **AUTOMATIC DISCOVERY**
>
> After the Tomcat device is added to SecTrail CM, the IP addresses and ports of all Virtual Servers defined on the device are automatically included in the discovery period and scanned regularly.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



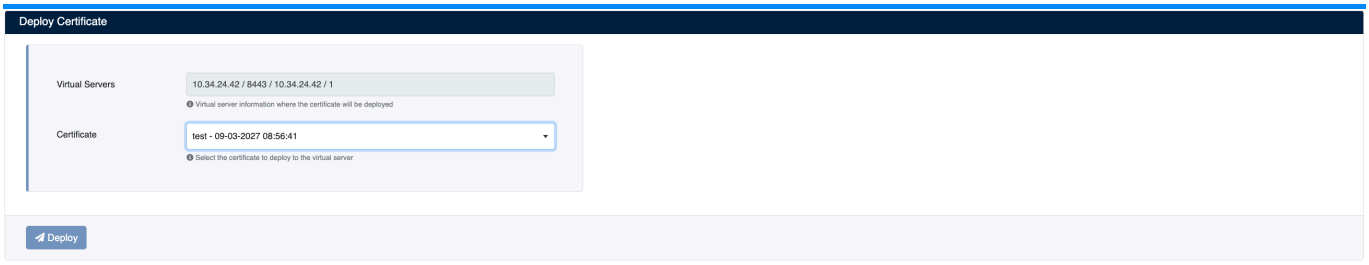
- **Port**: SSL ports that Tomcat listens on (e.g., `8446`, `8448`)
- **Server Name**: Virtual server IP address (e.g., `10.34.24.42`)
- **Others**: Current SSL configuration details
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: Virtual Server and Certificate Selection

1. Select your Tomcat device from **Automation > Devices**
2. In the device details, find the **Virtual Server** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target Virtual Server information is displayed (IP and port)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

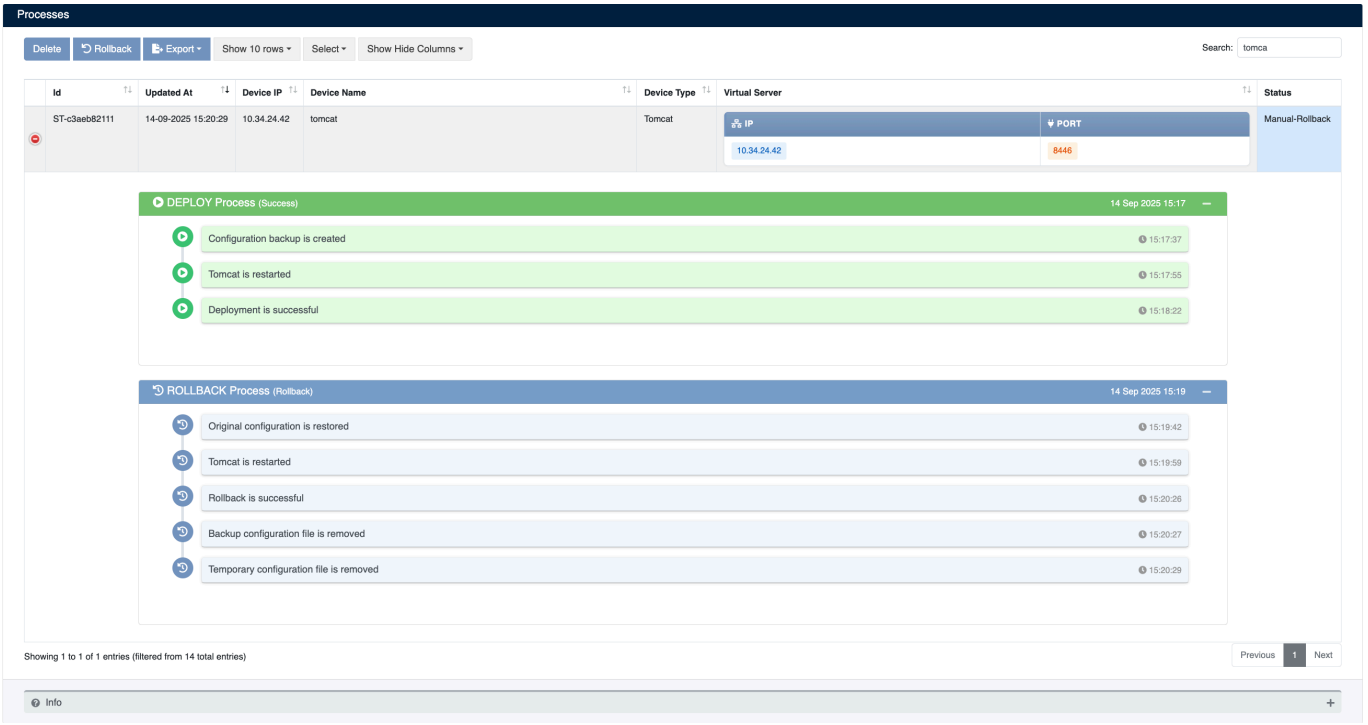


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Configuration backup file is created
2	JKS (Java KeyStore) file is created and certificate is loaded
3	Changes are made in the configuration file
4	Tomcat service is restarted

Rollback Operation

The **Manual Rollback** feature can be used in case of issues after certificate deployment.

AUTOMATIC ROLLBACK

If an error occurs at any step during the deployment process, the system automatically performs a rollback and all changes are reverted.

Rollback Steps

1. Navigate to **Automation > Processes**
2. Find the operation you want to rollback
3. Use the **Manual-Rollback** option in the **Status** column
4. Confirm

Operations During Rollback

Step	Operation
1	Original configuration is restored
2	Tomcat service is restarted
3	Newly created keystore file is removed
4	Backup and temporary files are cleaned up

Java Keystore (JKS)

SecTrail CM enables automatic management of SSL certificates by establishing **agentless** connections to applications using Java Keystore (JKS/PKCS12).

> **PLATFORM SUPPORT**
>
> SecTrail CM supports Java KeyStores running on both **Linux** and **Windows** systems. You can perform automatic certificate deployment and management for both platforms.

Use Cases

- **Java Applications**: Standalone Java applications
- **Microservices**: Spring Boot, Quarkus, Micronaut microservices
- **Message Brokers**: Apache Kafka, RabbitMQ (TLS)
- **Databases**: Elasticsearch, Cassandra (SSL/TLS)

Connection Requirements

Linux Systems

Requirement	Detail	Description
Protocol	SSH (Secure Shell)	Secure remote connection protocol
Port	`22`	Standard SSH port or custom port
Authentication	SSH Key or Password	Authentication via SSH key or password
User Permission	Keystore read/write permission	Access and edit permission to keystore files

Windows Systems

Requirement	Detail	Description
Protocol	WinRM (Windows Remote Management)	Windows remote management protocol
Port	`5985` (HTTP) / `5986` (HTTPS)	Standard WinRM ports
Authentication	Username and Password	Windows user authentication
User Permission	Keystore read/write permission	Access and edit permission to keystore files

Automated Operations

SecTrail CM automatically performs the following operations on Java KeyStore:

1. **Keystore Backup**: Backing up the existing keystore
2. **Certificate Import**: Importing new certificate and private key with `keytool`

3. **Truststore Update**: Adding Root/Intermediate CA certificates to truststore
4. **Validation**: SSL/TLS connection testing and validation

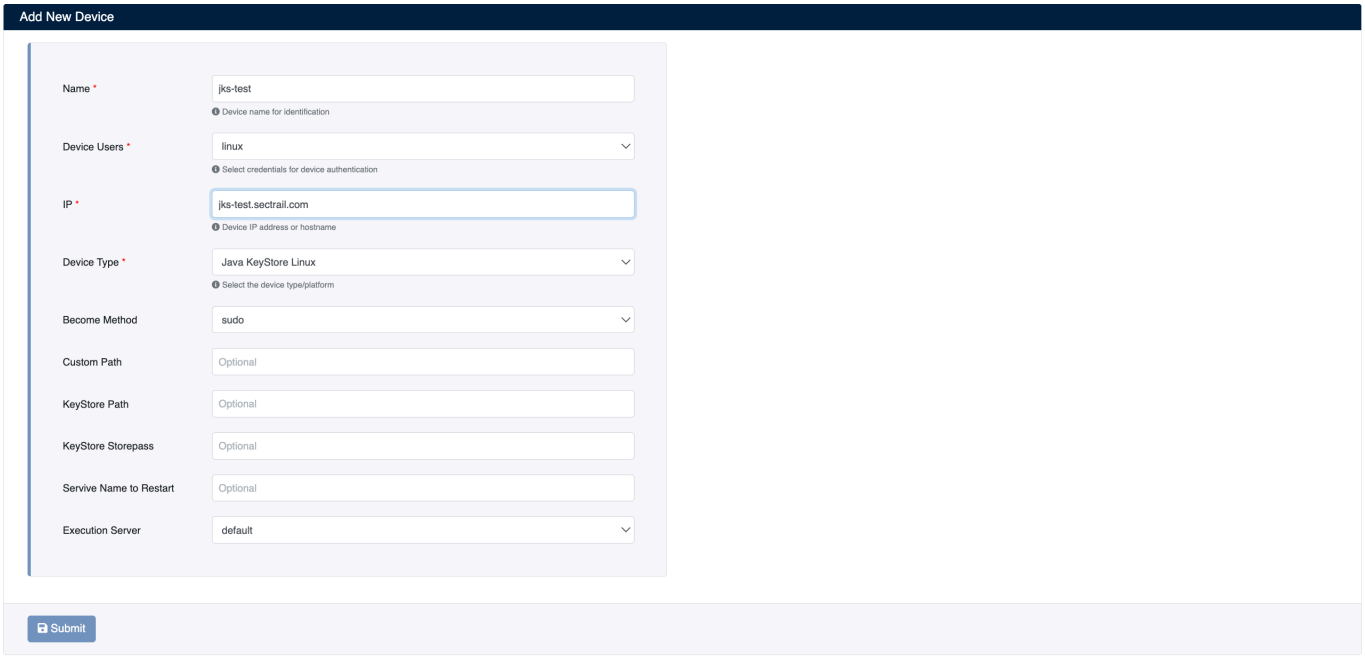
Configuration Steps

1. Creating Java KeyStore Linux User

Navigate to **Automation > Device Users** and create a user for Java KeyStore.

2. Adding Java KeyStore Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:

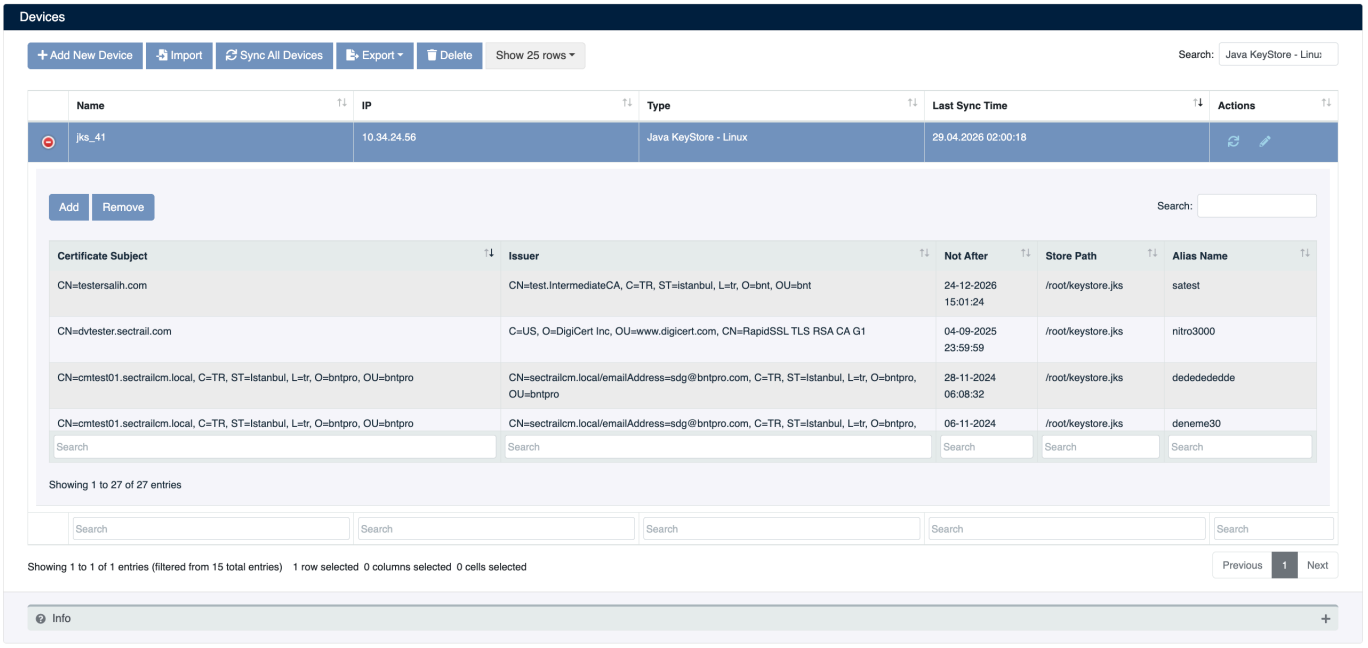


- **Name**: Provide a descriptive name for the device
- **Device Users**: Select the user created in Step 1
- **IP**: Enter the IP address of the Java KeyStore server
- **Device Type**: Select `Java KeyStore Linux` from the dropdown menu
- **Become Method**: Select privilege escalation method (e.g., `sudo`)
- **Custom Path**: (Optional) You can specify a custom path
- **KeyStore Path**: Enter the path to the KeyStore file
- **KeyStore Storepass**: Enter the KeyStore password
- **Service Name to Restart**: (Optional) Enter the service name to restart

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the Java KeyStore device is added to SecTrail CM, certificates in the KeyStore are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



The following information is displayed in device details:

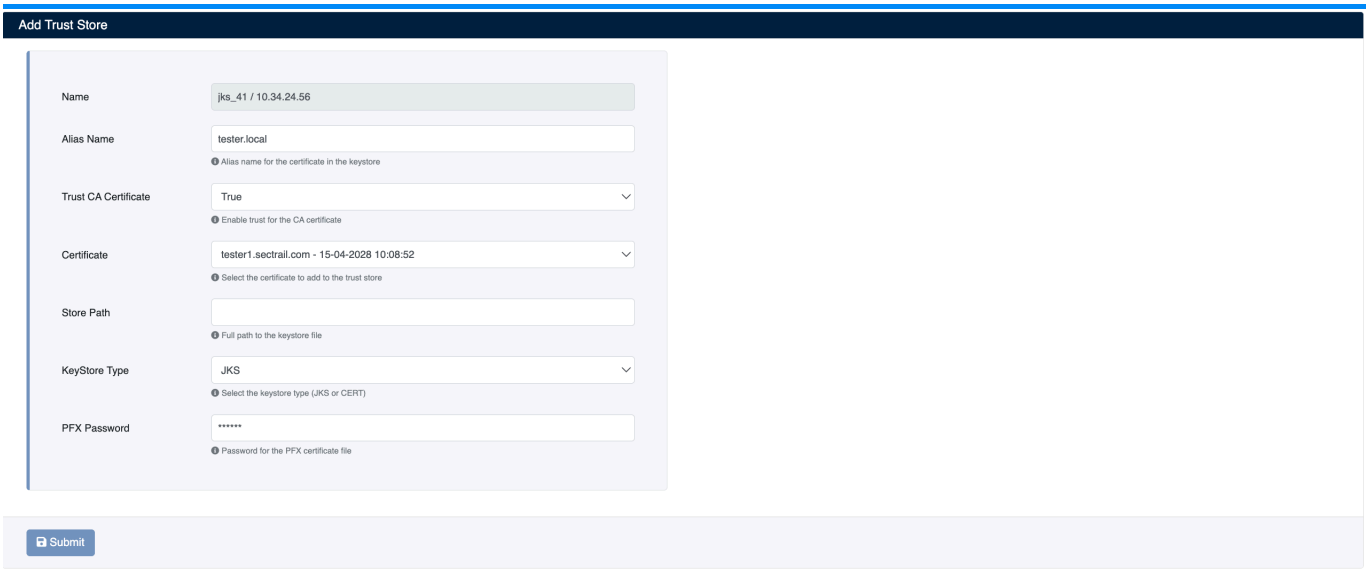
- **Certificate Subject**: Certificate subject information (CN, ST, L, O, OU)
- **Issuer**: CA information that issued the certificate
- **Not After**: Certificate expiration date
- **Store Path**: KeyStore file path
- **Alias Name**: Certificate alias name
- **Deploy**: For certificate deployment

Certificate Deployment

Step 1: KeyStore and Certificate Selection

1. Select your Java KeyStore device from **Automation > Devices**
2. In the device details, find the **KeyStore** where you want to deploy the certificate
3. Click the **Deploy** button on the relevant row
4. In the **Deploy Certificate** window that opens:

- **Virtual Servers**: Target KeyStore information is displayed (IP, Subject, Alias Name)
- **Certificate**: Select the certificate you want to deploy from the dropdown menu

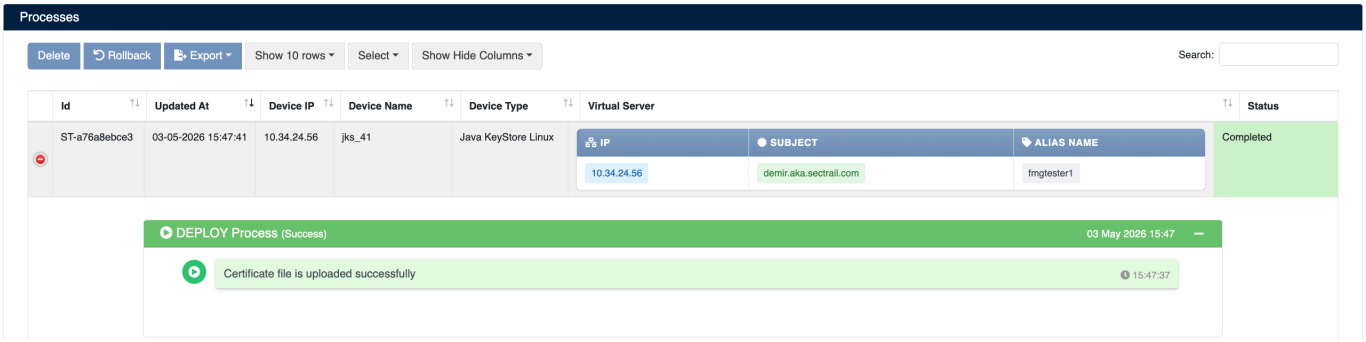


Step 2: Starting the Deployment Process

Click the **Deploy** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



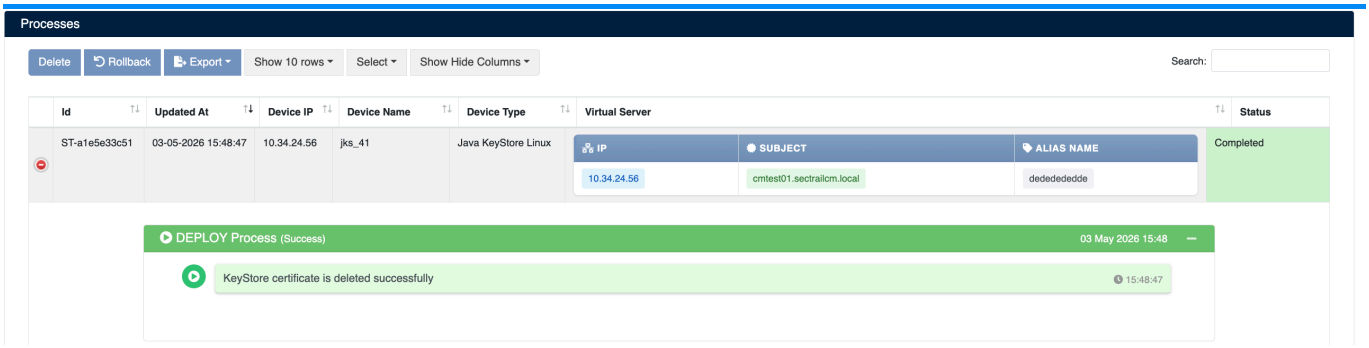
Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate file is uploaded to the server
2	New certificate is added to existing keystore file

Certificate Removal (Remove)

SecTrail CM supports certificate removal from Java KeyStore.



Removal Operation Steps

1. Select your Java KeyStore device from **Automation > Devices**
2. Select the relevant operation in the row of the certificate you want to remove
3. Confirm to start the removal operation

Removal Operation Task Details

The removal operation can be tracked from **Automation > Processes**. The following steps are performed during the operation:

Step	Operation Description
1	Existing keystore file is backed up
2	Certificate is deleted from keystore with specified alias

Windows TrustStore

SecTrail CM enables automatic management of trusted certificates (Trusted Root and Intermediate CA) by establishing **agentless** connections to Windows TrustStore.

> **PLATFORM SUPPORT**
>
> SecTrail CM supports TrustStores running on Windows systems. You can perform automatic certificate deployment and management via WinRM protocol.

Use Cases

- **Trusted Root CA Management**: Centralized management of Root CA certificates
- **Intermediate CA Certificates**: Distribution of intermediate CA certificates
- **Corporate PKI**: Enterprise PKI infrastructure management
- **Certificate Chain Management**: Establishing certificate chain trust relationships

Connection Requirements

Requirement	Detail	Description
Protocol	WinRM (Windows Remote Management)	Windows remote management protocol
Port	`5986` or `5985`	Secure WinRM port (recommended)
Authentication	Username and Password	Windows user authentication
Transport	NTLM or Kerberos	Windows authentication protocol
User Permission	Certificate Store management permission	Permission to add/remove certificates to TrustStore

Automated Operations

SecTrail CM automatically performs the following operations on Windows TrustStore:

1. **Certificate Discovery**: Listing existing TrustStore certificates
2. **Certificate Import**: Adding trusted certificates to TrustStore
3. **Certificate Remove**: Removing existing certificates from TrustStore
4. **Validation**: Certificate validity and chain testing

Supported Certificate Stores

Store Location	Description
LocalMachine	Machine-based certificate store
My	Personal certificates
Root	Trusted root CA certificates
CA	Intermediate CA certificates

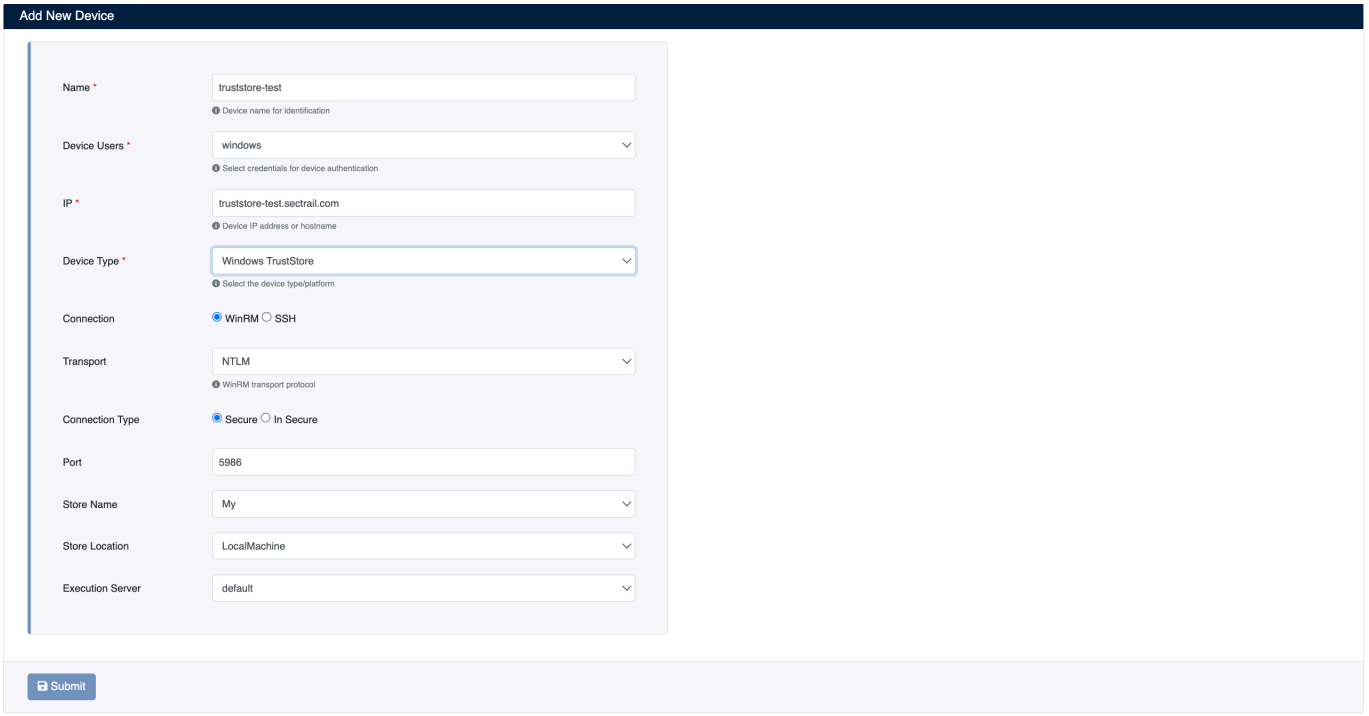
Configuration Steps

1. Creating Windows TrustStore User

Navigate to **Automation > Device Users** and create a user for Windows TrustStore.

2. Adding Windows TrustStore Device to SecTrail CM

Click **Automation > Devices > Add New Device** button and enter the following information:



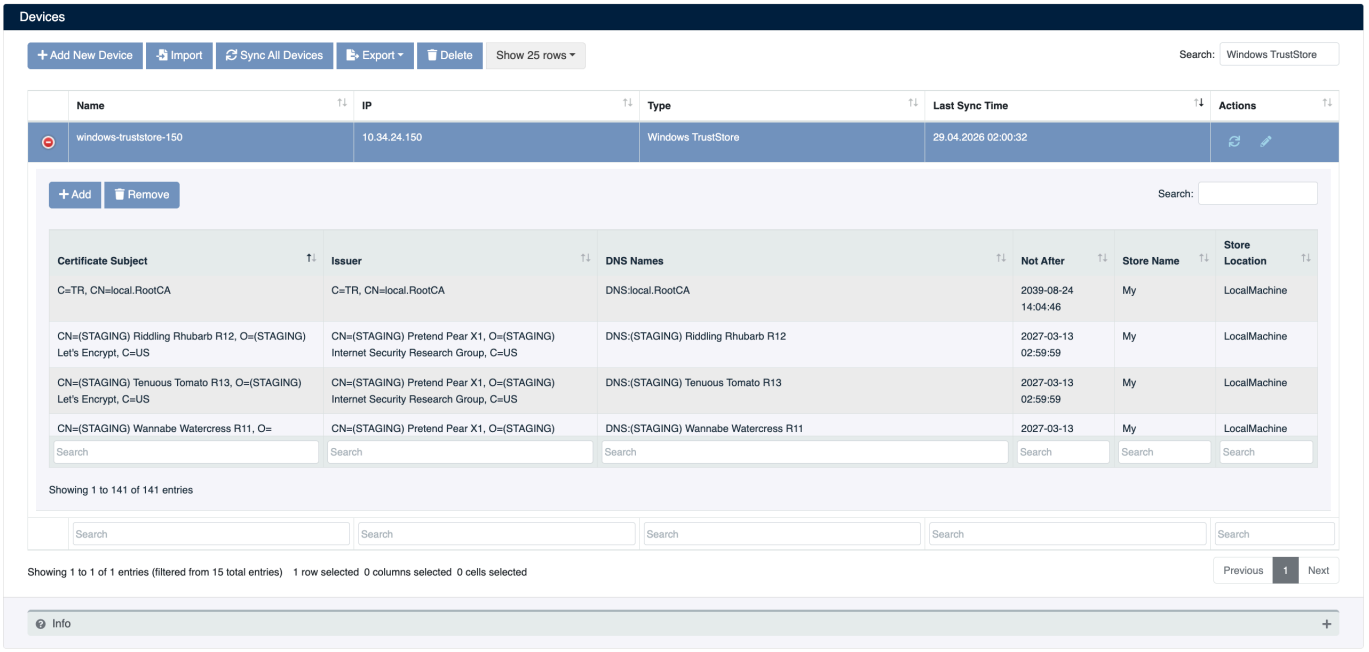
- **Name**: Provide a descriptive name for the device (e.g., `wintrust`)
- **Device Users**: Select the user created in Step 1 (e.g., `windows`)
- **IP**: Enter the IP address of the Windows TrustStore server (e.g., `10.34.24.150`)
- **Device Type**: Select `Windows TrustStore` from the dropdown menu
- **Connection**: Select `WinRM` or `SSH` (WinRM recommended for Windows)
- **Transport**: Select `NTLM` (or Kerberos)
- **Connection Type**: Select `Secure` (for HTTPS)
- **Port**: Enter WinRM port (e.g., `5986`)

- **Store Name**: Select store name (e.g., `My`)
- **Store Location**: Select store location (e.g., `LocalMachine`)

> **AUTOMATIC DISCOVERY AND MONITORING**
>
> After the Windows TrustStore device is added to SecTrail CM, certificates in the TrustStore are automatically included in the discovery period and scanned regularly. Automatic alarms are created for certificates that are about to expire or have issues.

3. Viewing Device Information

After the device is added, it will be displayed in the **Automation > Devices** list. Click on the row to view device details:



The following information is displayed in device details:

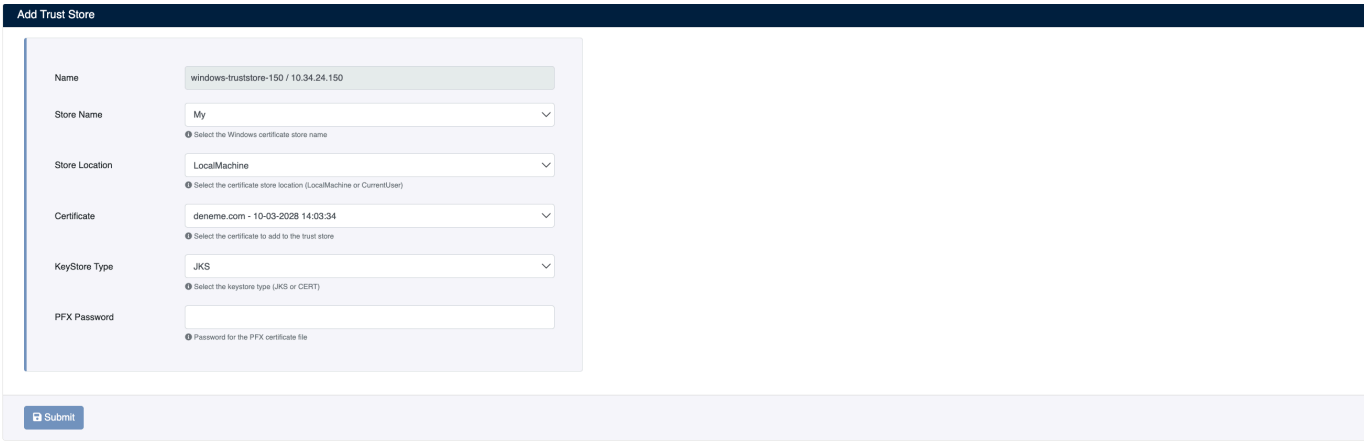
- **Certificate Subject**: Certificate subject information (CN, ST, L, O, OU)
- **Issuer**: CA information that issued the certificate
- **DNS Names**: DNS names defined in the certificate
- **Not After**: Certificate expiration date
- **Store Name**: Certificate Store name
- **Store Location**: Certificate Store location

Certificate Deployment

Step 1: TrustStore and Certificate Selection

1. Select your Windows TrustStore device from **Automation > Devices**
2. Click the **Add** button in device details
3. In the **Add Trust Store** window that opens:

- **Name**: Provide a descriptive name for the certificate (e.g., `wintrusttest / 10.34.24.150`)
- **Store Name**: Select store name (e.g., `My`)
- **Store Location**: Select store location (e.g., `LocalMachine`)
- **Certificate**: Select the certificate you want to add from the dropdown menu (e.g., `dvtester.sectrail.com - 09-11-2025 23:59:59`)
- **KeyStore Type**: Select `JKS` (or PKCS12)
- **Pfx Password**: Enter certificate password

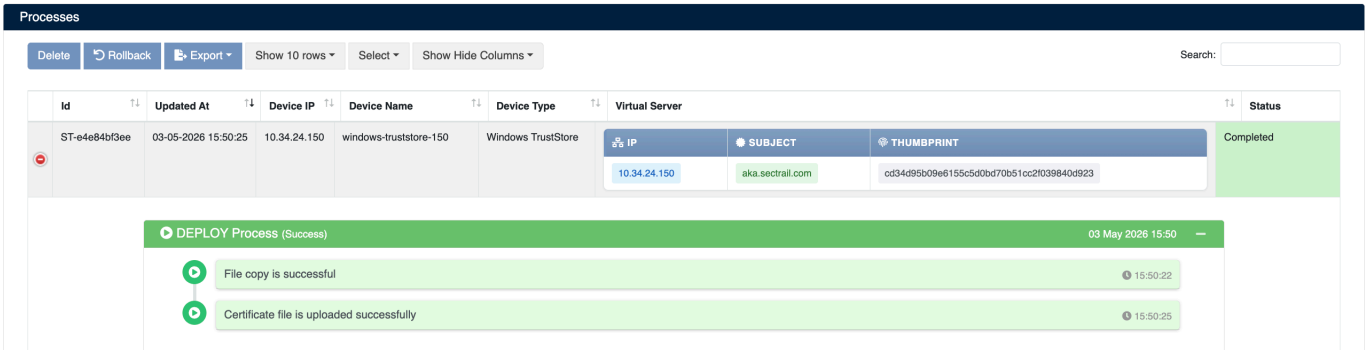


Step 2: Starting the Deployment Process

Click the **Submit** button to start the certificate deployment process.

Step 3: Process Tracking

The deployment process can be tracked from **Automation > Processes**:



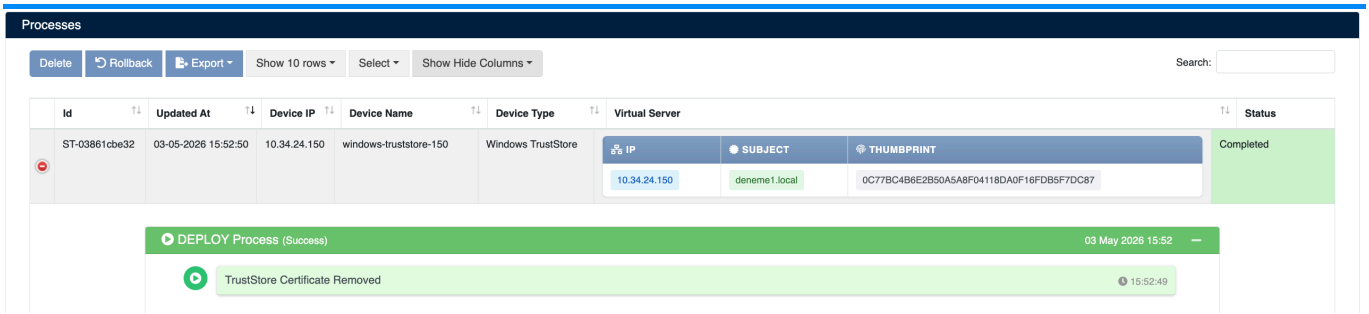
Operation Details

The following steps are performed during deployment:

Step	Operation Description
1	Certificate file is copied to the server (`File copy is successful`)
2	Certificate is successfully uploaded to Windows TrustStore (`Certificate file is uploaded successfully`)

Certificate Removal (Remove)

SecTrail CM supports certificate removal from Windows TrustStore.



Removal Operation Steps

1. Select your Windows TrustStore device from **Automation > Devices**
2. Click the **Remove** button in the row of the certificate you want to remove
3. Confirm to start the removal operation

Removal Operation Task Details

The removal operation can be tracked from **Automation > Processes**. The following steps are performed during the operation:

Step	Operation Description
1	Specified certificate is removed from Windows TrustStore (`TrustStore Certificate Removed`)

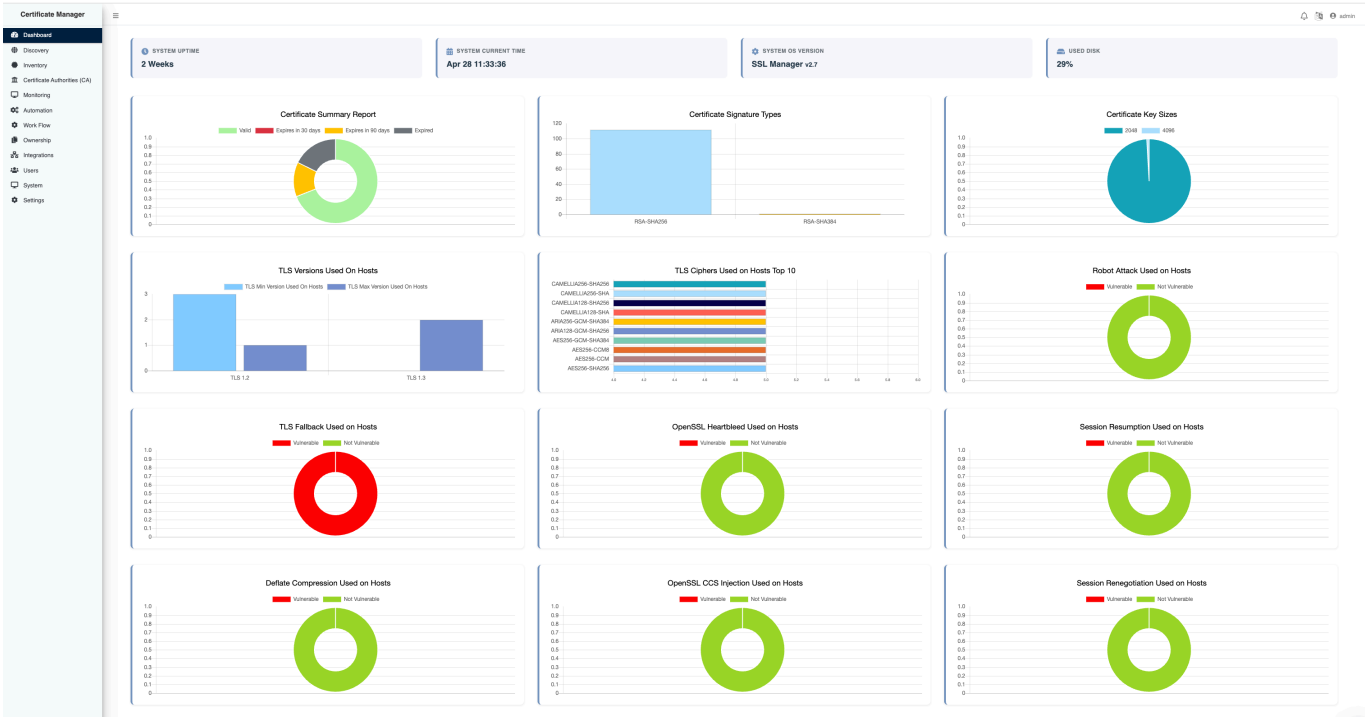
Dashboard

Dashboard is the main screen in SecTrail CM that provides a comprehensive view of your system status and certificate inventory.

Overview

After logging in, you'll encounter the dashboard which consolidates the status of all certificates in your infrastructure, security metrics, and system information on a single screen. The dashboard includes:

- **Real-time certificate metrics** and status reports
- **Security vulnerability analysis** and TLS/SSL configuration status
- [!] **Alarm system** with expiring certificate warnings
- **Visualized reports** for easy monitoring



SecTrail CM Main Dashboard - System Overview

System Metrics

At the top of the dashboard, you'll find metrics showing the overall system status:

Metric	Description
System Uptime	System continuous operation time
System Current Time	Current system time
System OS Version	Operating system version (SSL Manager v2.6.9)
Used Disk	Percentage of disk space used

SYSTEM HEALTH

These metrics allow you to monitor system performance and resource usage in real-time.

Dashboard Charts and Reports

The dashboard offers various charts that visualize the status of certificates in your infrastructure:

Certificate Status Charts

Certificate Summary Report

Shows the general status of certificates by category:

- [OK] **Valid** - Valid certificates
- **Expiring within 60 days** - Will expire within 60 days
- **Expiring within 30 days** - Will expire within 30 days
- **Expired** - Expired certificates

Certificate Signature Types

Shows the distribution of certificate signature types used. Modern and secure algorithms (RSA-SHA256, ECDSA-SHA256) should be preferred. Legacy algorithms (RSA-SHA1, MD5) pose security risks.

Certificate Key Sizes

Shows the distribution of certificate key sizes. A minimum of 2048-bit RSA or 256-bit ECC keys is recommended. 1024-bit and smaller keys are not secure.

Security and Protocol Charts

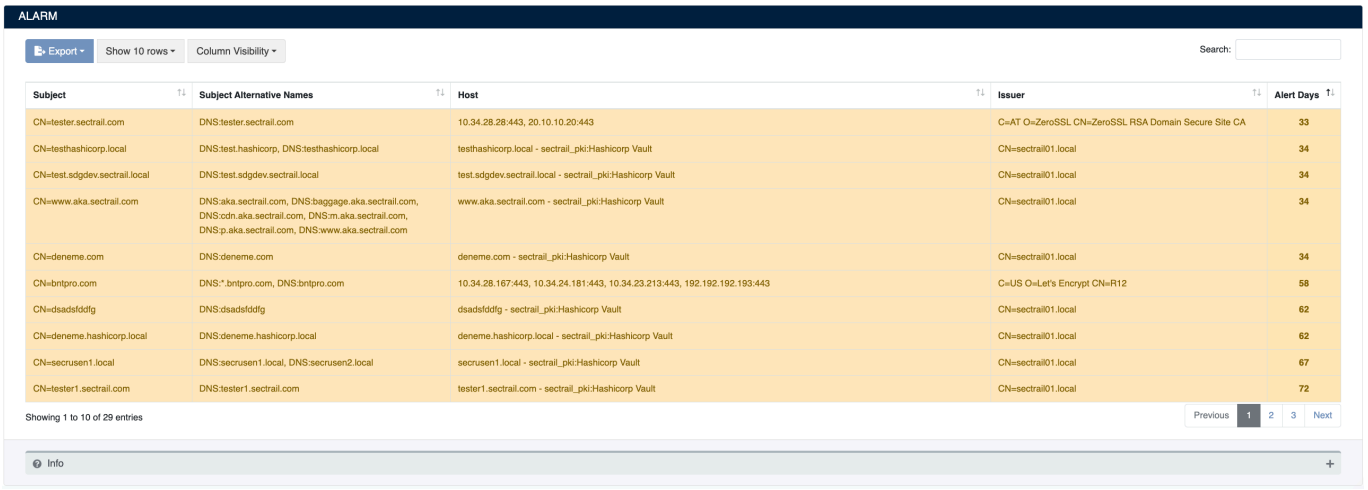
Chart	Description
TLS Versions Used On Hosts	Distribution of TLS versions used on hosts (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)
TLS Ciphers Used on Hosts Top 10	Most commonly used TLS cipher suites
TLS Fallback Used on Hosts	TLS Fallback SCSV usage status (Vulnerable/Not Vulnerable)
OpenSSL Heartbleed	Heartbleed (CVE-2014-0160) vulnerability detection
OpenSSL CCS Injection	CCS Injection (CVE-2014-0224) vulnerability detection

[!] Security Vulnerability Charts

Chart	Description
Robot Attack Used on Hosts	ROBOT attack security status detection
Deflate Compression Used on Hosts	TLS compression (CRIME attack) vulnerability status
Session Resumption Used on Hosts	TLS session resumption mechanism usage status
Session Renegotiation Used on Hosts	TLS session renegotiation security configuration

Alarm Table

At the bottom of the dashboard, there is a detailed table showing the alarm statuses of certificates in your infrastructure:



Dashboard Alarm Table - Certificate Warnings and Status Information

- **Subject** - Certificate subject *(CN, O, OU information)*
- **Subject Alternative Names** - Alternative domain names (SAN). Shows all domains for which the certificate is valid.
- **Host** - Server/host address where the certificate is used *(IP address or hostname)*
- **Issuer** - Certificate Authority (CA) that issued the certificate *(e.g., Let's Encrypt, DigiCert, Sectigo)*
- **Progress** - Progress status in the certificate lifecycle. Shown with a visual progress bar.
- **Alert Days** - Number of days until certificate expiration ⏰ Critical warning time

Alarm Color Codes

The alarm table visually shows certificate status with colors:

Color	Status	Action
Red	Expired or very soon to expire certificates	**CRITICAL** - Immediate action required
Orange/Yellow	Certificates expiring within 30-60 days	**WARNING** - Plan renewal
Green	Valid certificates with long expiry	**NORMAL** - In good condition

> **ALARM NOTIFICATIONS**
>
> **Regularly check** the alarm table on the dashboard. Plan urgent actions for red or orange certificates and initiate renewal processes.

Understanding and Interpreting Charts

The charts on the dashboard provide valuable insights about your certificate security and infrastructure status.

Certificate Status Monitoring

Pay attention to priority levels to understand certificate statuses:

- [OK] **Valid** - Normal monitoring period, no cause for concern
- [!] **Expiring within 60 days** - Start renewal planning, contact vendor
- **Expiring within 30 days** - High priority, urgent renewal process should be initiated
- **Expired** - **CRITICAL STATUS** - Service interruption risk, immediate action required

:::

> **AUTOMATIC NOTIFICATIONS**
>
> SecTrail CM provides automatic notification system for critical situations. You can receive instant alerts by configuring email and integration settings.

Discovery Configuration

This guide explains step-by-step how to discover, manage, and monitor certificates in SecTrail CM.

> **ABOUT THE FEATURE**
>
> To learn what the Certificate Discovery feature is, how it works, and its advantages, first review the Features: Certificate Discovery page.

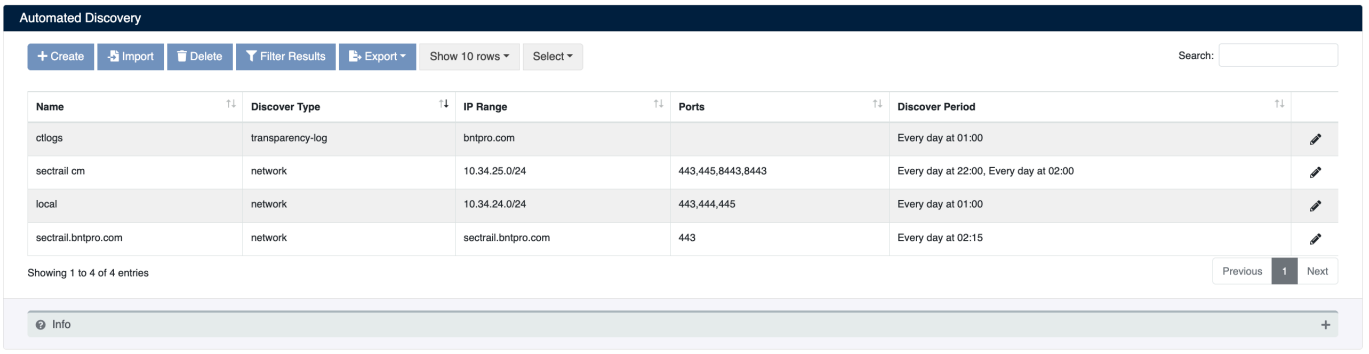
Certificate Discovery

Accessing Discovery Configurations

> **ACCESS PATH**
>
> To manage discovery operations, go to: **Discovery -> Automated Discovery** in the application panel.

Discovery Configurations List

You can view all discovery periods and configurations defined in SecTrail CM in a centralized list.



Discovery Configurations List - All Defined Discovery Tasks

List Information

The following information is displayed for each row in the discovery configurations list:

- **Name** - Descriptive name you gave to the discovery task
- **Discover Type** - Which discovery method is used (`Network Scan` or `CT Logs`)
- **IP Range** - IP range or domain name to be scanned
- **Ports** - Which ports are scanned (e.g., `443, 444, 8443`)
- **Discover Period** - How frequently discovery runs

Available Operations

You can perform the following operations from the list:

- **View and Filter** - Review discovery configurations
- **Edit** - Update existing configurations
- **Delete** - Remove unnecessary configurations

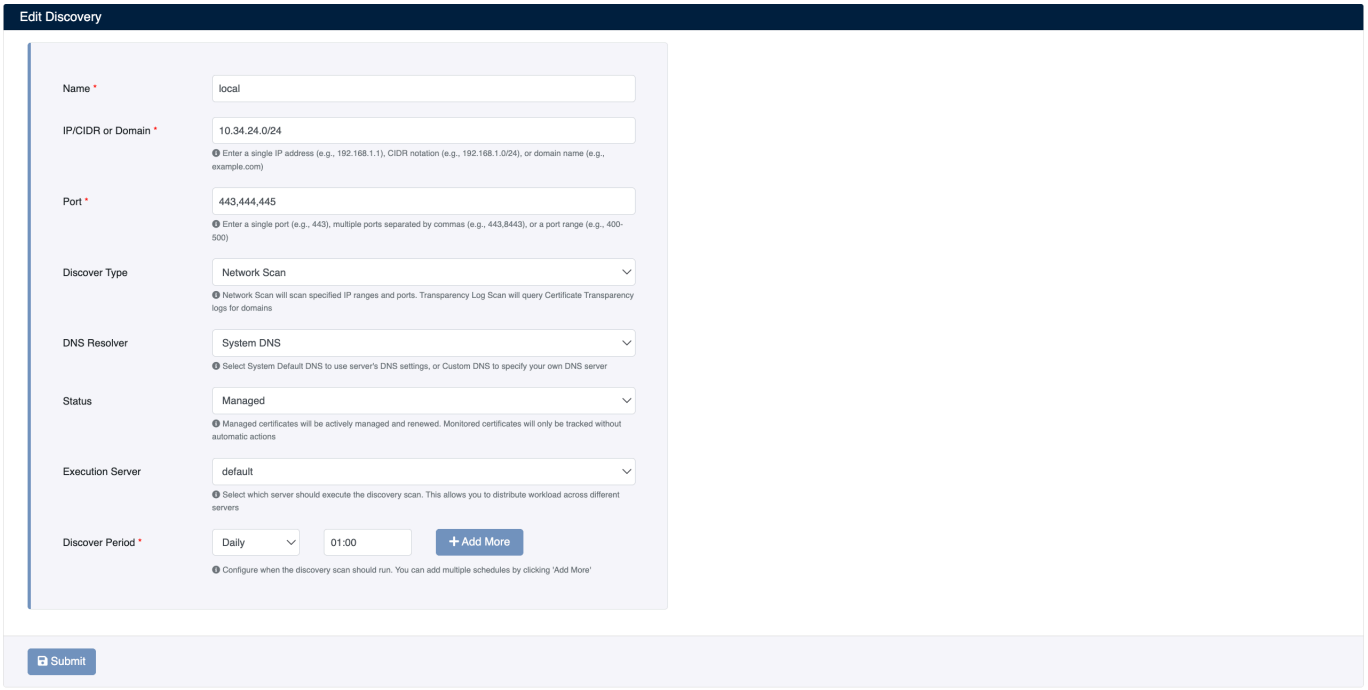
- **Create New** - Add new discovery configuration

Network Scan Configuration

With Network Scan, you can discover SSL/TLS certificates in your internal network.

Creating New Network Scan

As shown in the image below, you can create a Network Scan configuration:



Network Scan Configuration Form

Configuration Parameters

Parameter	Description	Options
Name	Provide a descriptive name for the discovery task	Use IP range or target system name
IP or CIDR	Enter the IP address, CIDR notation, or domain name you want to scan	- Single IP: `192.168.1.100` - IP range: `10.34.24.0/24` - Subnet: `172.16.0.0/16` - Domain: `example.com`
Port	Enter ports to scan, separated by commas	- Single port: `443` - Multiple: `443,444,8443`
Discover Type	Select discovery method	Select `Network Scan`
Status	Determine status of discovered certificates	- **Managed:** Managed certificates - **Monitored:** Only monitored certificates
Discover Period	Set how frequently the scan runs	- **Period type:** Daily or Weekly - **Time:** HH:MM format - **Add More** to add multiple times

TIPS

- Scanning outside business hours reduces network traffic
- Use **Add More** button to scan at different times each day

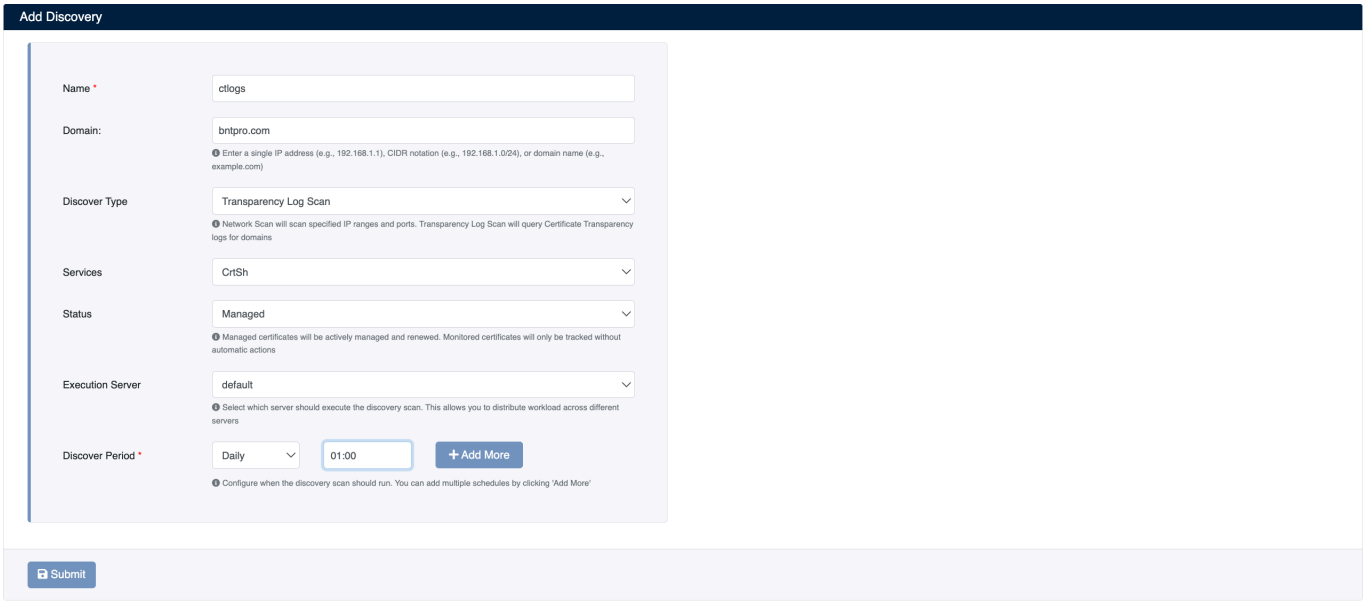
After entering the form information, click the **Submit** button to save the configuration.

CT Logs Configuration

With CT Logs, you can discover your publicly published domain certificates.

Creating New CT Log Scan

As shown in the image below, you can create a CT Logs configuration:



CT Logs Configuration Form

Configuration Parameters

Parameter	Description	Options
Name	Provide a descriptive name for the discovery task	Example: `Example.com CT Scan`, `Company Domains`
Domain	Enter the domain name you want to scan	- Example: `example.com` - Subdomains are automatically included - No need to use wildcard (`*.example.com`)
Discover Type	Select discovery method	Select `CT Logs`
Status	Determine status of discovered certificates	- **Managed:** Managed certificates - **Monitored:** Only monitored certificates
Discover Period	Set how frequently the scan runs	- **Period type:** Daily or Weekly - **Time:** HH:MM format

SUBDOMAIN DISCOVERY

When you enter `example.com`, all subdomain certificates for this domain are also automatically found: `www.example.com`, `api.example.com`, `mail.example.com`, and others.

CT LOGS RECOMMENDATIONS

- **Daily scanning** is recommended for CT Logs (to catch new certificates)
- Be sure to perform daily scanning for Shadow IT detection
- New certificates may take a few hours to be recorded in CT logs

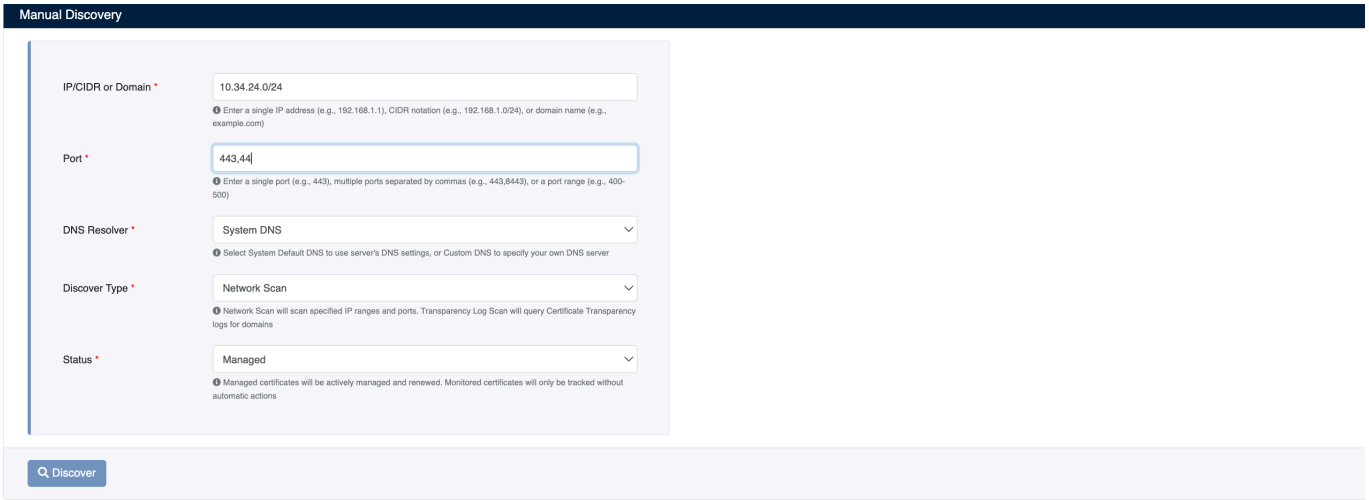
After entering the form information, click the **Submit** button to save the configuration.

Manual Discovery

You can navigate to **Discovery > Manual Discovery** to perform quick and instant scans without creating scheduled discovery tasks.

WHEN TO USE MANUAL DISCOVERY?

- Quick check when adding a new server
- Emergency certificate check
- Test scans
- One-time inventory updates



Manual Discovery Form - Quick Scan

Manual Discovery Parameters

Parameter	Description	Options
IP or CIDR	Enter IP, CIDR, or domain to scan	- Single IP: `1.1.1.1` - IP range: `1.1.1.0/24` - Domain: `example.com`
Port	Specify ports to scan	- Single port: `443` - Multiple ports: `443,844,444`
Discover Type	Select discovery method	- **Network Scan:** For IP/Port scanning - **CT Logs:** For domain scanning
Status	Determine certificate status	- **Managed:** Managed - **Monitored:** Monitored

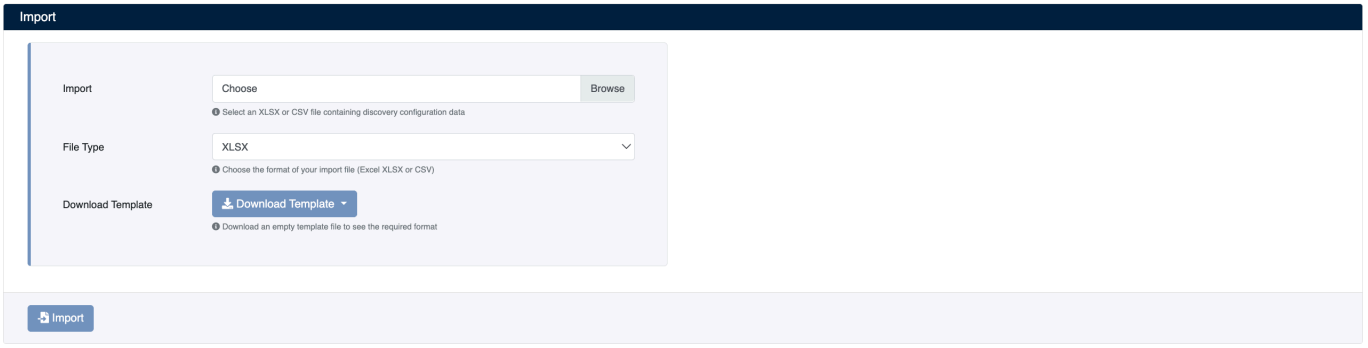
After filling out the form, click the **Discover** button to start scanning immediately.

> **IMPORTANT NOTE**
>
> - Manual discovery results are **automatically added to inventory**
> - However, it **does not create periodic scanning**
> - For regular scanning, you must create a scheduled discovery configuration

Bulk Discovery Configuration

You can perform bulk import via Excel (XLSX) file to create multiple discovery configurations at once.

> **WHEN TO USE BULK IMPORT?**
>
> - When you want to add many IP ranges or domains at once
> - When you want to create discovery configurations from an existing inventory list
> - When you want to bulk import network lists from different departments



File Import Screen - Bulk Discovery Configuration

How to Perform File Import?

Access the bulk import page from **Discovery -> Automated Discovery -> File Import** menu.

1. Download and Fill Template

Click the **Download Template** button to download the Excel (XLSX) template file. Fill in the following columns in the template:

> **TEMPLATE TIPS**
>
> - Each row in Excel represents a discovery configuration
> - Don't fill empty rows, Excel will automatically skip them
> - For multiple ports in the Port column, separate with commas: `443,8443,636`
> - Use IP/CIDR for Network Scan, use domain for CT Logs

2. Upload File

1. Click the **Choose File** or **Browse** button
2. Select the filled Excel file
3. Ensure `XLSX` is selected in the **File Type** field
4. Click the **Import** button

3. Check Results

- [OK] Successfully imported configurations are shown with green checkmarks
- Rows with errors are marked in red and error message is displayed
- Check all added records from the discovery configurations list

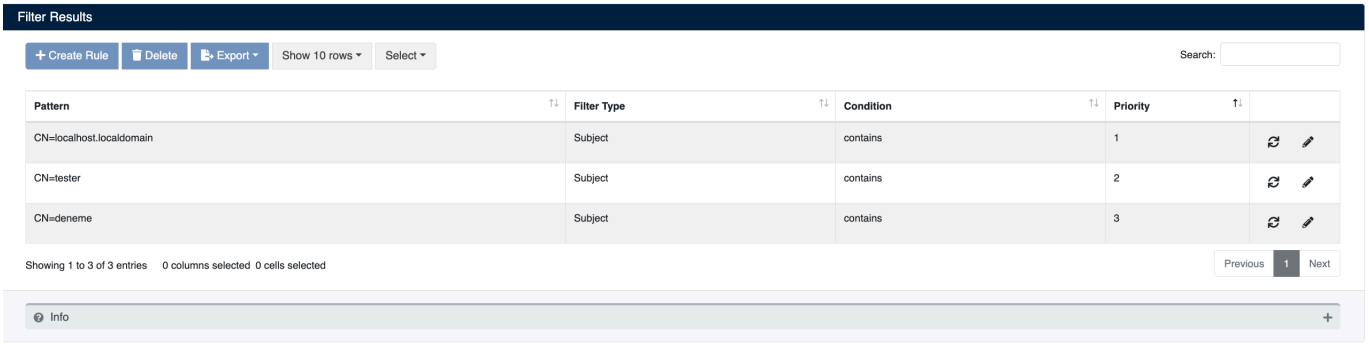
How to Configure Discovery Filters?

If you want certain IP addresses, ranges, or domains to never be discovered during any discovery operation, you can use the **Discovery Filter** feature. Targets defined with a filtering rule are automatically excluded from all discovery processes.

> **ACCESS PATH**
>
> Go to **Discovery -> Automated Discovery -> Filter** menu.

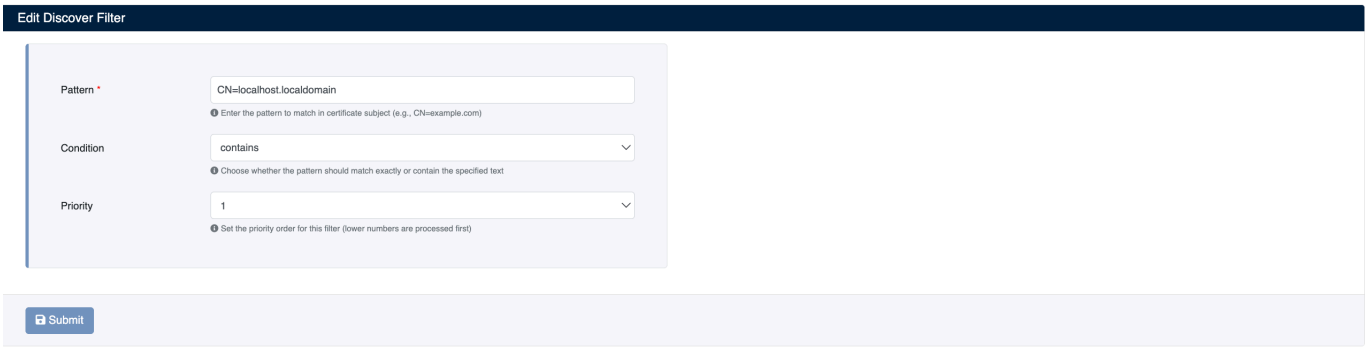
> **WHEN TO USE?**
>
> - If there are specific IP addresses or ranges you do not want discovered
> - If certain systems must be excluded from the inventory
> - For network segments that should be kept out of scanning

Filter List



Defined Discovery Filters List

Creating a New Filter



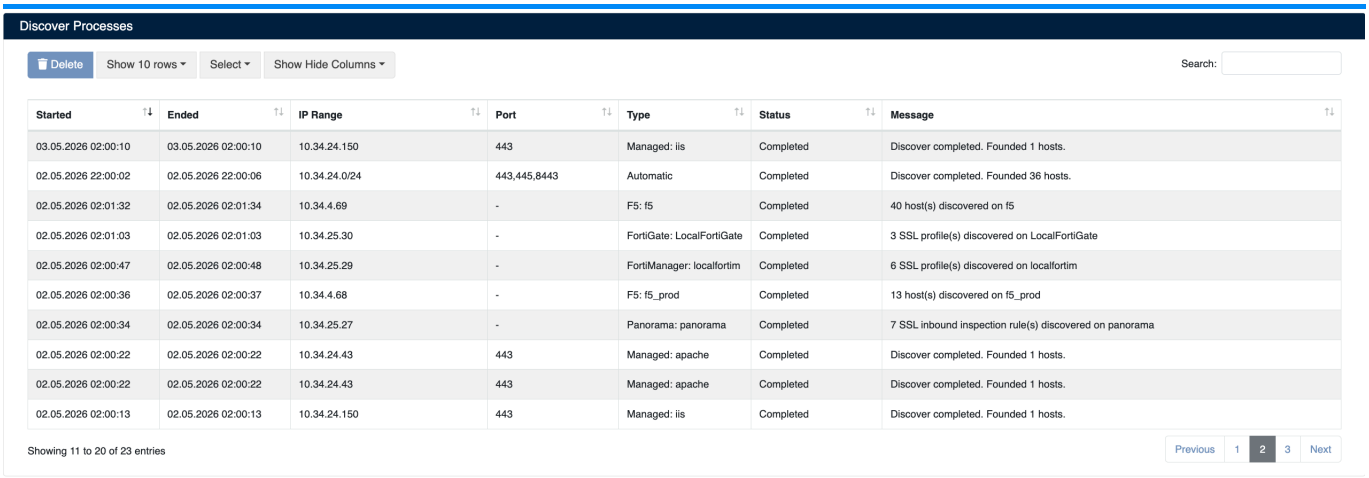
Discovery Filter Creation Form

Parameter	Description	Example
IP or CIDR	IP address or range to exclude from discovery	`192.168.1.50`, `10.0.0.0/8`
Port	Port to exclude from discovery (optional)	`443`, `8443`

After filling in the form and clicking the **Submit** button, the rule becomes active and these targets will be skipped in the next discovery operation.

Monitoring Discovery Results

You can track the results of all discovery operations from the **Discovery -> Processes** menu.



Discovery Results Page - Scan Statuses and Statistics

Displayed Information

On this page, you can see the following details for each discovery operation:

Scan Status : Ongoing, completed, or failed scans

Discovery Type : Network Scan or CT Logs

Target Information : Scanned IP range or domain name

Start Time : Date and time the scan started

End Time : Date and time the scan completed

Duration : Total scan duration

Certificates Found : Number of certificates found in the scan

Scan Details : Detailed log records of each scan

Scan Statuses

Discovery operations can be in the following states:

Status	Icon	Description	Action Required
In Progress		Scan is currently ongoing	Wait for completion
Completed	[OK]	Scan completed successfully	Review results
Failed	[X]	Scan ended with error	Check error logs

> **USEFUL INFORMATION**
>
> From this page, you can view the results of both scheduled discovery tasks and manual discovery operations. Past scan records are also saved, allowing you to analyze your discovery performance.

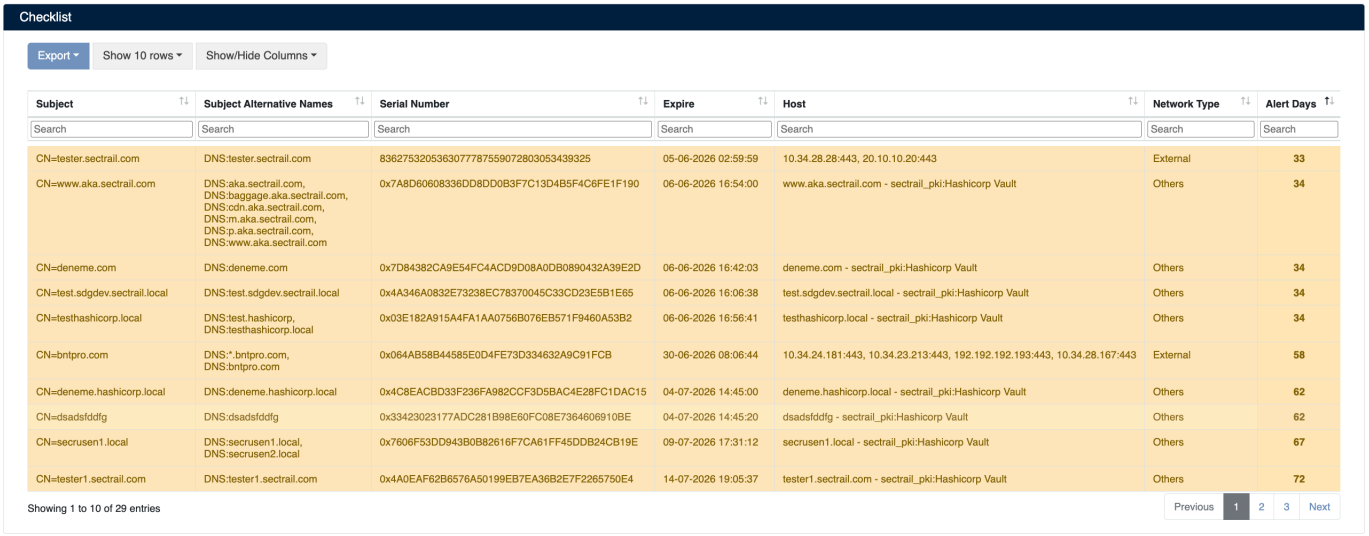
Alerts and Notifications

In SecTrail CM, you can monitor certificate expiration status, receive automatic notifications when critical deadlines approach, and create alarm configurations.

> **ACCESS PATH**
>
> You can access alarm and notification features in the application panel through the following paths:
>
> - **Monitoring -> Checklist** - Certificate alarm list and configuration

Alarm List

The alarm list allows you to track the status of certificates approaching expiration with color-coded visualization.



Expiration Status Alarm List

List Information

The following information is displayed for each certificate in the alarm list:

- **Subject** - Certificate's Common Name (CN) information
- **Subject Alternative Names** - Certificate's SANs (DNS names) list
- **Serial Number** - Certificate serial number
- **Expire** - Certificate expiration date and time
- **Host** - Server address and port information where the certificate is located
- **Issuer** - CA (Certificate Authority) that signed the certificate
- **Network Type** - Certificate's network type category (External, Internal, etc.)
- **Alert Days** - Number of days remaining until certificate expiration

Alarm Color Codes

Certificate expiration status is shown with color codes in the **Alert Days** column:

Color	Status	Description
Red	Critical (0-7 days)	Certificate will expire within 7 days or has expired
Orange	Warning (8-30 days)	Certificate will expire within 8-30 days
Yellow	Attention (31-90 days)	Certificate will expire within 31-90 days

> **CRITICAL ALARM**
>
> Certificates shown in red require urgent action. These certificates must be renewed or updated before expiration.

List Operations

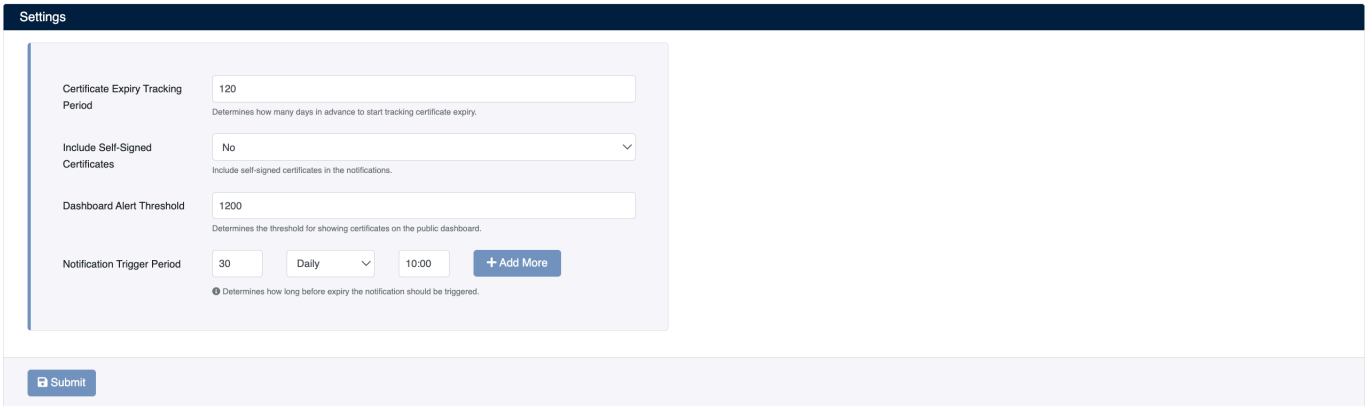
From the toolbar at the top of the page, you can perform the following operations:

- **Show X entries** - Set the number of records to display per page
- **Search** - Search by certificate information
- **Alarm Configuration** - Navigate to the alarm configuration page

Alarm Configuration

On the Alarm Configuration page, you can customize certificate expiration notifications and set automatic notification times.

> **ACCESS**
>
> You can access alarm configuration settings from **Monitoring -> Settings**.



Alarm Configuration Page

Configuration Settings

Parameter	Description	Options
Track If Certificates Expires In	Determines how many days in advance to start tracking certificate expiration	Enter number of days
Send Notification If Certificates Expires In	Set time periods for sending automatic notifications	- **Number of days:** How many days before to send notification - **Period:** Daily or Weekly - **Day:** Which day for weekly notifications - **Hour:** What time to send the notification
Send Self-Signed Certificate	Should notifications be sent for self-signed certificates?	- **Yes:** Notify for self-signed as well - **No:** Exclude self-signed
Public Dashboard Threshold	Threshold value for certificates to display on public dashboard	Enter number of days

> **SELF-SIGNED CERTIFICATES**
>
> Self-signed certificates are typically used in test environments or internal systems. Using certificates signed by trusted CAs in production environments is recommended.

Saving Configuration

After making all settings, click the **Submit** button to save the configuration.

:::success Successful Save After the configuration is saved, automatic notifications will start being sent at the specified periods. :::

Notification Integrations

SecTrail CM can send alarm notifications through different channels:

- **Email** - Automatic notification delivery to specified email addresses
- **SNMP Trap** - Alarm delivery to network management systems via SNMP protocol

Network Type Alarm Configuration

Network Type Alarm Configuration allows you to periodically send a list of all certificates in a specific network type via email. With this feature, you can regularly receive a complete list of certificates in External, Internal, or other network types and track which domains you're using.

> **ACCESS PATH**
>
> You can access network type-based alarm configurations from **Monitoring -> Alert Rules -> Network Type Based**.

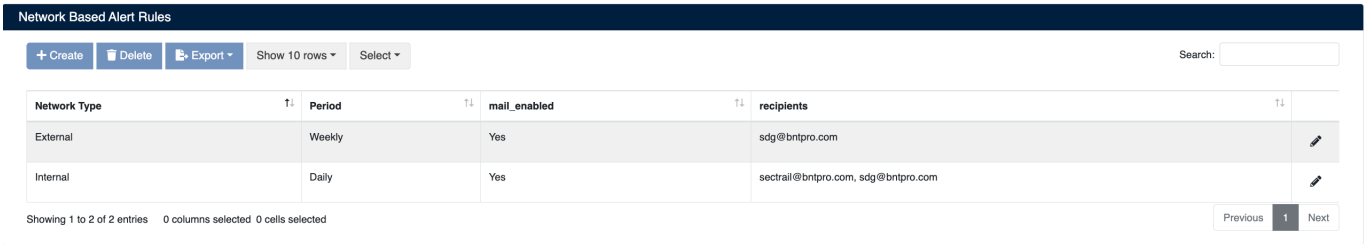
What is Network Type Alarm Configuration?

Network Type Alarm Configuration automatically sends a list of all certificates belonging to a specific network type via email. This allows you to:

- Receive a complete list of **External** certificates daily or weekly
- Regularly track the inventory of **Internal** certificates
- Send separate lists to different teams for each network type
- Report all domains and certificates in use

> **WHAT IS NETWORK TYPE?**
>
> Network Type determines which network category certificates belong to. These values are configured from the **Monitoring -> Alert Rules -> Network Type Based** page and automatically categorize certificates.

Network Type Alarm Configuration List



Network Type Alarm Configuration - Existing Configurations

List Information

On the list page, you can see all defined network type alarm configurations:

- **Network Type** - Network type category (External, Internal, etc.)
- **Period** - Notification period (Daily, Weekly)
- **Mail** - Is email notification active? (Yes/No)
- **To Mails** - Email addresses to receive notifications

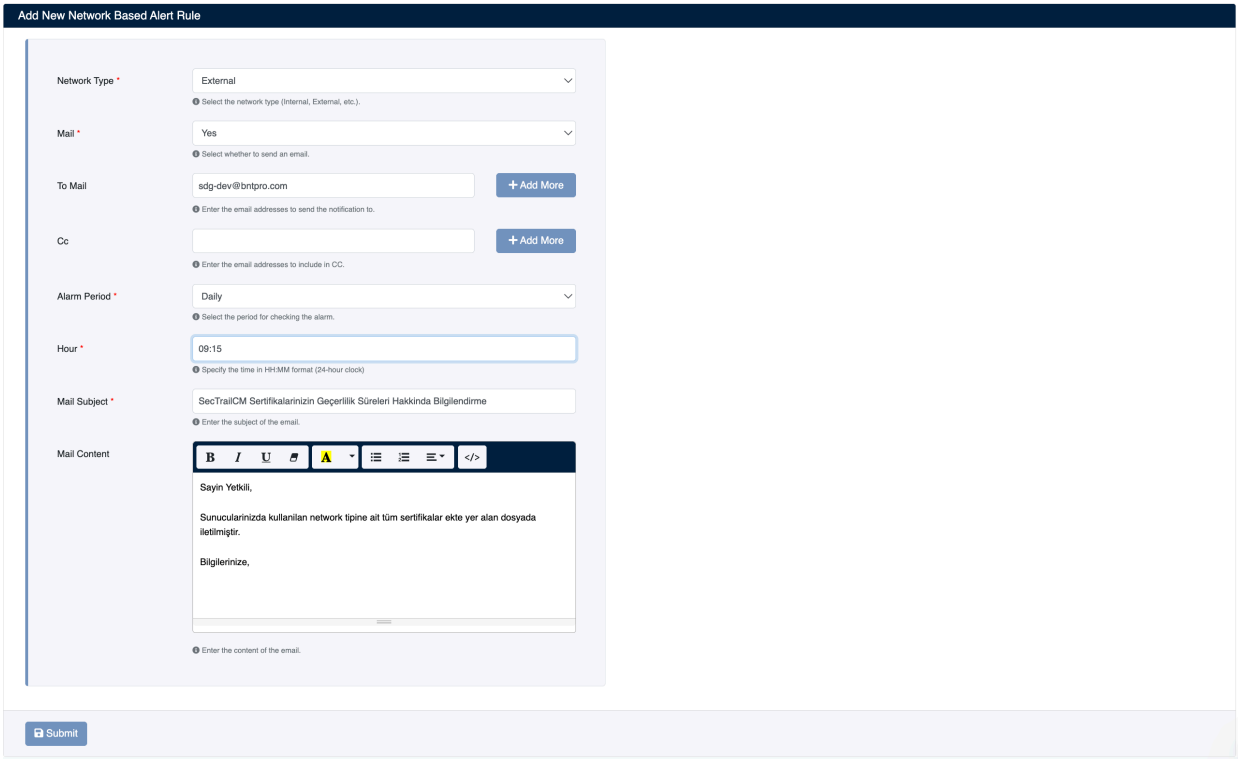
List Operations

You can perform the following operations for each row:

- **Edit** - Edit existing configuration
- **Delete** - Delete configuration

> **NEW CONFIGURATION**
>
> Click the **Create** button to create a new Network Type Alarm Configuration.

Creating New Network Type Alarm Configuration



Add New Network Type Alarm Configuration Form

Configuration Parameters

Parameter	Description	Options
Network Type	Select the network type for which the alarm configuration will apply	- **External:** External network certificates - **Internal:** Internal network certificates - Custom types defined in Network Configuration
Mail	Should email notifications be sent?	- **Yes:** Email notification active - **No:** Email notification disabled
To Mail	Email addresses to receive notifications	Multiple email addresses can be added (with **Add More**)
Cc	Copy recipients (optional)	Multiple email addresses can be added
Alarm Period	How frequently notifications will be sent	- **Daily:** Every day - **Weekly:** Weekly
Hour	What time notifications will be sent	24-hour format (e.g., `10:00`)
Mail Subject	Email subject line	Enter email subject
Mail Content	Email content	Enter email content

NETWORK TYPE RULE

You can create only one alarm configuration per Network Type. You cannot create a new configuration for an existing Network Type.

AUTOMATIC CERTIFICATE LIST

A **list of all certificates** in the selected network type is automatically attached to the email content as an attachment (Excel/CSV).

The list includes:

- Certificate Subject (CN) information
- Certificate expiration dates
- Host and port information
- All domain names used

Saving Configuration

After filling in all fields, click the **Submit** button to save the configuration.

:::success Successful Save After the configuration is saved, the **list of all certificates** in the relevant network type will automatically start being sent via email at the specified period and time. :::

Alarm Customization

Alarm Customization allows you to customize certificate alarms based on much more detailed criteria. With this feature, you can create special alarm rules for certificates with specific characteristics and send different alarm notifications to different teams.

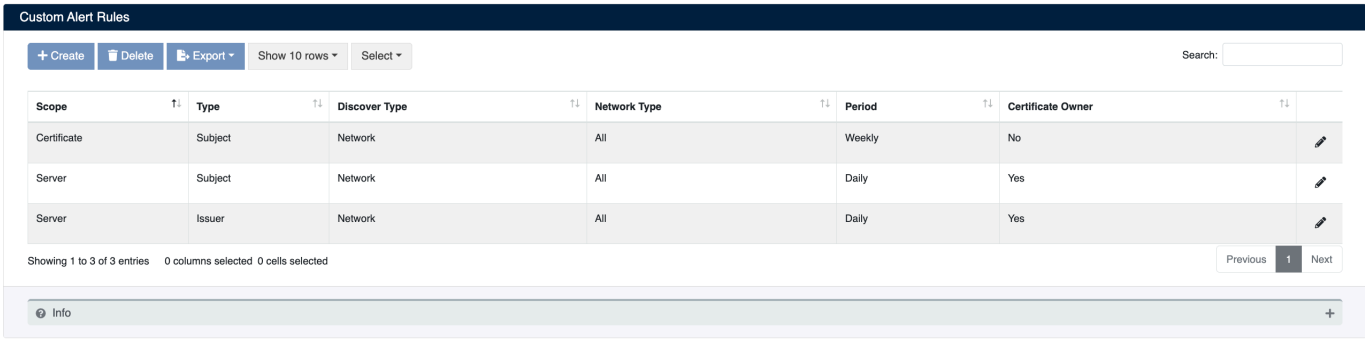
> **ACCESS PATH**
>
> You can access alarm customization configurations from **Monitoring -> Alert Rules -> Advanced Rules**.

What is Alarm Customization?

Alarm Customization allows you to create much more granular and specific alarm rules beyond standard alarm configuration. This enables you to:

- **Scope-based alarms:** Separate alarms for servers or certificates
- **Type-based alarms:** Separate rules for server or CA certificates
- **Network Type filtering:** Only certificates from external, local, or specific network types
- **Certificate Owner filtering:** Special alarms for certificates owned by specific owners
- **Key Size warnings:** Automatic notifications for insecure key sizes
- **Expired certificates:** Separate notifications for expired certificates
- **Self-signed checking:** Special rules for self-signed certificates

Alarm Customization List



Alarm Customization - Existing Rules

List Information

On the list page, you can see all defined custom alarm rules:

- **Type** - Alarm type (Subject, Issuer)
- **Scope** - Scope (Server, Certificate)
- **Discover Type** - Discovery type (Network, TLS, etc.)
- **Network Type** - Network type filter (All, External, Internal)
- **Threshold Day** - How many days in advance to send alarm
- **Certificate Owner** - Certificate owner filter (Yes/No)

- **To Mails** - Email addresses to receive notifications

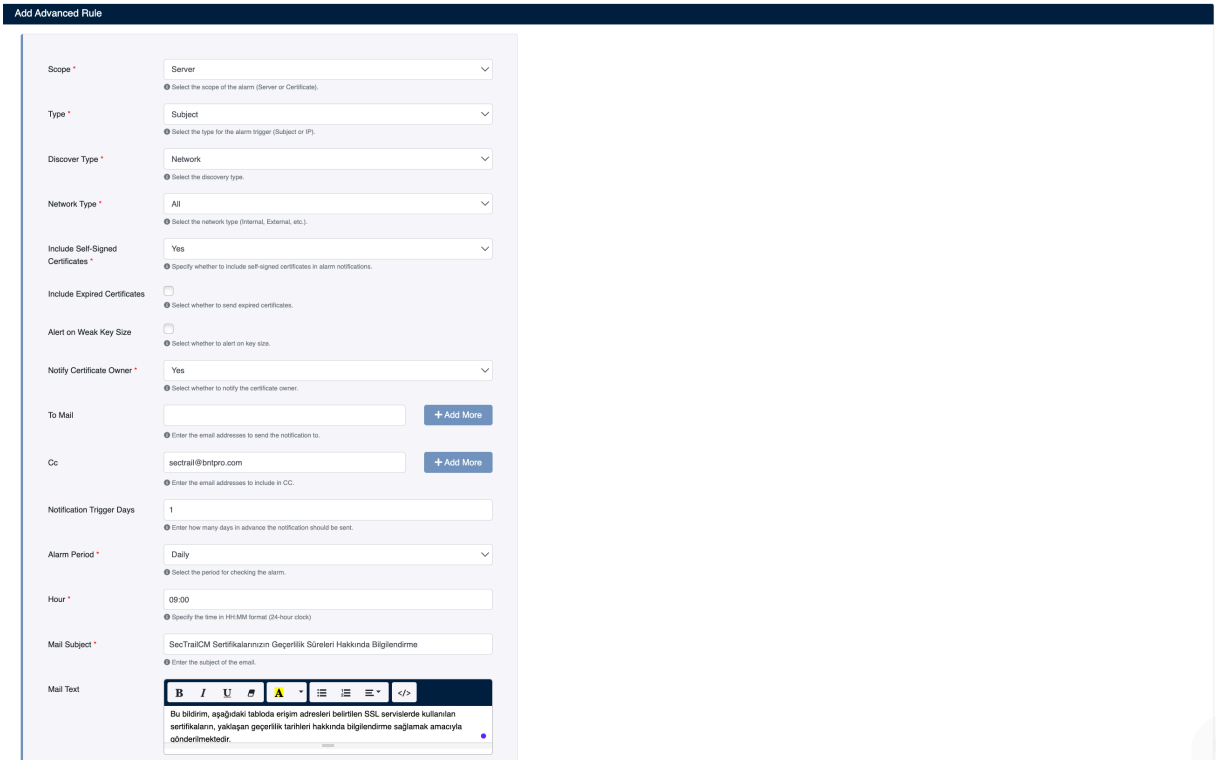
List Operations

You can perform the following operations for each row:

- **Edit** - Edit existing rule
- **Delete** - Delete rule

> **NEW RULE**
>
> Click the **Create** button to create a new custom alarm rule.

Creating New Alarm Customization Rule



Add New Alarm Customization Rule Form

Configuration Parameters

Basic Filters

Parameter	Description	Options
Scope	Determines the scope in which the alarm will operate	- **Server:** Separate notification for each server - **Certificate:** Notification for unique certificates
Type	Select the type of certificates for which alarms will be created	- **Subject:** Server certificates - **Issuer:** CA certificates
Discover Type	Filter by how certificates were discovered	- **Network:** Network scanning - **TLS:** TLS connection - **File:** File system
Network Type	Select the network type for which alarms will be created	- **All:** All network types - **External:** External certificates only - **Internal:** Internal certificates only - Custom types defined in Network Configuration

Alarm Rules

Parameter	Description	Options
Send Alarm If Certificate Expires in	Determines how many days before certificate expiration to send alarm	Enter number of days (e.g., 30, 15, 7)
Send Expired Certificates	Should notifications be sent for expired certificates?	- **Yes:** Notify for expired certificates as well - **No:** Only non-expired certificates
Key Size Alert	Warning for insecure key sizes	- **Yes:** Warning for small key sizes (e.g., 1024-bit RSA) - **No:** Don't check key size
Send Self-Signed Certificate	Should self-signed certificates be included?	- **Yes:** Notify for self-signed as well - **No:** Exclude self-signed
Certificate Owner	Filter for certificates owned by specific owners	- **Yes:** Only certificates with specific owners - **No:** All certificates

Notification Settings

Parameter	Description	Options
Alarm Period	How frequently notifications will be sent	- **Daily:** Every day - **Weekly:** Weekly
Hour	What time notifications will be sent	24-hour format (e.g., `10:00`)
To Mail	Email addresses to receive notifications	Multiple email addresses can be added (with **Add More**)
Cc	Copy recipients (optional)	Multiple email addresses can be added
Mail Subject	Email subject line	Enter email subject
Mail Text	Email content	Enter email content

Saving Configuration

After filling in all fields, click the **Submit** button to save the rule.

:::success Successful Save After the rule is saved, automatic notifications will start being sent for certificates matching the specified criteria. :::

TLS Alarm Configuration

TLS Alarm Configuration allows you to receive automatic notifications about old and insecure TLS versions (TLS 1.0, TLS 1.1) used on your servers. With this feature, you can detect and update old TLS versions that create security vulnerabilities.

> **ACCESS PATH**
>
> You can access TLS alarm configurations from **Monitoring -> Alert Rules -> TLS Version Based**.

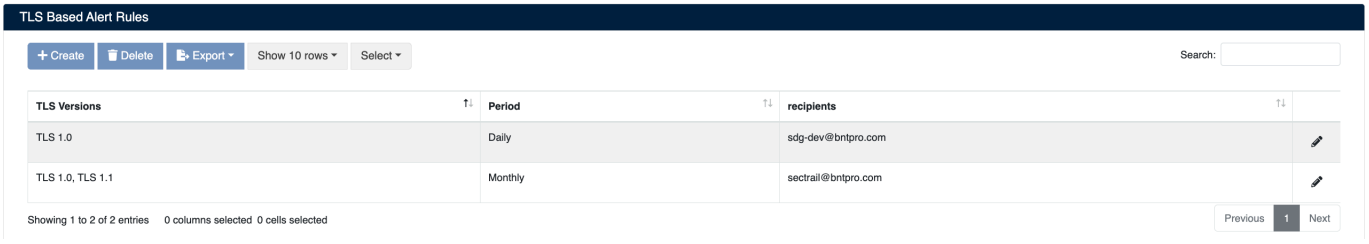
What is TLS Alarm Configuration?

TLS Alarm Configuration monitors TLS protocol versions used on your servers and sends automatic notifications for old versions considered insecure. This allows you to:

- Detect servers using **TLS 1.0**
- Detect servers using **TLS 1.1**
- Report services non-compliant with security standards

> **SECURITY WARNING**
>
> TLS 1.0 and TLS 1.1 versions are considered insecure and should no longer be used. Modern security standards require a minimum of TLS 1.2 or TLS 1.3.

TLS Alarm Configuration List



TLS Alarm Configuration - Existing Configurations

List Information

On the list page, you can see all defined TLS alarm configurations:

- **TLS Versions** - Monitored TLS versions (TLS 1.0, TLS 1.1)
- **Period** - Notification period (Daily, Weekly)
- **To Mails** - Email addresses to receive notifications

List Operations

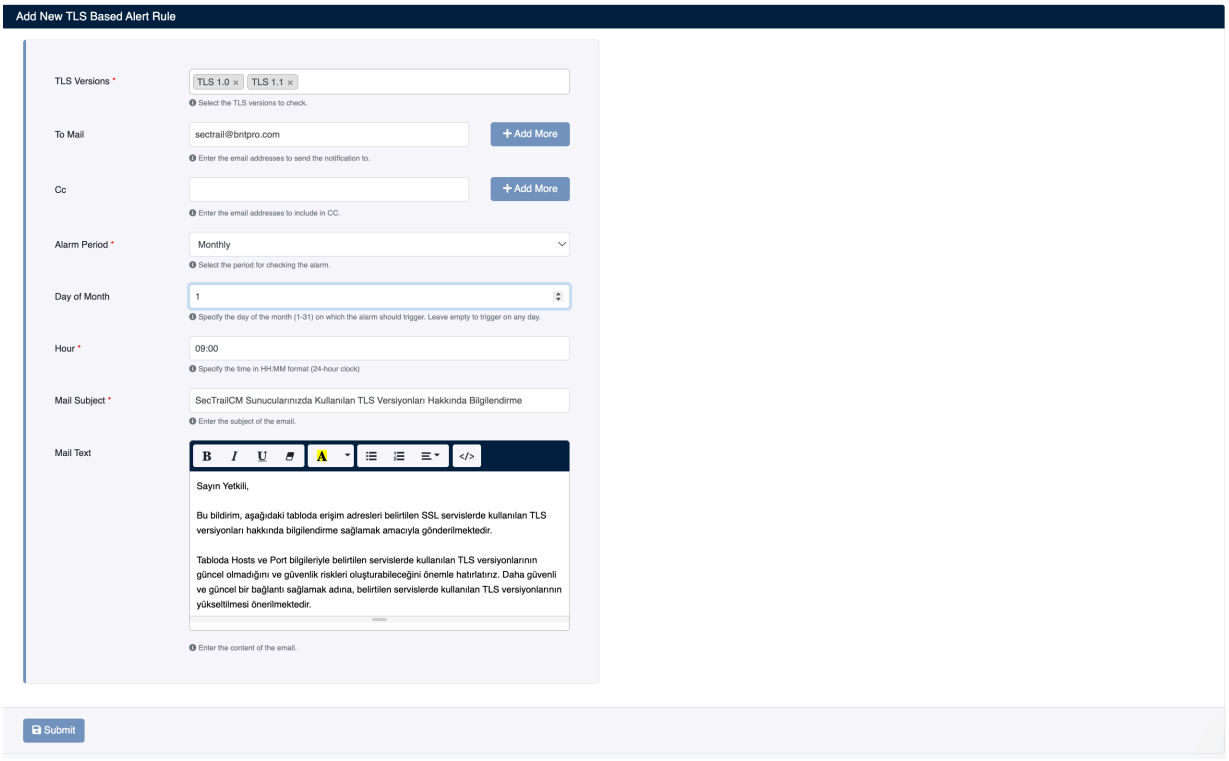
You can perform the following operations for each row:

- **Edit** - Edit existing configuration
- **Delete** - Delete configuration

NEW CONFIGURATION

Click the **Create** button to create a new TLS Alarm Configuration.

Creating New TLS Alarm Configuration



Add New TLS Alarm Configuration Form

Configuration Parameters

Parameter	Description	Options
TLS Versions	Select TLS versions to monitor (Multiple selections possible)	- **TLS 1.0:** Very old and insecure (1999) - **TLS 1.1:** Old and insecure (2006)
To Mail	Email addresses to receive notifications	Multiple email addresses can be added (with **Add More**)
Cc	Copy recipients (optional)	Multiple email addresses can be added
Alarm Period	How frequently notifications will be sent	- **Daily:** Every day - **Weekly:** Weekly
Hour	What time notifications will be sent	24-hour format (e.g., `11:00`)
Mail Subject	Email subject line	Enter email subject
Mail Text	Email content	Enter email content

TLS VERSION SECURITY

- **TLS 1.0** - Released in 1999, has serious security vulnerabilities

- **TLS 1.1** - Released in 2006, has security vulnerabilities
- **TLS 1.2** - Released in 2008, considered secure (minimum recommended)
- **TLS 1.3** - Released in 2018, most secure version

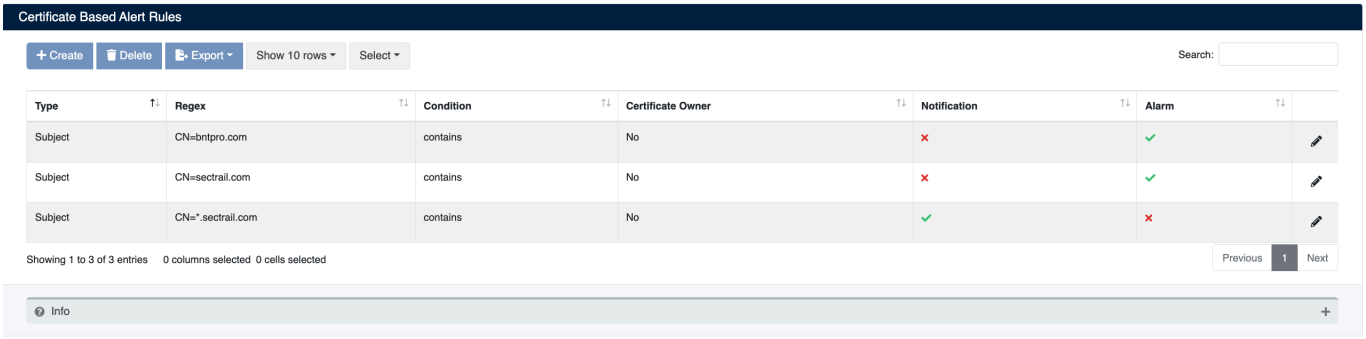
Saving Configuration

After filling in all fields, click the **Submit** button to save the configuration.

:::success Successful Save After the configuration is saved, automatic notifications will start being sent for servers using the selected TLS versions at the specified period and time. :::

Certificate Based Alert Rules

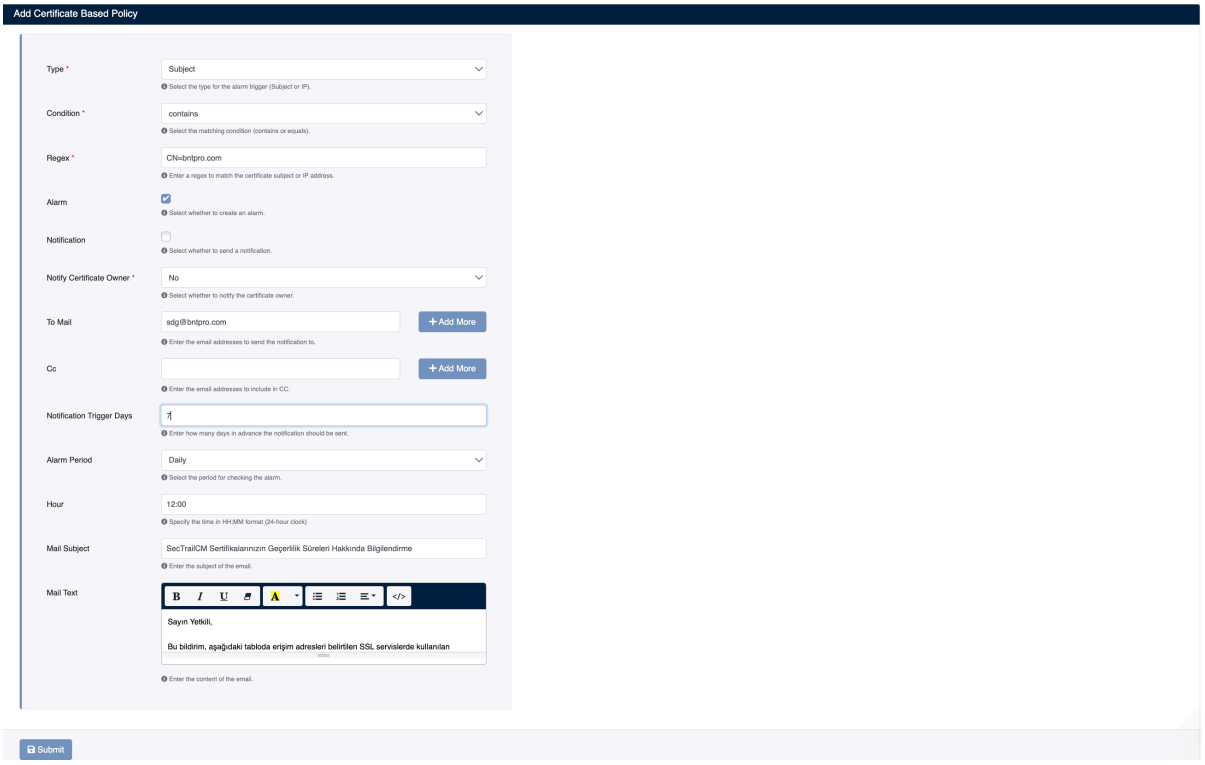
SecTrail CM allows you to define customized alarm and notification rules based on the certificate subject or IP address. You can access these rules from **Monitoring -> Alert Rules -> Certificate Based**.



The list displays **Type**, **Regex**, **Condition**, **Certificate Owner**, **Notification**, and **Alarm** columns for each defined rule.

Creating a New Rule

Click the **+ Create** button to add a new certificate based alert rule:



- **Type**: Select the alarm trigger type (`Subject` or `IP`)
- **Condition**: Select the matching condition (`contains` or `equals`)
- **Regex**: Enter the expression to match against the certificate subject or IP address (e.g. `CN=bntpro.com`)
- **Alarm**: Should an alarm be created when the rule matches?
- **Notification**: Should a notification be sent after the certificate is renewed?

RENEWAL NOTIFICATION

When the **Notification** option is enabled, a renewal notification is automatically sent to the relevant recipients when a matching certificate is renewed.

- **Notify Certificate Owner**: Should the certificate owner be notified? (`Yes` / `No`)
- **To Mail**: Email addresses to send the notification to; click **+ Add More** to add multiple recipients
- **Cc**: Carbon copy email addresses
- **Notification Trigger Days**: How many days in advance should the notification be sent?
- **Alarm Period**: Alarm check period (`Daily` , `Weekly` , etc.)
- **Hour**: Time for the alarm check in HH:MM format
- **Mail Subject**: Subject line of the notification email
- **Mail Text**: Body template of the notification email (editable via rich text editor)

Inventory Management

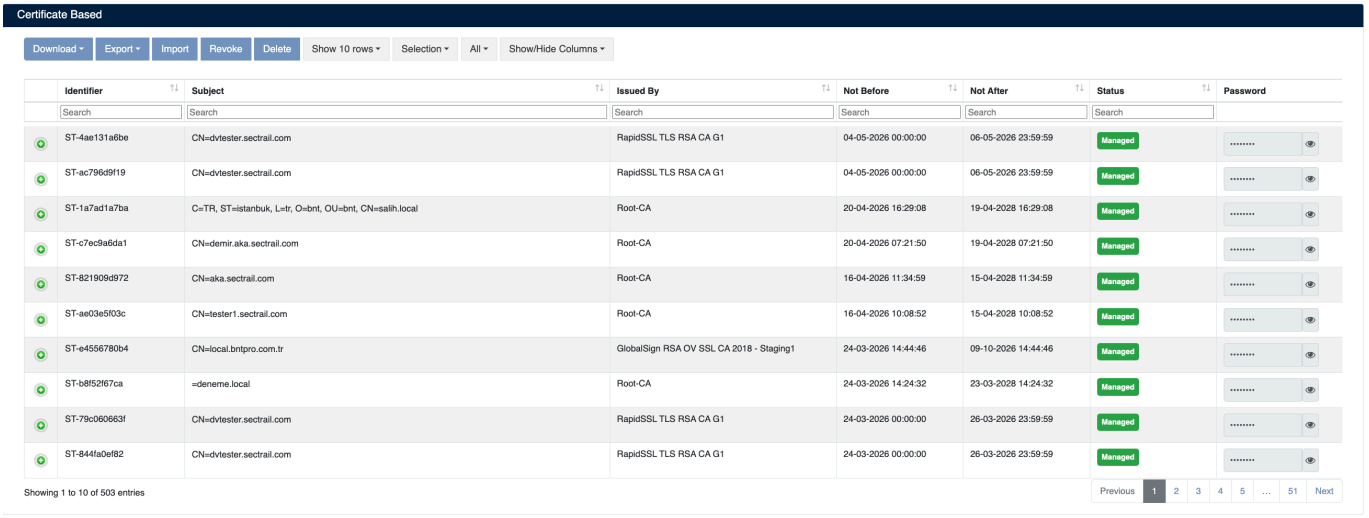
This guide explains step-by-step how to manage certificate inventory in SecTrail CM, import certificates, manage CSR (Certificate Signing Request), and track certificate lists.

> **ABOUT THE FEATURE**
>
> Inventory management allows you to view a centralized list of certificates signed through SecTrail CM and certificates imported from external sources. For certificates found through discovery, review the Discovery Configuration page.

Certificate List

View and manage all imported and discovered certificates in a centralized list.

> **ACCESS PATH**
>
> To access the certificate list: Go to **Inventory -> Certificate Store -> Certificate&Keys** menu.



Certificate List - All Certificates and Their Status

List Information

The following details are displayed for each certificate in the certificate list:

Column	Description
Identifier	Auto-generated unique identifier for the certificate
Created At	Date and time the certificate was added to the system
Subject	Certificate subject information (CN, O, OU, C, ST, L)
Certificate Type	Certificate type (CERT/KEY, Certificate, CSR)
Issued By	CA (Certificate Authority) that signed the certificate
Not Before	Certificate validity start date and time
Not After	Certificate validity end date and time
Status	Certificate management status: `Managed` (Managed) or `Monitored` (Monitored)
Password	Certificate private key password

Certificate Statuses

Each certificate has a status indicator on the left:

Icon	Status	Description
	Active	Certificate is valid and active
	Expiring Soon	Certificate will expire soon
	Expired	Certificate has expired

Available Operations

Top Menu Operations

- **Show 10 rows** - Set number of certificates to display per page
- **Selection** - Select certificates for batch operations
- **Export** - Export certificate list (CSV, Excel, PDF)
- **Import** - Import new certificate
- **Revoke** - Revoke selected certificates
- **Delete** - Delete selected certificates
- **Download** - Download selected certificates in different formats (Zip, Pfx, Jks, Cer, Chain, Bundle, Der, P7b, Key)
- **Last** - View recently added certificates
- **Show/Hide Columns** - Customize displayed columns

Filtering and Search

You can search each column in the list and adjust the number of records displayed per page.

Row-Based Operations

You can perform view, download, delete, and detail view operations on each certificate row.

Batch Operations

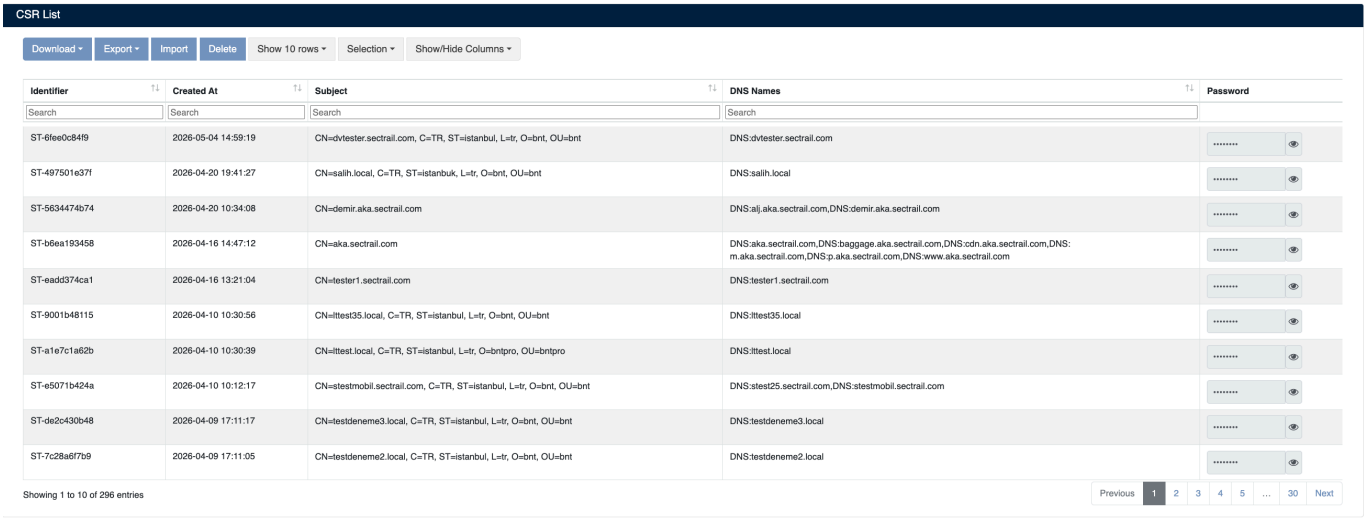
You can select multiple certificates to perform Export, Download, Revoke, or Delete operations in bulk.

> **CAUTION**
>
> **Revoke** operation revokes the certificate from the CA and is irreversible. **Delete** operation only removes it from SecTrail CM inventory.

CSR List

You can view and manage all certificate requests (CSR) in a centralized list.

> **ACCESS PATH**
>
> To access the CSR list: Go to **Inventory -> Certificate&Keys -> CSR List** menu.



CSR List - Certificate Requests

List Information

The following information is displayed for each record in the CSR list:

Column	Description
Identifier	Auto-generated unique identifier for the CSR
Created At	Date and time the CSR was created
Subject	Subject information in the CSR (CN, O, OU, C, ST, L)
E-Mail Address	Email address defined in the CSR
Certificate Type	CSR type (usually `CSR`)
Password	CSR private key password (shown hidden if exists)

Available Operations

Top Menu Operations

- **Show 10 rows** - Set number of records to display per page
- **Selection** - Select CSR for batch operations
- **Export** - Export CSR list
- **Import** - Add new CSR
- **Delete** - Delete selected CSRs
- **Download** - Download selected CSRs

Filtering and Search

You can search each column in the list and adjust the number of records displayed per page.

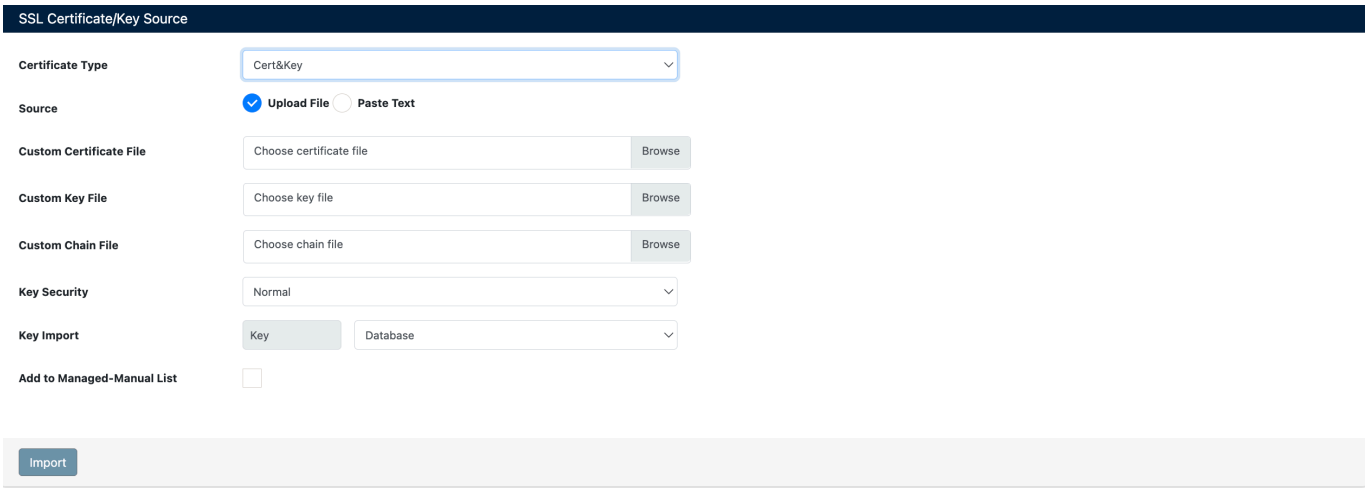
Row-Based Operations

You can perform view, download, and delete operations on each CSR row.

Certificate Import

SecTrail CM offers flexible import options that support different certificate types and sources.

> **ACCESS PATH**
>
> To import certificates: Go to **Inventory -> Certificate Store -> Certificate&Keys** or **CSR List** page and click the **Import** button.



Certificate Import Screen

Certificate Types

You can select one of the following certificate types on the import screen:

Type	Description	Use Case
Cert&Key	Certificate and private key together	For importing existing active certificates and keys
Certificate	Certificate file only	For monitoring purposes or adding certificate only without key
CSR	Certificate Signing Request	For creating and managing certificate requests
PKCS12	Certificate and key packaged in PKCS#12 format	For certificates exported from Windows or Java environments

Cert&Key Import

Used to import certificate and private key together.

Configuration Parameters

Parameter	Description	Options
Certificate Type	Select data type to import	Select `Cert&Key`
Source	Determine how to provide certificate and key	- **Upload File:** File upload - **Paste Text:** Paste text
Custom Certificate File	Upload certificate file	In `.crt`, `.cer`, `.pem` formats
Custom Key File	Upload private key file	In `.key`, `.pem` formats
Custom Chain File	(Optional) Certificate chain file	For Intermediate and Root CA certificates
Key Security	Determine key security level	- **Normal:** Unencrypted key - **Password:** Encrypted key (passphrase required)
Key Import	Select where the key will be stored	- **Key:** In SecTrail CM database - **Database:** Store in separate database
Add to Managed-Manual List	Add certificate to managed list	Check for manual management

> **IMPORTANT**
>
> - Use **Custom Chain File** to add Intermediate CA and Root CA certificates
> - For encrypted keys, select `Password` in **Key Security** field and enter password
> - **Key Import** option is important for secure key storage

Steps

1. Select `Cert&Key` as **Certificate Type**
2. Select `Upload File` or `Paste Text` as **Source**
3. Upload certificate, key, and chain files via **Browse** buttons or paste their contents
4. If key is encrypted, select **Key Security** `Password` and enter password
5. Select **Key Import** method (Key or Database)

6. Optionally check **Add to Managed-Manual List** option
7. Click **Import** button to complete the import

Certificate Import

Used to import certificate file only (without private key).

> **WHEN TO USE?**
>
> - When adding public certificates for monitoring purposes
> - For certificates that will only be monitored
> - For third-party certificates you don't have the private key for

Configuration

Select `Certificate` as **Certificate Type** and upload only the certificate file. Other steps are the same as Cert&Key.

CSR Import

Used to import Certificate Signing Request (CSR) files.

> **WHAT IS CSR?**
>
> Certificate Signing Request (CSR) is a special file used when requesting an SSL/TLS certificate from a Certificate Authority (CA). CSR contains domain name, organization information, and public key.

Configuration

1. Select `CSR` as **Certificate Type**
2. Upload your CSR file or paste its content
3. Click **Import** button

PKCS12 Import

Imports certificates and keys packaged in PKCS#12 format.

> **WHAT IS PKCS12?**
>
> PKCS#12 (usually with `.pfx` or `.p12` extension) is a format that packages certificate, private key, and chain in a single file. It's commonly used when exporting from Windows IIS and Java Keystores.

Configuration

1. Select `PKCS12` as **Certificate Type**
2. Upload `.pfx` or `.p12` file
3. Enter PKCS12 file password (if exists)
4. Click **Import** button

Discovered Certificates

You can view, manage, and categorize all certificates found through discovery operations.

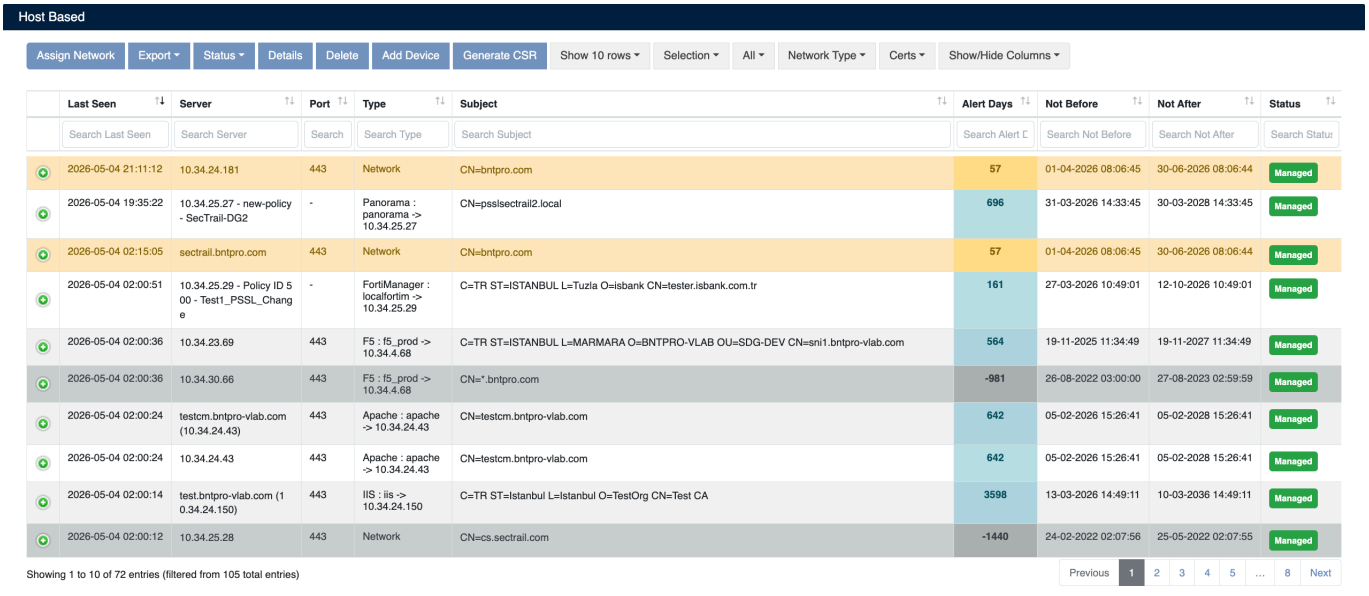
> **ACCESS PATH**
>
> To view discovered certificates, you can use the following paths in the application panel:
>
> - **Inventory -> Certificate Registry -> Host Based** - Server-based view
> - **Inventory -> Certificate Registry -> Certificate Based** - Certificate-based view

Discovered Certificates List

You can examine discovered certificates in SecTrail CM in two different views:

- **Certificate-Based List** - Shows each unique certificate in a single row
- **Server-Based List** - Lists certificates according to the servers they're found on

Server-Based List View



Discovered Certificates - Server-Based View

List Information

The following information is displayed for each row in the server-based view:

- **Last Seen** - Date and time the certificate was last seen
- **Server** - IP address or hostname of the server where the certificate is found
- **Port** - Which port the certificate is running on (e.g., `443`, `8443`)
- **Type** - Network type of the certificate (`Network`, `External`, `F5`, etc.)
- **Subject** - Common Name (CN) information of the certificate
- **Not Before** - Certificate validity start date

- **Not After** - Certificate validity end date
- **Status** - License status of the certificate (`Managed` or `Monitored`)

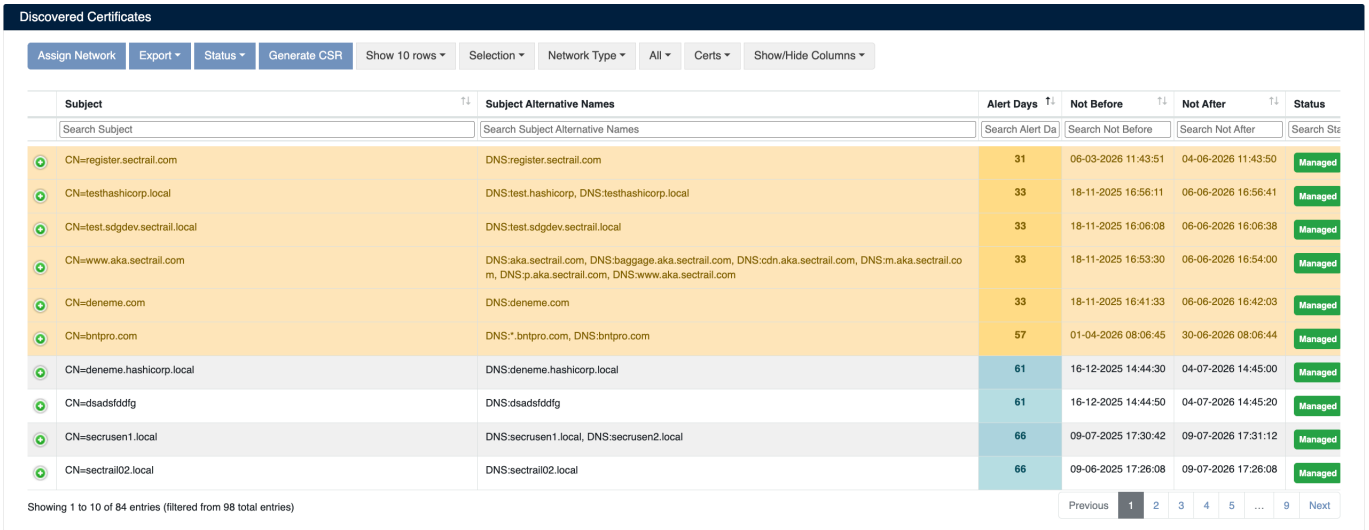
Operations on the List

From the toolbar at the top of the page, you can perform the following operations:

- **Show X rows** - Set the number of rows to display per page (25, 50, 100)
- **Selection** - Select multiple rows for batch operations
- **Export** - Export the list (in Excel, CSV, PDF formats)
- **Status** - Filter by license status (`Managed` , `Monitored`)
- **Details** - View details of selected certificate
- **Delete** - Delete selected records
- **Add Device** - Add new device
- **Generate CSR** - Create Certificate Signing Request (CSR)
- **Last** - Filter by last seen time
- **Network Type** - Filter by network type
- **Certs** - Filter by certificate chain type (Server Certificate, Signing Certificate)
- **Show/Hide Columns** - Customize displayed columns

> **COLUMN CUSTOMIZATION**
>
> With the **Show/Hide Columns** button, you can customize displayed columns. You can add or remove columns according to your needs to use the list more efficiently.

Certificate-Based List View



Discovered Certificates - Certificate-Based View

List Information

In the certificate-based view, each row represents a unique certificate and includes the following information:

- **Subject** - Certificate's Common Name (CN) and DN information
- **Subject Alternative Names** - Certificate's SANs (DNS names) list

- **Not Before** - Certificate validity start date
- **Not After** - Certificate validity end date
- **Status** - Certificate license status

Status (License Status)

There are two different statuses for discovered certificates:

Status	Description	Usage Purpose
Managed	Certificates fully managed by SecTrail CM	Automatic renewal, deployment, lifecycle
Monitored	Certificates only displayed in inventory (read-only)	Provides inventory visibility, no alarms/warnings

MANAGED VS MONITORED

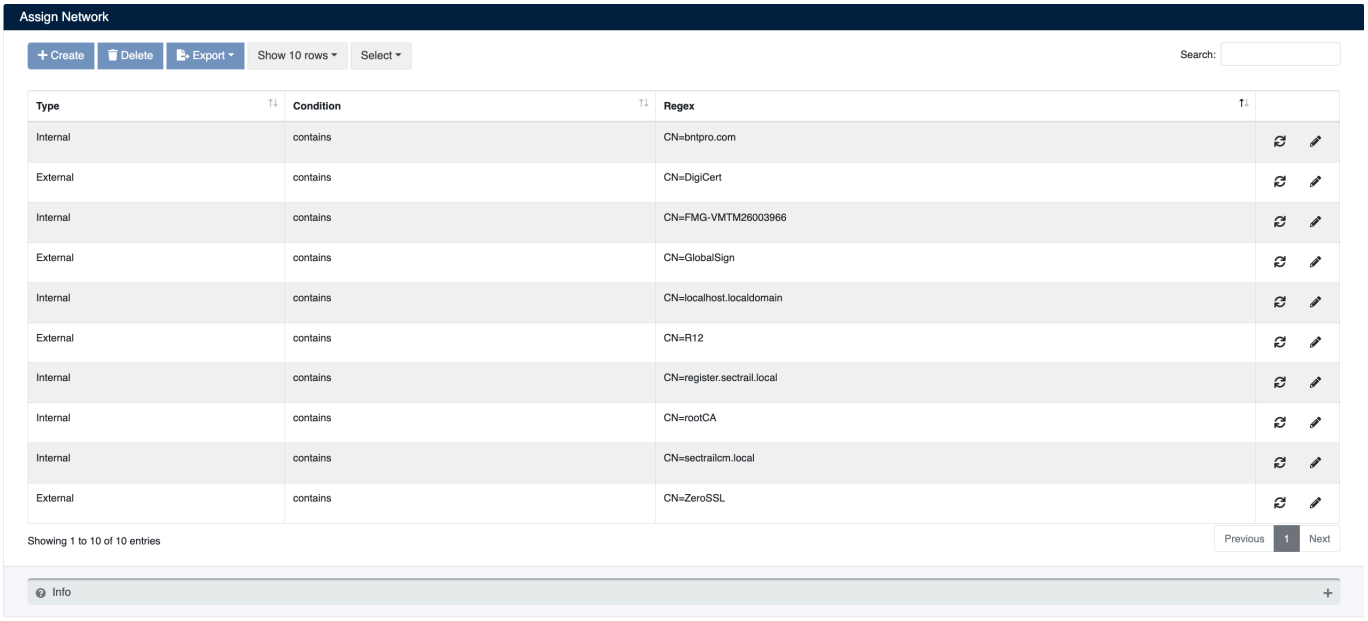
- **Managed:** Full control over certificates - create, renew, deploy, rotate operations possible
- **Monitored:** Inventory visibility only - certificates are displayed in inventory, but alarm, warning, and management operations cannot be performed

Network Configuration (Network Type Configuration)

Values in the Network Type column determine which network category the certificates belong to. These values can be customized with the **Network Configuration** feature.

NETWORK CONFIGURATION ACCESS

You can access network type configuration settings by clicking the **Assign Network** button on the **Inventory -> Certificate Registry -> Certificate Based** or **Host Based** pages.



Network Configuration Management - Network Type Definitions

What is Network Configuration?

Network Configuration allows you to automatically categorize certificates based on Subject (CN) information. This way:

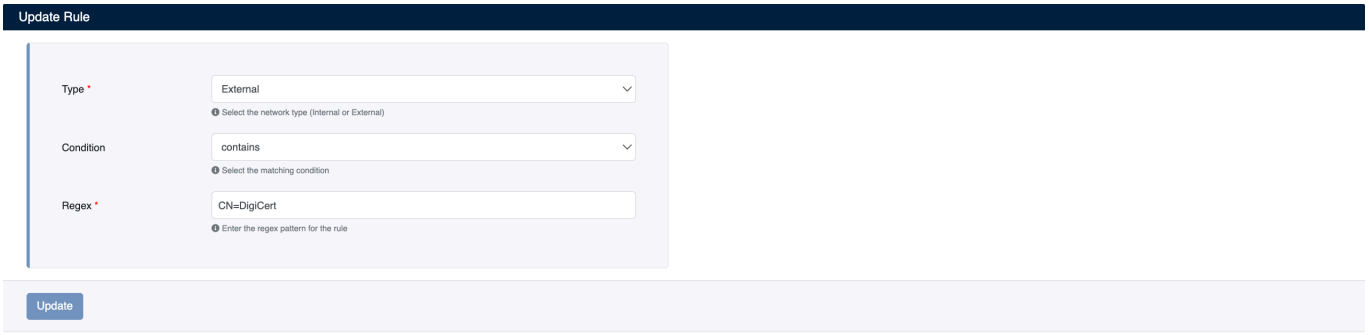
- You can automatically separate internal and external certificates
- You can group certificates belonging to specific Certificate Authorities (CA)
- You can make certificate reporting more meaningful
- You can speed up filtering and search operations

Network Configuration List

On the list page, you can see all defined network type rules:

- **Type** - Network type category (`External` , `Internal`)
- **Condition** - Matching condition (usually `contains`)
- **Regex** - Matching rule (text or regex to search within Subject)

Creating New Network Configuration



New Network Configuration Add Form

Configuration Parameters

Parameter	Description	Options
Type	Determine network type	- **External:** External certificates (signed by public CAs) - **Internal:** Internal certificates (private CAs, self-signed)
Condition	Select matching method	- **contains:** Text searched in Subject (used in most cases) - **equals:** Exact match - **regex:** Regular expression matching
Regex	Enter text or regex pattern to search in Subject	- `CN=GlobalSign` (all certificates containing GlobalSign) - `CN=localhost` (localhost certificates) - `CN=.*\.mycompany\.com` (all subdomains under mycompany.com)

After entering the form information, click the **Submit** button to save the configuration.

Viewing Certificate Details

You can view detailed information of a certificate by clicking on any certificate row or pressing the **Details** button:

- **Subject DN** - Full Distinguished Name information
- **Issuer DN** - CA that signed the certificate
- **Serial Number** - Certificate serial number
- **Signature Algorithm** - Signature algorithm (e.g., SHA256withRSA)
- **Public Key** - Public key information and algorithm
- **Validity** - Validity dates (Not Before / Not After)
- **Extensions** - Certificate extensions (SAN, Key Usage, etc.)
- **Thumbprint** - Certificate fingerprint (SHA1, SHA256)

> **AUTOMATION TIP**
>
> When you define Network Configuration rules correctly, newly discovered certificates are automatically assigned to the correct categories and no manual action is required.

Managed-Manual List

This guide explains how to manually add certificates that cannot be discovered to the managed list and monitor them in SecTrail CM.

> **ABOUT THE FEATURE**
>
> The Managed-Manual List allows you to include certificates that cannot be discovered through the network in the alarm and monitoring system. This way, you can monitor all your certificates from a central point and receive expiry alarms.

Overview

When to Use?

The Managed-Manual List is used in the following situations:

- Certificates on internal systems that cannot be accessed by network scanning
- Certificates behind firewalls
- Certificates on offline systems
- Test certificates that need to be managed manually

Key Features

Alarm and Monitoring : Expiry alarms are created for added certificates

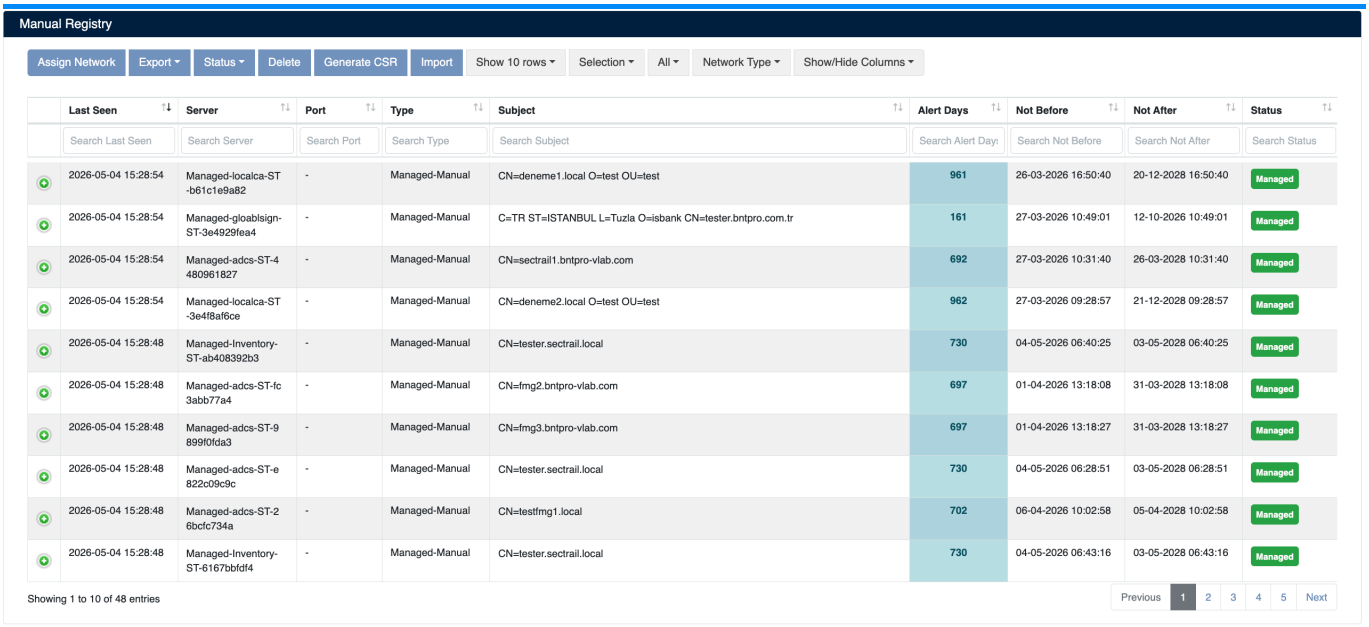
Manual Management : Manually add certificates that cannot be discovered through network scanning to monitoring

Centralized Monitoring : Track all your certificates from a single point

Managed-Manual Certificates List

Manually added certificates or certificates included in the managed list are displayed in this list.

> **ACCESS PATH**
>
> To access the Managed-Manual Certificates list: Go to **Inventory -> Certificate Registry -> Manual Registry** menu.



Managed-Manual Certificates List

List Information

The following information is displayed for each certificate in the Managed-Manual Certificates list:

Column	Description
Last Seen	Date and time the certificate was last seen
Server	Server information where the certificate is located
Port	Port number where the certificate is used
Type	Certificate type (Managed-Manual, Discovered, etc.)
Subject	Certificate subject information (CN, O, OU, C, ST, L)
Not Before	Certificate validity start date
Not After	Certificate validity end date

Available Operations

Top Menu Operations

- **Show 25 rows** - Set the number of records to display per page
- **Selection** - Select certificates for batch operations
- **Export** - Export the list
- **Import** - Add manual certificate
- **Delete** - Remove selected certificates from the list
- **Last** - View recently added certificates
- **Network Type** - Filter by network type
- **Show/Hide Columns** - Customize displayed columns

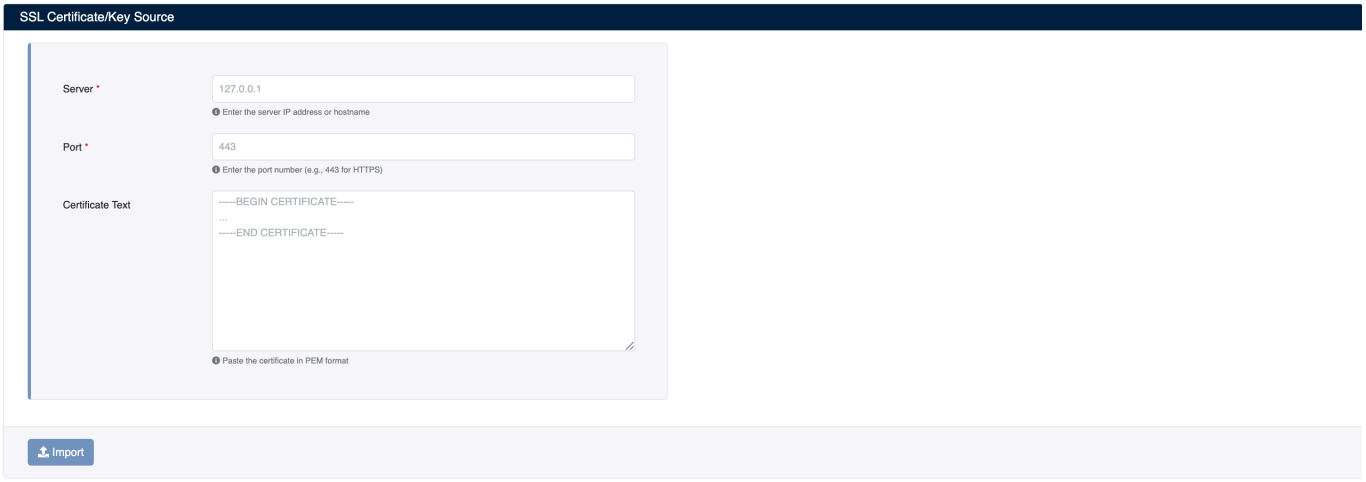
Filtering and Search

You can search each column in the list and adjust the number of records displayed per page.

Manual Certificate Addition

You can manually add certificates that cannot be discovered through the network. You can use two different methods:

> **ACCESS PATH**
>
> Access the addition screen from **Inventory -> Certificate Registry -> Manual Registry -> Import** menu.



Manual Certificate Addition Screen

Addition Methods

Automatic Retrieval with Server and Port

If you have access to the server, you can automatically retrieve the certificate by providing the IP address and port information:

1. Enter the IP address or hostname in the **Server** field (e.g., `192.168.1.100`, `internal.example.com`)
2. Enter the port number in the **Port** field (e.g., `443`, `8443`)
3. Click the **Import** button
4. The system automatically retrieves the certificate and adds it to the list

> **AUTOMATIC RETRIEVAL**
>
> With this method, SecTrail CM automatically retrieves the certificate from the specified server and port. Access to the server must be available.

Manual Addition with Certificate Text

If there is no server access or you have the certificate file, you can paste the certificate text (PEM format) directly:

1. Paste the certificate text in the **Certificate Text** field (must start with `-----BEGIN CERTIFICATE-----`)
2. Optionally enter **Server** and **Port** information (for description purposes)

3. Click the **Import** button

Adding to Managed-Manual List from Inventory

You can also add certificates in the Certificate List to the Managed-Manual list.

Steps

1. Go to **Inventory -> Certificate Registry** menu
2. Select the certificate you want to add to the Managed-Manual list
3. Check the **Add to Managed-Manual List** option on the certificate detail page
4. Save changes

> **USAGE SCENARIO**
>
> This feature is used to monitor certificates that have been imported or added through other methods.

Certificate Creation

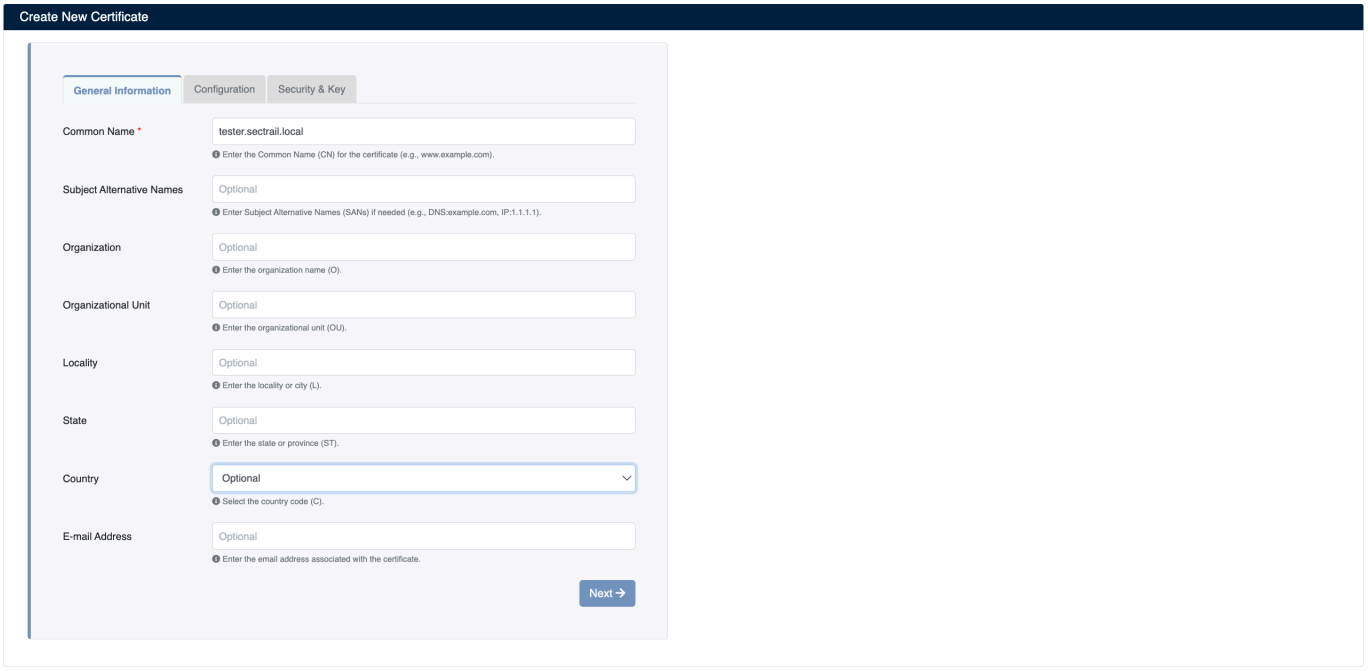
This guide explains step-by-step how to create different types of certificates through SecTrail CM. SecTrail CM allows you to manage your own Certificate Authority (CA) infrastructure and sign certificates for various purposes.

> **ABOUT THE FEATURE**
>
> With the certificate creation feature, you can perform Root CA, Intermediate CA, Self-Signed, CSR, and external CA signing operations. Each certificate type is optimized for different use cases.

Certificate Creation Screen

You can use the built-in certificate manager in SecTrail CM to create a new certificate.

> **ACCESS PATH**
>
> To create certificates: Go to **Inventory -> Issue Certificate -> New Certificate** menu.



Certificate Creation Form - General Information

Certificate Types

SecTrail CM supports the following certificate types for different use cases:

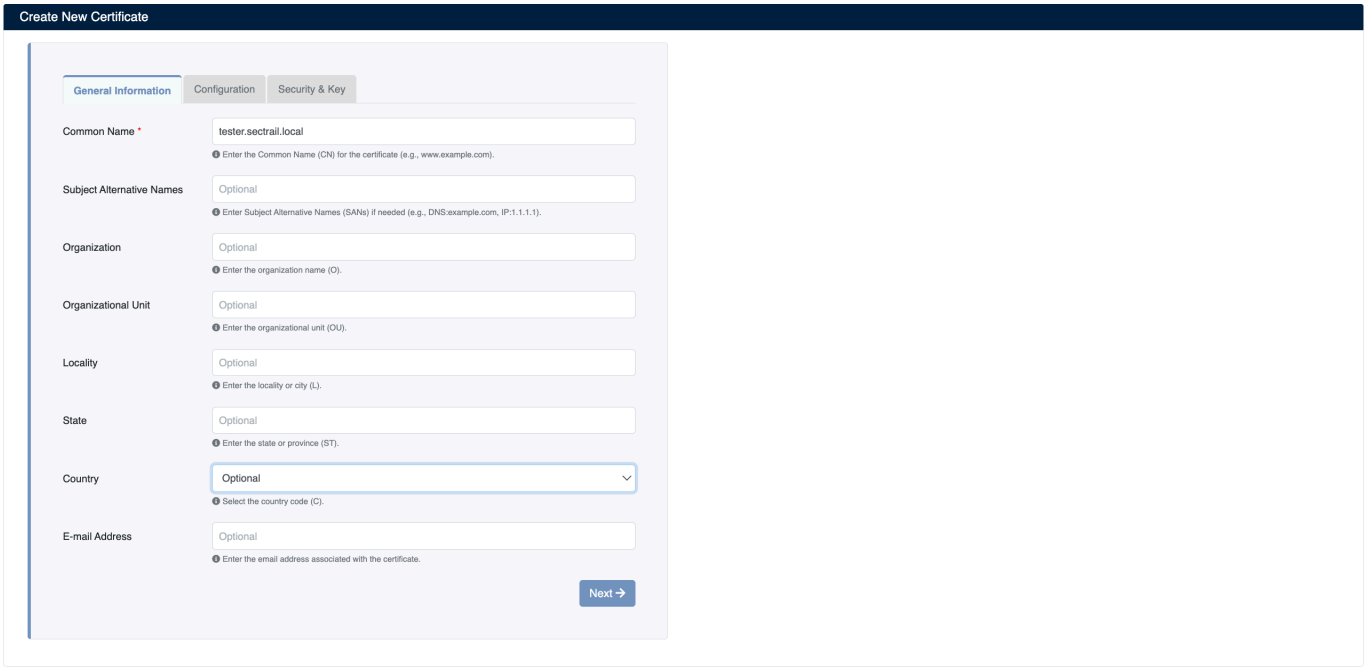
Certificate Type Options

Certificate Type	Description	Usage Purpose
Root CA	Root certificate authority	Top level of your CA infrastructure, signs all other certificates
Intermediate CA	Intermediate certificate authority	Signed by Root CA, signs end-user certificates
Self-Signed	Self-signed certificate	For test environments, internal applications, development
Sign With Local CA	Signing with local CA	Sign new certificates with existing CA in SecTrail CM
CSR	Certificate Signing Request	Create certificate request to be signed by external CAs
External CA	Signing with external CA	Signing with integrated CAs like ADCS, GlobalSign, DigiCert, Hashicorp Vault

Certificate Parameters

The certificate creation form is presented in three tabs.

Tab 1: General Information

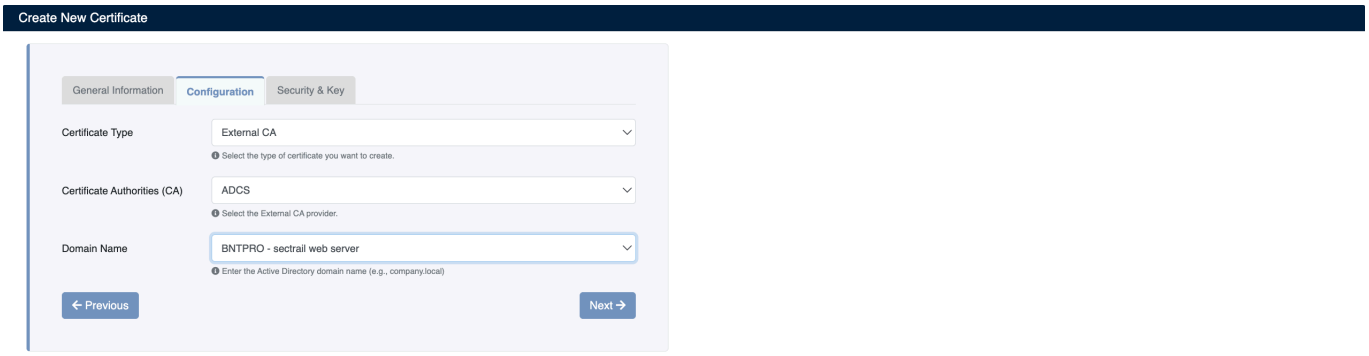


- **Common Name**: Main domain name (FQDN) of the certificate — required (e.g. `example.com`, `*.example.com`)
- **Subject Alternative Names**: Additional domain names and IP addresses (e.g. `DNS:example.com,IP:1.1.1.1`)
- **Organization**: Organization name (O)
- **Organizational Unit**: Department or unit (OU)
- **Locality**: City (L)
- **State**: State or province (ST)

- **Country**: Country code — select from dropdown (C)
- **E-mail Address**: Contact email address

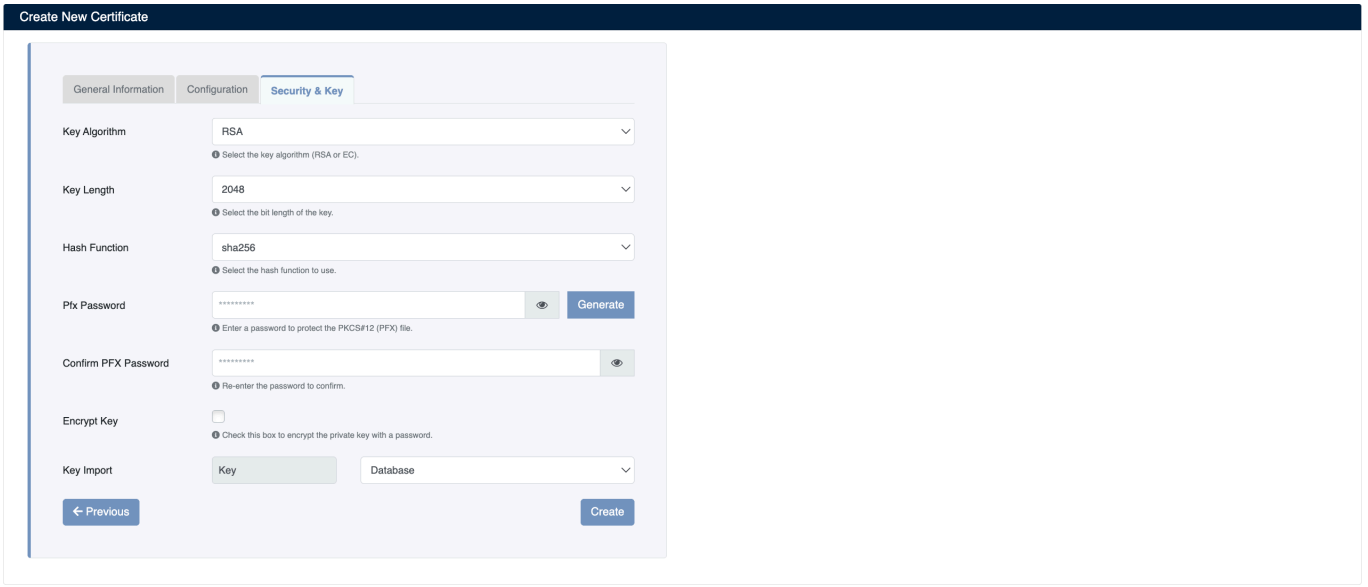
> **SUBJECT ALTERNATIVE NAMES (SAN)**
>
> Separate multiple values with commas: `DNS:example.com,DNS:www.example.com,IP:1.1.1.1`

Tab 2: Configuration



- **Certificate Type**: Certificate type (External CA, Local CA, Self-Signed, CSR, etc.)
- **Certificate Authorities (CA)**: External CA provider to use (e.g. `ADCS`, `GlobalSign`, `DigiCert`)
- **Domain Name**: Active Directory domain name (for External CA)

Tab 3: Security & Key



- **Key Algorithm**: Key algorithm (`RSA` or `EC`)
- **Key Length**: Key bit length (e.g. `2048`, `4096`)
- **Hash Function**: Hash algorithm (e.g. `sha256`)
- **Pfx Password**: Private key protection password; can be auto-generated with **Generate**
- **Confirm PFX Password**: Password verification
- **Encrypt Key**: Should private key be stored encrypted?

- **Key Import**: Where the key will be stored (`Key` , `Database` , `HSM` , `BeyondTrust`)

> **KEY STORAGE OPTIONS**
>
> SecTrail CM offers multiple options for securely storing private keys:
>
> - **Key:** Private key is stored together with certificate (default)
> - **Database:** Stored encrypted in SecTrail CM database
> - **HSM (Hardware Security Module):** Stored in hardware security module (most secure, recommended for enterprise environments)
> - **BeyondTrust Password Safe:** Stored in central password vault with BeyondTrust integration
>
> For configuring HSM and BeyondTrust integrations, review the Integrations page.

Extended Key Usage (EKU) Values

Determines the purposes for which the certificate can be used:

EKU Value	Description	Use Case
serverAuth	Server authentication	Web servers (HTTPS), TLS/SSL
clientAuth	Client authentication	VPN, mutual TLS, user certificates
codeSigning	Code signing	Software, application signing
emailProtection	Email protection	S/MIME, email encryption
timeStamping	Time stamping	Document and transaction timestamps
ocspSigning	OCSP response signing	OCSP responder certificates

Certificate Types and Creation Steps

1. Creating Root CA

Root CA forms the foundation of your own PKI infrastructure. It is used to sign all other certificates.

> **WHEN TO USE?**
>
> - When setting up a new PKI infrastructure
> - When creating your own internal certificate authority
> - When you want to centrally manage all organization certificates

Steps

1. Select `Root CA` from **Certificate Type** field
2. Fill in **basic information**:

- **Common Name:** CA name (e.g., `MyCompany Root CA`)
- **Organization:** Company name
- **Country:** Country code

3. Set **security parameters**:

- **Lifetime:** 3650 days (10 years - Root CAs are long-lived)
- **Key Length:** 4096 bit (maximum security)
- **Hash Function:** sha256 or sha384

4. Set and confirm **Pfx Password**
5. Leave **Extended Key Usage** field empty (Root CA is used for all purposes)
6. Click **Submit** button

> **VERY IMPORTANT**
>
> The Root CA private key is extremely critical. If you lose or have this key stolen, your entire PKI infrastructure is compromised. You must:
>
> - Use a strong password
> - Take encrypted backup
> - Keep access limited

2. Creating Intermediate CA

Intermediate CA acts as a bridge between Root CA and end-user certificates.

> **WHEN TO USE?**
>
> - To protect Root CA (Root CA can be kept offline)
> - When creating separate CAs for different departments or regions
> - As a good security practice (recommended)

Steps

1. Select `Intermediate CA` from **Certificate Type** field
2. Fill in **basic information**:

- **Common Name:** `MyCompany Intermediate CA`
- Fill in fields like **Organization, Country**

3. Set **security parameters**:

- **Lifetime:** 1825 days (5 years)
- **Key Length:** 2048 or 4096 bit
- **Hash Function:** sha256

4. **Signing with Root CA:** The existing Root CA in the system will automatically sign this Intermediate CA
5. Set **Pfx Password**
6. Click **Submit** button

> **BEST PRACTICE**

> Use Intermediate CA for daily certificate signing operations, keep Root CA offline and in a secure location.

3. Creating Self-Signed Certificate

Self-signed certificates are ideal for quick test and development environments.

> **WHEN TO USE?**
>
> - For development and test environments
> - For internal network applications
> - For proof-of-concept work
> - For quick prototyping

Steps

1. Select `Self-Signed` from **Certificate Type** field
2. Fill in **basic information**:

- **Common Name:** `dev.example.com` or `*.dev.example.com` (wildcard)
- **Subject Alternative Names:** `DNS:dev.example.com,DNS:*.dev.example.com`

3. Set **security parameters**:

- **Lifetime:** 365 days
- **Key Length:** 2048 bit (sufficient for testing)
- **Hash Function:** sha256

4. **Extended Key Usage:** `serverAuth` (for web servers)
5. Set **Pfx Password**
6. Click **Submit** button

> **CAUTION**
>
> Self-signed certificates are marked as untrusted by browsers. Do not use in production environments.

4. Sign With Local CA (Signing with Local CA)

Create new certificates using your existing CAs in SecTrail CM.

> **WHEN TO USE?**
>
> - When creating certificates for production servers
> - When signing certificates with your trusted CA
> - When producing certificates compliant with corporate standards

Steps

1. Select `Sign With Local CA` from **Certificate Type** field
2. **Select CA to sign:** Choose one of the registered CAs in the system

3. Fill in **basic information**:

- **Common Name:** `web.example.com`
- **Subject Alternative Names:** Add all needed domains

4. Set **security parameters**:

- **Lifetime:** 365 or 825 days (according to public trust requirements)
- **Key Length:** 2048 bit
- **Hash Function:** sha256

5. **Extended Key Usage:**

- For web servers: `serverAuth`
- For VPN: `serverAuth,clientAuth`

6. Set **Pfx Password**
7. Click **Submit** button

5. Creating CSR (Certificate Signing Request)

Create CSR to obtain certificate from an external CA (Let's Encrypt, DigiCert, GlobalSign, etc.).

> **WHEN TO USE?**
>
> - When purchasing public certificates
> - When using third-party CA services
> - If your organization has external CA agreements

Steps

1. Select `CSR` from **Certificate Type** field
2. Carefully fill in **basic information**:

- **Common Name:** Domain for which you'll request certificate
- **Organization:** Company name to be verified by CA
- **Organizational Unit, Locality, State, Country:** Required for verification
- **E-mail Address:** Contact email

3. Set **security parameters**:

- **Key Length:** 2048 bit (accepted by most CAs)
- **Hash Function:** sha256

4. Set **Pfx Password** (for private key protection)
5. Click **Submit** button
6. **Download the created CSR** and send to CA

> **POST-CSR STEPS**
>
> 1. Download CSR from SecTrail CM

2. Go to your CA provider's website
3. Upload or paste CSR
4. Complete domain verification process
5. Receive signed certificate from CA
6. Import certificate to SecTrail CM (Import)

6. External CA (Signing with External CA)

Sign certificates directly with external CA systems integrated with SecTrail CM.

WHEN TO USE?

- If you have Microsoft ADCS (Active Directory Certificate Services) integration
- If you have enterprise CA agreements like GlobalSign, DigiCert
- If you're using Hashicorp Vault PKI
- If you want automatic certificate management

Supported External CAs

SecTrail CM supports the following external CA integrations:

CA Provider	Description	Usage
ADCS	Microsoft Active Directory Certificate Services	Windows environments, enterprise PKI
GlobalSign	GlobalSign HVCA (Managed PKI)	Enterprise, high-volume certificate management
DigiCert	DigiCert CertCentral API	Public SSL/TLS certificates
Hashicorp Vault	Vault PKI Secrets Engine	Cloud-native, dynamic certificate management

PREREQUISITE: CA INTEGRATION

You must configure the relevant CA integration **before** signing certificates with external CA.

For Integration Setup:

1. Go to **Settings -> Integrations -> CA Integrations** section
2. Select the CA you want to use (ADCS, GlobalSign, DigiCert, Hashicorp Vault)
3. Configure API information and connection settings
4. Test the connection

For detailed setup instructions, review the Integrations page.

ADCS Signing Steps

1. **Certificate Type:** Select `External CA`
2. **From External CA Dropdown:** Select `ADCS`
3. **ADCS Configuration:**

- **CA Server:** ADCS server address
- **Certificate Template:** Template name to use
- **Credentials:** Authorization information

4. Fill in **certificate information** (Common Name, SAN, etc.)
5. Click **Submit** button

GlobalSign Signing Steps

1. **Certificate Type:** Select `External CA`
2. **From External CA Dropdown:** Select `GlobalSign`
3. **GlobalSign Configuration:**

- **API Key:** GlobalSign HVCA API key
- **API Secret:** API secret key
- **Profile:** Certificate profile

4. Fill in **certificate information**
5. Click **Submit** button

DigiCert Signing Steps

1. **Certificate Type:** Select `External CA`
2. **From External CA Dropdown:** Select `DigiCert`
3. **DigiCert Configuration:**

- **API Key:** DigiCert CertCentral API key
- **Organization ID:** Org ID in DigiCert
- **Certificate Type:** OV, EV, DV selection

4. Fill in **certificate information**
5. Click **Submit** button

Hashicorp Vault Signing Steps

1. **Certificate Type:** Select `External CA`
2. **From External CA Dropdown:** Select `Hashicorp Vault`
3. **Vault Configuration:**

- **Vault Address:** Vault server address
- **PKI Path:** PKI secrets engine path
- **Token:** Vault authentication token
- **Role:** Vault PKI role name

4. Fill in **certificate information**
5. Click **Submit** button

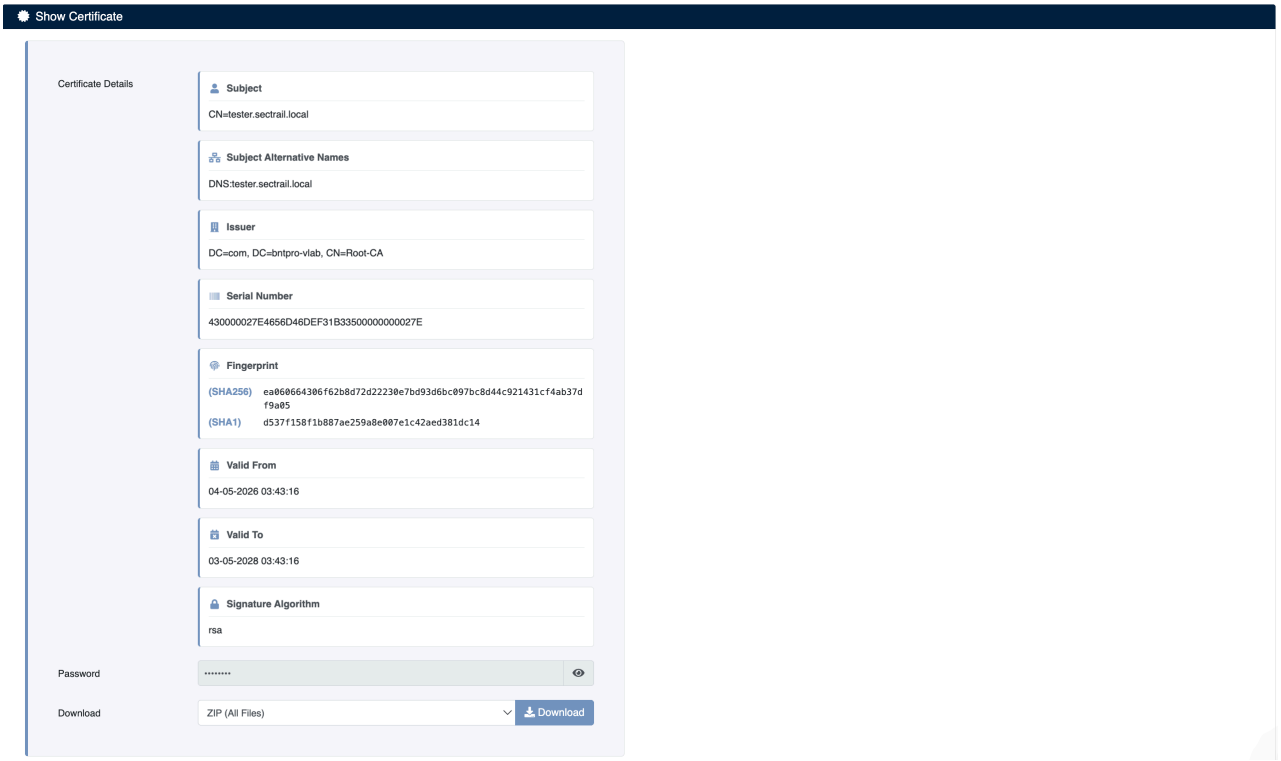
Post-Certificate Creation Operations

After a certificate is successfully created, it is automatically added to inventory and you can perform various operations.

> **AUTOMATIC INVENTORY RECORDING**
>
> Every certificate you create is automatically added to the inventory list on the **Inventory -> Certificate Store -> Certificates & Keys** page. From here you can view, manage, and track all your certificates. For detailed information about the inventory list, review the Inventory Management page.

Viewing and Downloading Certificate

Immediately after certificate creation, the **Show Certificate** screen opens and you can view certificate information:



Certificate Details and Download Options

Displayed Information

Field	Description
Name	Certificate's Common Name (CN) value (e.g., `sectrail.local`)
Certificate	Complete certificate content in PEM format (starts with `-----BEGIN CERTIFICATE-----`)
Password	Certificate private key password (shown hidden for security, can be viewed by clicking eye icon)

Downloading Certificate

After certificate creation, you can download in different formats using download buttons on the screen:

- **Download Zip** - Archive containing all files (cert, key, chain, pfx, der, jks, bundle)

- **Download Pfx** - PFX/P12 format for Windows IIS and Exchange
- **Download Jks** - Java KeyStore format for Java/Tomcat
- **Download Crt** - Certificate file only (public key)
- **Download Chain** - CA chain files
- **Download Bundle** - Complete certificate chain (cert + intermediate + root)
- **Download Key** - Private key only

> **IMPORTANT NOTE**
>
> You will need the **Pfx Password** value you set to use downloaded certificates.

Access from Inventory List

After certificate creation, you can also access and manage from the **Inventory -> Certificate Store -> Certificates & Keys** page. You can view, filter, and perform various operations on your certificates in the list.

CSR Signing

This guide explains step-by-step how to sign CSR (Certificate Signing Request) through SecTrail CM. You can sign CSRs with local CA or external CA integrations.

> **ABOUT THE FEATURE**
>
> The CSR signing feature allows you to obtain certificates without sharing the private key. You can perform the signing process by uploading a CSR created in your own application to SecTrail CM or by creating a CSR through SecTrail CM.

CSR Signing Scenarios

SecTrail CM supports two different CSR signing scenarios:

1. External CSR Signing (Recommended)

Used when you don't want to share the private key:

1. **Create CSR on your own server/application** (private key stays on your server)
2. **Import CSR to SecTrail CM**
3. **Sign CSR through SecTrail CM**
4. **Download signed certificate and install on your server**

> **SECURITY ADVANTAGE**
>
> With this method, the private key is never shared and only stays on your own server. It is the most secure method.

2. Creating CSR on SecTrail CM

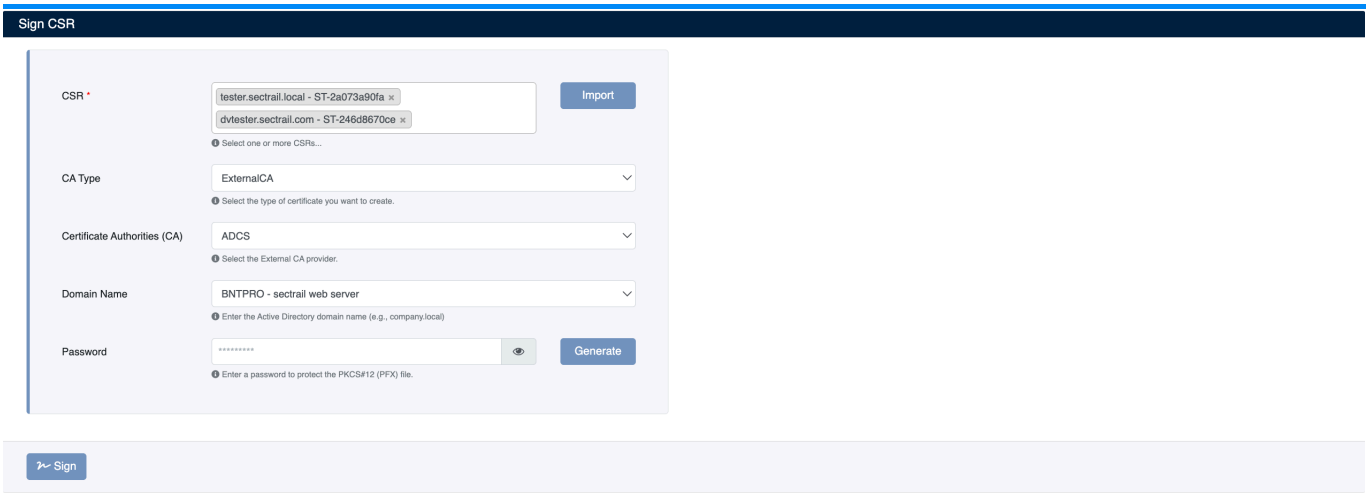
Used for centralized management:

1. **Create CSR through SecTrail CM**
2. **Sign the created CSR immediately**
3. **Download certificate and private key together**

CSR Signing Screen

There is a special interface in SecTrail CM for CSR signing operations.

> **ACCESS PATH**
>
> To sign CSR: Go to **Inventory -> Issue Certificate -> Sign CSR** menu.



CSR Signing Form

CSR Signing Parameters

Basic Information

Field	Description	Example
CSR	CSR selection to be signed	Select existing CSR from dropdown
CA Type	Signing type	Local CA, External CA
External CA	External CA selection (if CA Type: External CA)	ADCS, GlobalSign, DigiCert, Hashicorp Vault
Domain Name	Certificate domain name (optional)	Descriptive name
Password	Certificate private key password	Strong password

> **CSR SELECTION**
>
> All CSRs in SecTrail CM inventory are listed in the CSR dropdown. Format: `[Organization] - [Identifier]` (e.g., `bntpro.com - ST-5cc54e0593`)

CA Type Options

1. Local CA (Local CA)

Signing CSR with your existing CAs in SecTrail CM:

Usage Scenarios:

- For internal/corporate certificates
- For test and development environments
- For certificates managed with your own PKI infrastructure

Advantages:

- Fast signing

- Full control
- No additional cost
- Can work offline

2. External CA (External CA)

Signing with integrated CAs like ADCS, GlobalSign, DigiCert, Hashicorp Vault:

Usage Scenarios:

- For public certificates
- For certificates requiring browser trust
- For compliance requirements
- For enterprise CA integrations

Supported External CAs:

CA Provider	Description	Usage
ADCS	Microsoft Active Directory Certificate Services	Windows environments, enterprise PKI
GlobalSign	GlobalSign HVCA (Managed PKI)	Enterprise, high-volume certificate management
DigiCert	DigiCert CertCentral API	Public SSL/TLS certificates
Hashicorp Vault	Vault PKI Secrets Engine	Cloud-native, dynamic certificate management

> **PREREQUISITE: CA INTEGRATION**
>
> You must configure the relevant CA integration **before** using External CA.
>
> For detailed setup instructions, review the Integrations page.

CSR Signing Steps

Method 1: External CSR Signing (Private Key Not Shared)

This method is used to obtain certificates without sharing the private key.

Step 1: Creating CSR on Your Own Server

First create CSR and private key on your own server/application:

Creating CSR with Windows/IIS:

1. IIS Manager -> Server Certificates
2. Create Certificate Request
3. Fill in Distinguished Name information
4. Cryptographic Service Provider: Microsoft RSA SChannel, 2048 bit
5. Save CSR file

Step 2: Importing CSR to SecTrail CM

1. Go to **Inventory -> Import Certificate** menu
2. Select `CSR` as **Certificate Type**
3. Upload your CSR file or paste its content
4. Click **Import** button

After CSR is successfully imported, it is added to inventory and assigned an identifier (e.g., `ST-5cc54e0593`).

Step 3: Signing CSR

1. Go to **Inventory -> Issue Certificate -> Sign CSR** menu
2. **CSR Selection:**

- Select the CSR you imported from dropdown
- Format: `[Organization] - [Identifier]`

3. **CA Type Selection:**

- **Local CA:** Signing with CA in SecTrail CM
- **External CA:** Signing with External CA

4. **External CA Selection** (if External CA is selected):

- ADCS, GlobalSign, DigiCert, or Hashicorp Vault

5. **Domain Name** (Optional):

- Enter a descriptive name (e.g., `bntpro.local - copy of sectrail webserver`)

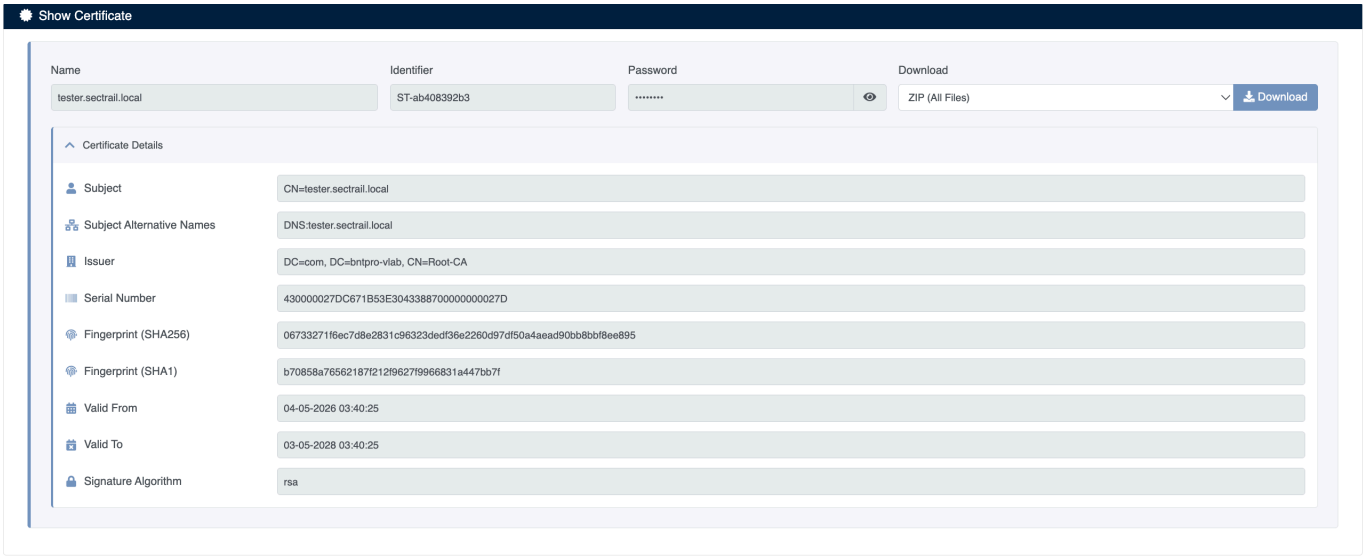
6. **Password:**

- Set a strong password for the certificate
- You can generate an automatic password with the Generate button

7. Click **Sign** button

Step 4: Downloading Signed Certificate

After signing is completed, the **Show Key** screen opens:



Signed Certificate and Download Options

Download Buttons:

- **Download Zip** - All files (cert, chain, bundle)
- **Download Jks** - Java KeyStore format
- **Download Crt** - Certificate file only
- **Download Chain** - CA chain
- **Download Bundle** - Complete certificate chain
- **Download Key** - Private key (only for CSRs created in SecTrail CM)

> **IMPORTANT**
>
> The **Download Key** button **does not work** for external CSRs because the private key is not in SecTrail CM but on your own server. This is a security feature.

Method 2: Creating CSR on SecTrail CM

This method is suitable for centralized management but the private key is also created in SecTrail CM.

Step 1: Creating CSR

1. Go to **Inventory -> Create Certificate** menu
2. Select `CSR` as **Certificate Type**
3. Fill in certificate information:

- Common Name, Organization, Country, etc.

4. **Key Length:** 2048 or 4096 bit
5. Set **Pfx Password**
6. Click **Submit** button

CSR and private key are created and added to inventory.

Step 2: Signing CSR

Follow the steps in **Step 3: Signing CSR** section above.

Step 3: Downloading Certificate and Private Key

In this scenario, since the private key is also in SecTrail CM, the **Download Key** button works and you can download all files.

Domain Name Field

The **Domain Name** field is optional and used for identification purposes:

```
Example: bntpro.local - copy of sectrail webserver
```

This field:

- Helps identify the certificate in inventory
- Used to distinguish multiple similar certificates

- Appears in reports and logs

Password Generation

For the **Password** field:

1. **Manual Input:** Write your own password
2. **Automatic Generation:** Click `GENERATE` button

- Creates strong, random password
- Minimum 16 characters
- Contains uppercase/lowercase letters, numbers, and special characters

3. **View:** You can view the password with the eye icon

> **PASSWORD SECURITY**
>
> Store the password in a secure password manager and use different passwords for each certificate.

Certificate Template Management

This guide explains how to create and manage certificate templates on SecTrail CM. Certificate templates speed up and standardize the certificate creation process by predefining organization information, key algorithm, and other parameters.

> **ABOUT THE FEATURE**
>
> By using templates, you can create certificates from ready-made templates instead of repeatedly entering the same information (Organization, OU, Country, etc.) each time. This saves time and ensures compliance with corporate standards.

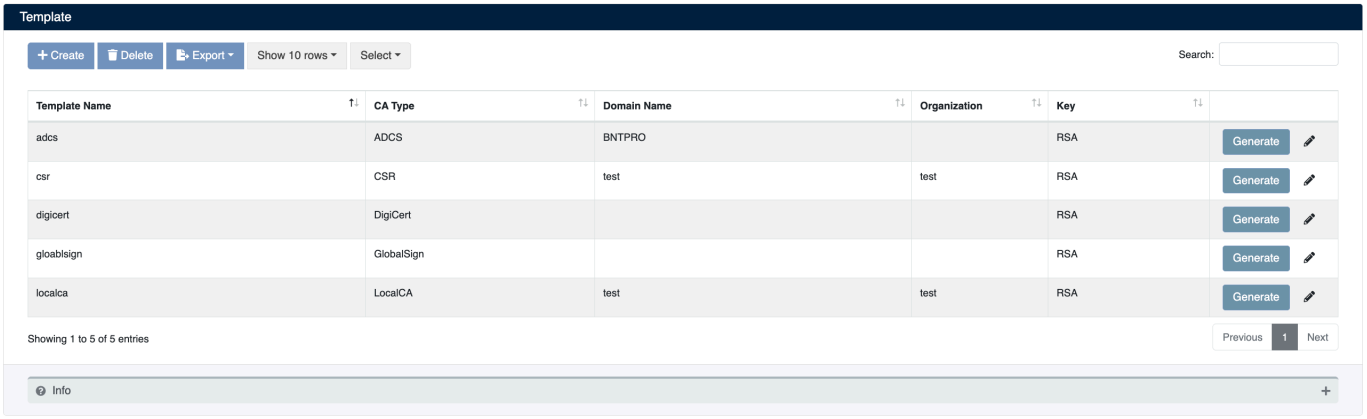
What is a Template?

A template is a predefined structure of certificate creation parameters. By using templates:

- **Fast certificate production:** Just fill in Common Name and SAN fields, all other fields are automatically filled
- **Standardization:** Ensure all certificates are created with the same organization information and security parameters
- **Error reduction:** Prevent manual input errors
- **CA Integration:** Work integrated with external CAs like ADCS, GlobalSign, DigiCert

Template List

> **ACCESS PATH**
>
> For template management: Go to **Inventory -> Issue Certificate -> Templates** menu.



Template List and Operations

You can view and manage all your existing templates in the template list.

List Columns

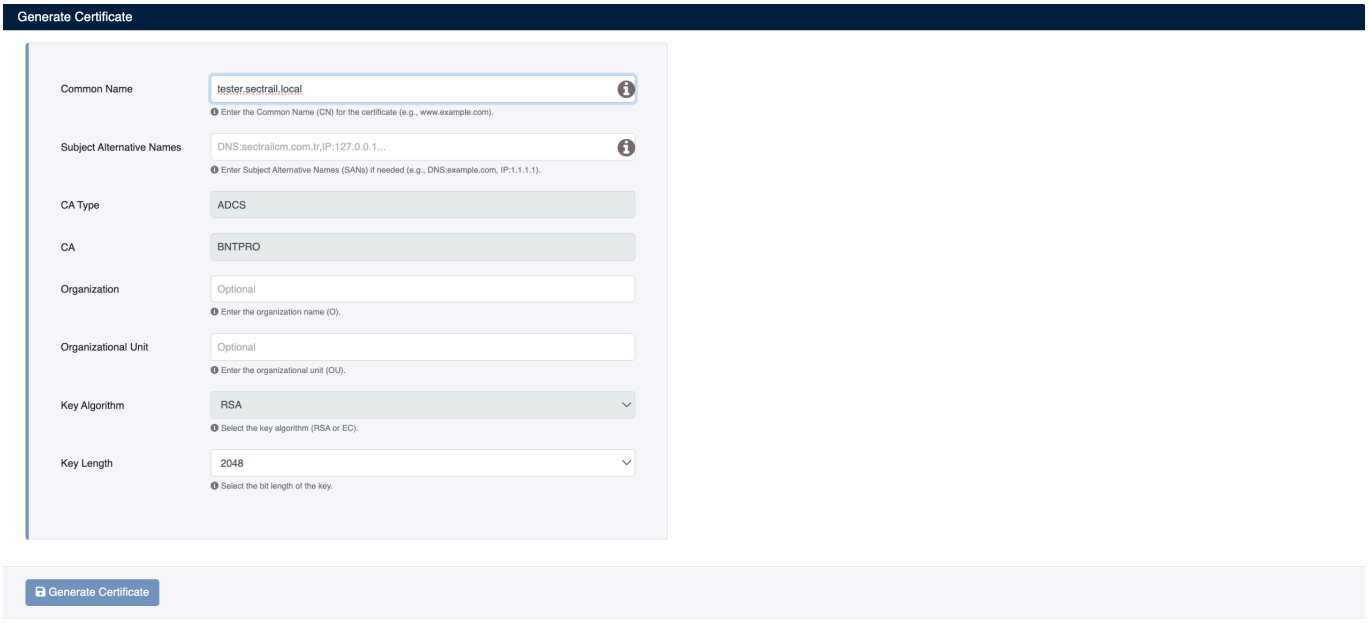
Column	Description
Template Name	Unique name of the template (e.g., `acme`, `adcs`, `csr`)
CA Type	Certificate authority type (ACME, ADCS, CSR, DigiCert, GlobalSign, Hashicorp, LocalCA)
Domain Name	Domain/organization domain the template is associated with
Organization	Organization name
E-mail	Contact email address
Key	Key algorithm (RSA, ECDSA)
Actions	Action buttons (Generate, Edit, Delete)

Template Operations

You can perform three basic operations for each template:

1. Generate (Create Certificate)

When you click the **Generate** button, the certificate creation screen opens with template parameters pre-filled. You only need to fill in Common Name and Subject Alternative Names (SAN) fields.



Creating Certificate with Template

When creating certificate with template:

1. Click the **Generate** button of the desired template from the template list
2. Check auto-filled fields in the opened form:

- CA Type, Organization, OU, Locality, State, Country
- Key Algorithm, Key Length, Hash Function
- Lifetime, E-mail Address

3. Fill in **Common Name** field (e.g., `test.sectrail.local`)
4. Add additional domains or IPs to **Subject Alternative Names** field (optional)
5. Click **Generate** button

> **TIME SAVINGS**
>
> Using templates, you can create certificates instantly by filling in only 2 fields (Common Name and SAN). In normal certificate creation, you need to fill in 15+ fields.

2. Edit (Edit)

Click the **Edit** button to edit existing template. You can update template parameters.

3. Delete (Delete)

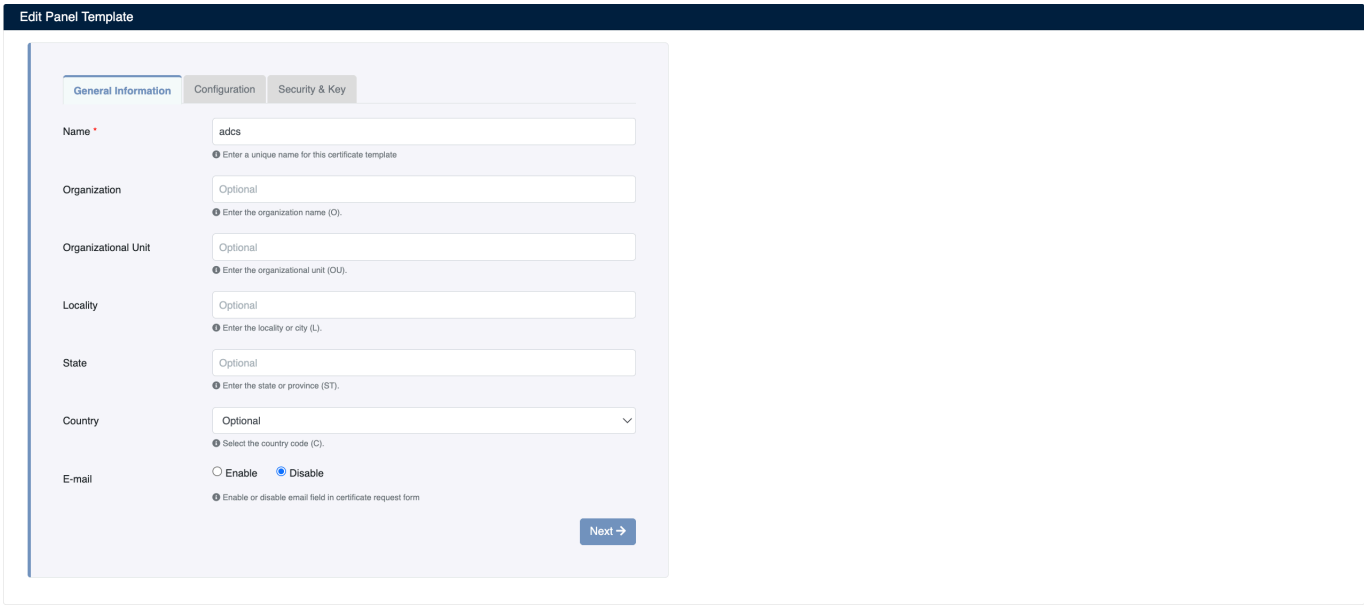
Click the **Delete** button to completely remove the template from the system.

> **CAUTION**
>
> When a template is deleted, certificates previously created with this template are not affected. Only this template cannot be used in future certificate creation operations.

Creating New Template

Click the **Create** button to create a new certificate template. The form is presented in three tabs.

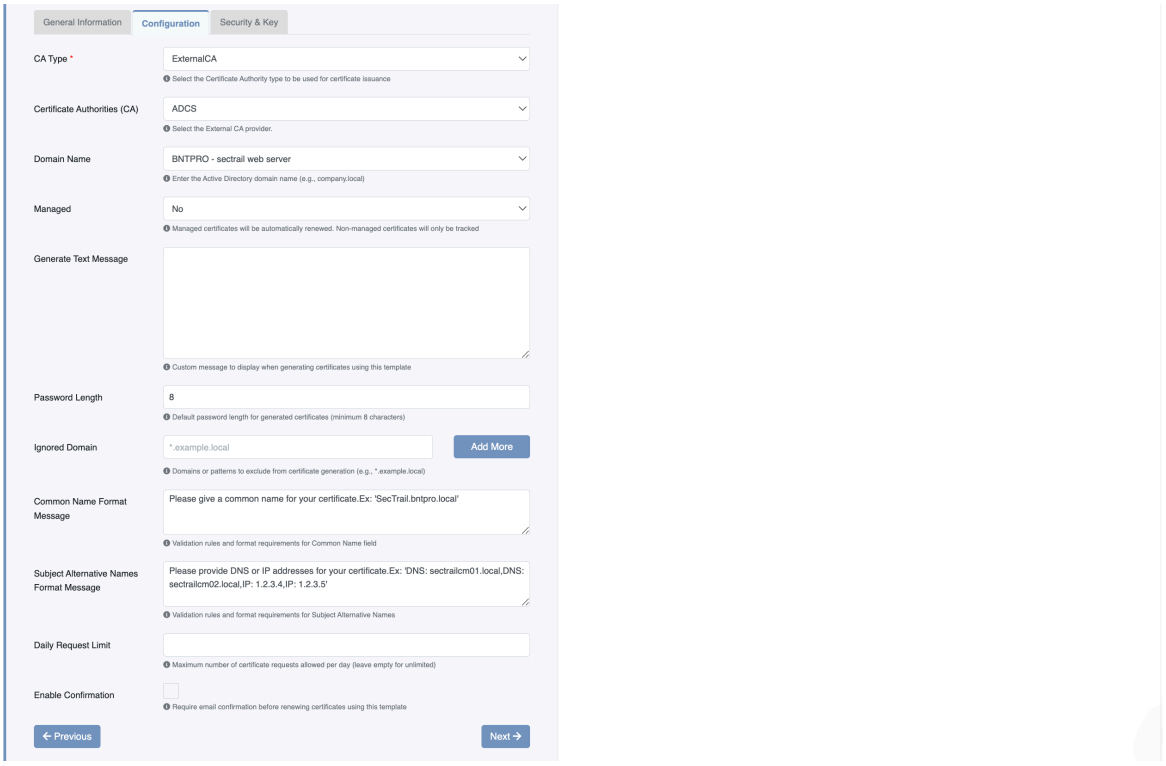
Tab 1: General Information



- **Name**: Unique name for the template (e.g., `adcs`, `prod-ssl`)
- **Organization**: Organization name (O)
- **Organizational Unit**: Department or unit (OU)
- **Locality**: City (L)
- **State**: State or province (ST)

- **Country**: Country code (dropdown selection)
- **E-mail**: Should the email field be shown in the certificate creation form? (`Enable` / `Disable`)

Tab 2: Configuration

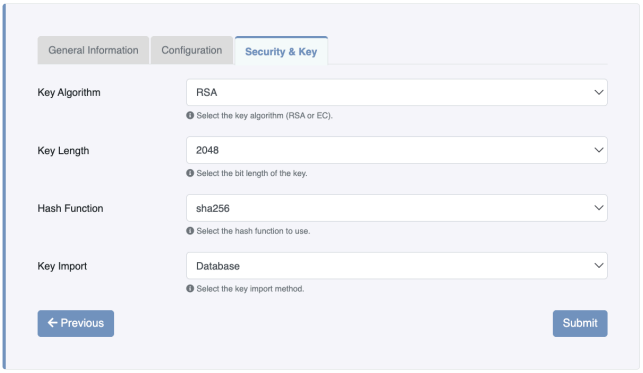


- **CA Type**: Certificate authority type (ExternalCA, LocalCA, etc.)
- **Certificate Authorities (CA)**: External CA provider to use (e.g., `ADCS`)
- **Domain Name**: Active Directory domain name (e.g., `company.local`)
- **Managed**: Should certificates be automatically managed? (`Yes` / `No`)

> **MANAGED CERTIFICATES**
>
> If you set **Managed** to `Yes` , certificates are automatically monitored and renewal alarms are sent. For details: Managed Certificates

- **Generate Text Message**: Custom message to display when a certificate is created
- **Password Length**: Length of automatically generated password (characters)
- **Ignored Domain**: Domains for which certificate creation will be blocked (e.g., `*.example.local`)
- **Common Name Format Message**: Guidance message shown to the user about Common Name format
- **Subject Alternative Names Format Message**: Guidance message about SAN format
- **Daily Request Limit**: Maximum number of certificate requests per day
- **Enable Confirmation**: Require confirmation before creating a certificate?

Tab 3: Security & Key



- **Key Algorithm**: Key algorithm (`RSA` or `EC`)
- **Key Length**: Key bit length (e.g., `2048`)
- **Hash Function**: Hash algorithm (e.g., `sha256`)
- **Key Import**: Where the private key will be stored (`Database` , `Key` , `HSM` , `BeyondTrust`)

Template Types

SecTrail CM supports various CA types for different use cases:

1. LocalCA Template

Used for signing certificates with your own local Certificate Authority.

When to Use:

- For internal network applications
- When producing certificates compliant with corporate standards
- Signing with Root/Intermediate CAs created in SecTrail CM

Example Configuration:

- **Name:** `localca`
- **CA Type:** `LocalCA`
- **Organization:** `secrusen`
- **Key Algorithm:** RSA
- **Key Length:** 2048
- **Lifetime:** 365 days

2. ADCS Template

Creates certificates with Microsoft Active Directory Certificate Services integration.

When to Use:

- In Windows environments
- In enterprise PKI with Active Directory integration
- When automatic domain verification is required

Example Configuration:

- **Name:** `adcs`
- **CA Type:** `ADCS`
- **Organization:** `bntpro`
- **Domain Name:** `bntpro.local`
- **Key Algorithm:** RSA
- **Key Length:** 2048

3. CSR Template

Used to create Certificate Signing Request. Used when you want to get certificates from external CAs.

When to Use:

- When getting certificates from external CAs (Let's Encrypt, DigiCert, etc.)
- For public SSL/TLS certificates
- When third-party verification is required

Example Configuration:

- **Name:** `csr`
- **CA Type:** `CSR`
- **Organization:** `sectrail`

4. ACME Template

Creates automatic certificates with ACME protocol (Let's Encrypt, ZeroSSL, etc.).

When to Use:

- For free SSL certificates with Let's Encrypt
- When you want automatic renewal
- For public domains

Example Configuration:

- **Name:** `acme`
- **CA Type:** `ACME`
- **Organization:** `bntpro`
- **Managed:** Yes (for automatic renewal)
- **Lifetime:** 90 days (Let's Encrypt standard)

5. DigiCert Template

Creates certificates with DigiCert CertCentral API integration.

When to Use:

- If you're a DigiCert customer
- For OV (Organization Validated) or EV (Extended Validation) certificates

- For enterprise SSL certificates

6. GlobalSign Template

Creates certificates with GlobalSign HVCA (Managed PKI) integration.

When to Use:

- If you have GlobalSign agreement
- For high-volume certificate management
- If you're using Managed PKI service

7. Hashicorp Vault Template

Creates dynamic certificates with Hashicorp Vault PKI Secrets Engine.

When to Use:

- In cloud-native environments
- In Kubernetes, microservices architectures
- For dynamic, short-lived certificates

System Integrations

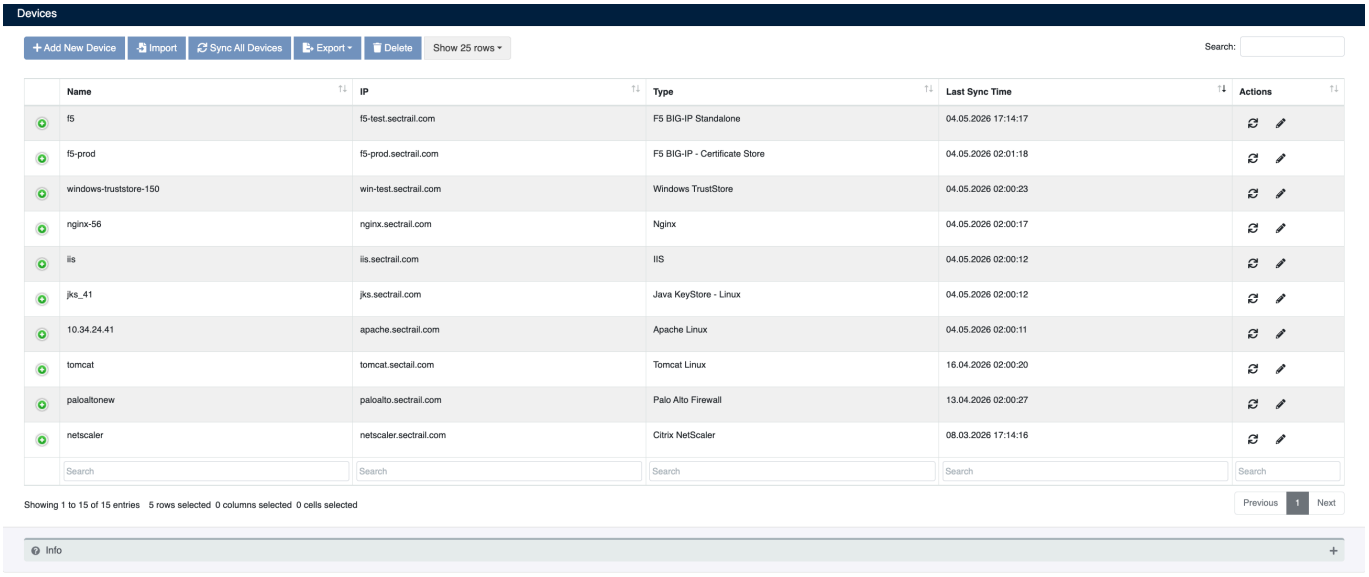
You can manage the configurations and deployment operations of system applications you want to integrate with SecTrail CM from this section. Supported systems:

- F5 BIG-IP · Citrix NetScaler · FortiWeb · FortiGate · FortiManager
- NGINX / NGINX Plus · Palo Alto Networks · PaloAlto Panorama
- Apache · IIS · Apache Tomcat
- Windows TrustStore · Java Keystore (JKS)
- IBM DataPower · HashiCorp Vault

> **INTEGRATION CONFIGURATIONS**
>
> You can access general configuration steps for all system integrations from the Integrations -> System page.

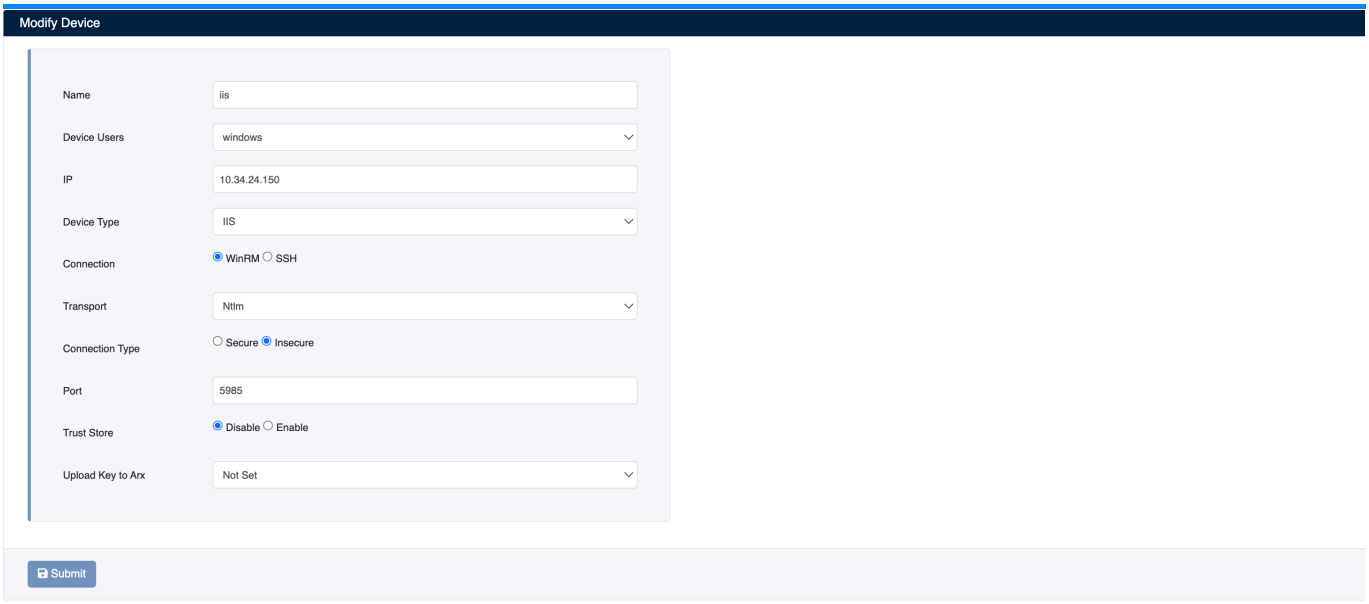
Devices

The configurations of system applications you want to integrate are listed on the **Automation -> Devices** page.



Defined Device List

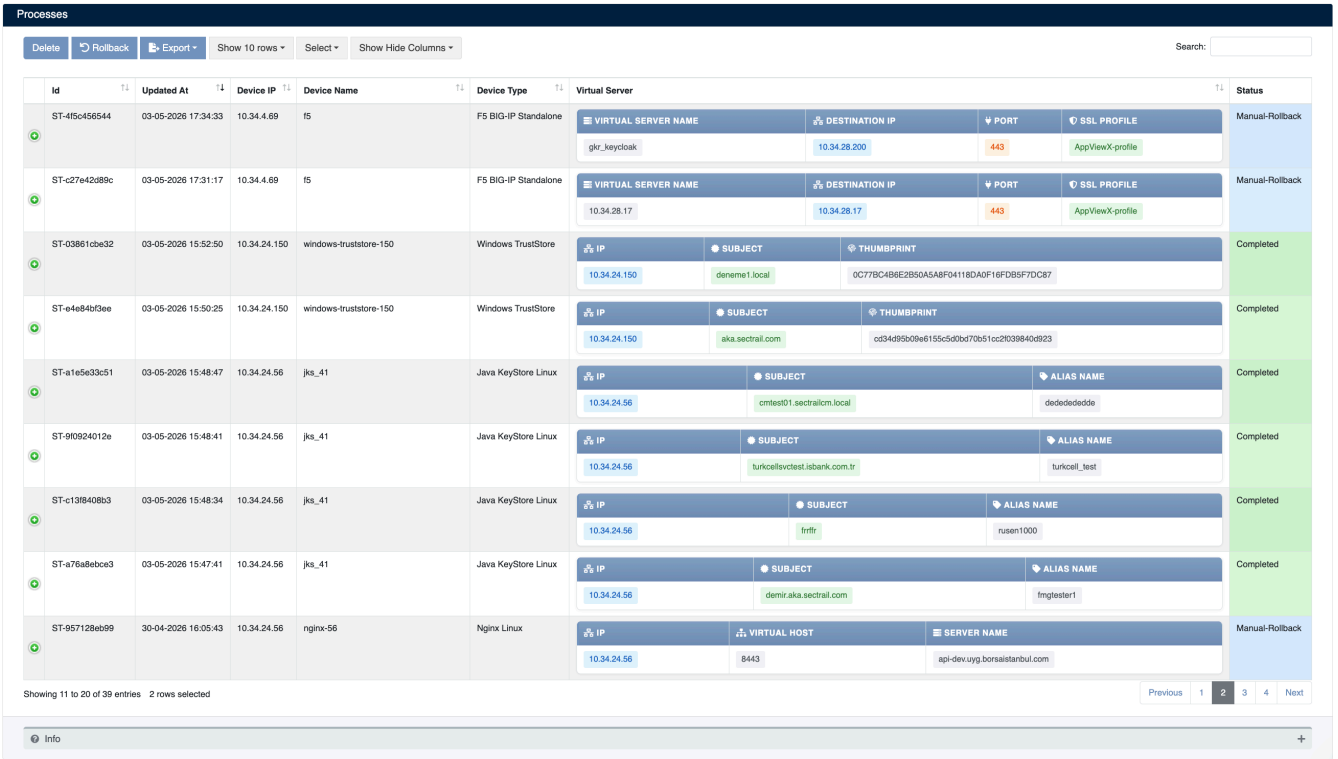
You can add a new device configuration by clicking the **Create** button.



New Device Configuration Form

Process

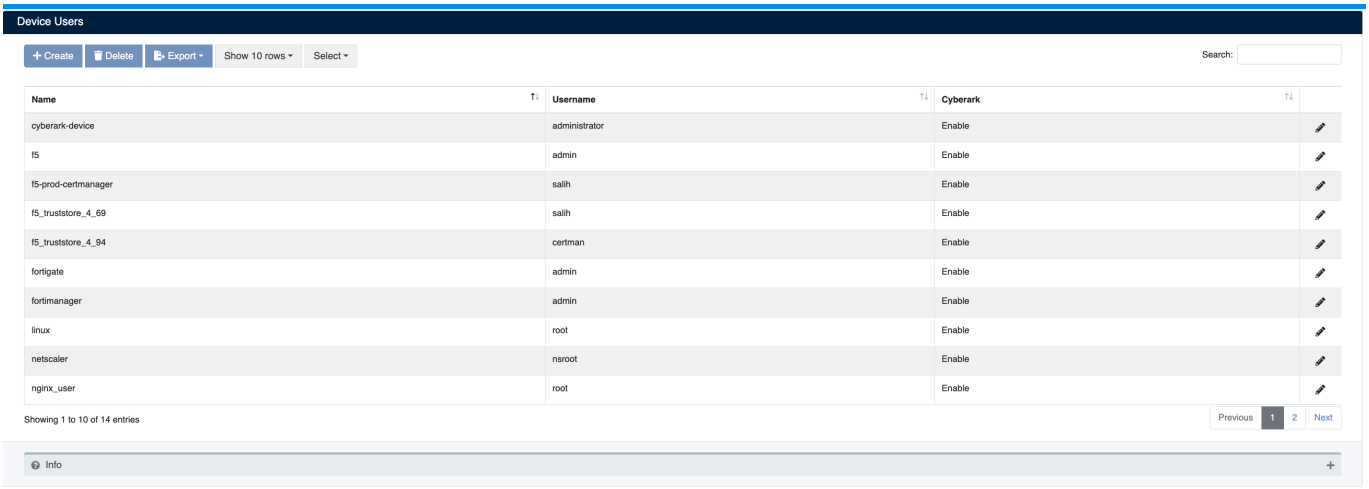
From the **Automation -> Process** section, all operations performed on devices (certificate deployment, etc.) can be viewed in detail.



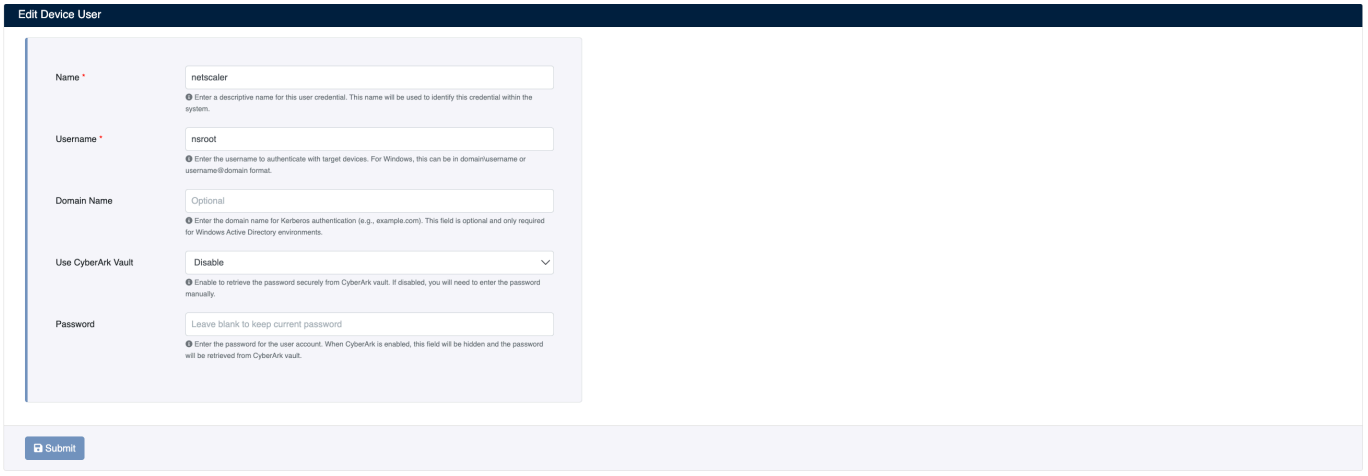
Process History - All Device Operations

Device Users

From the **Automation -> Device Users** section, you can create user definitions to be used in device connections.



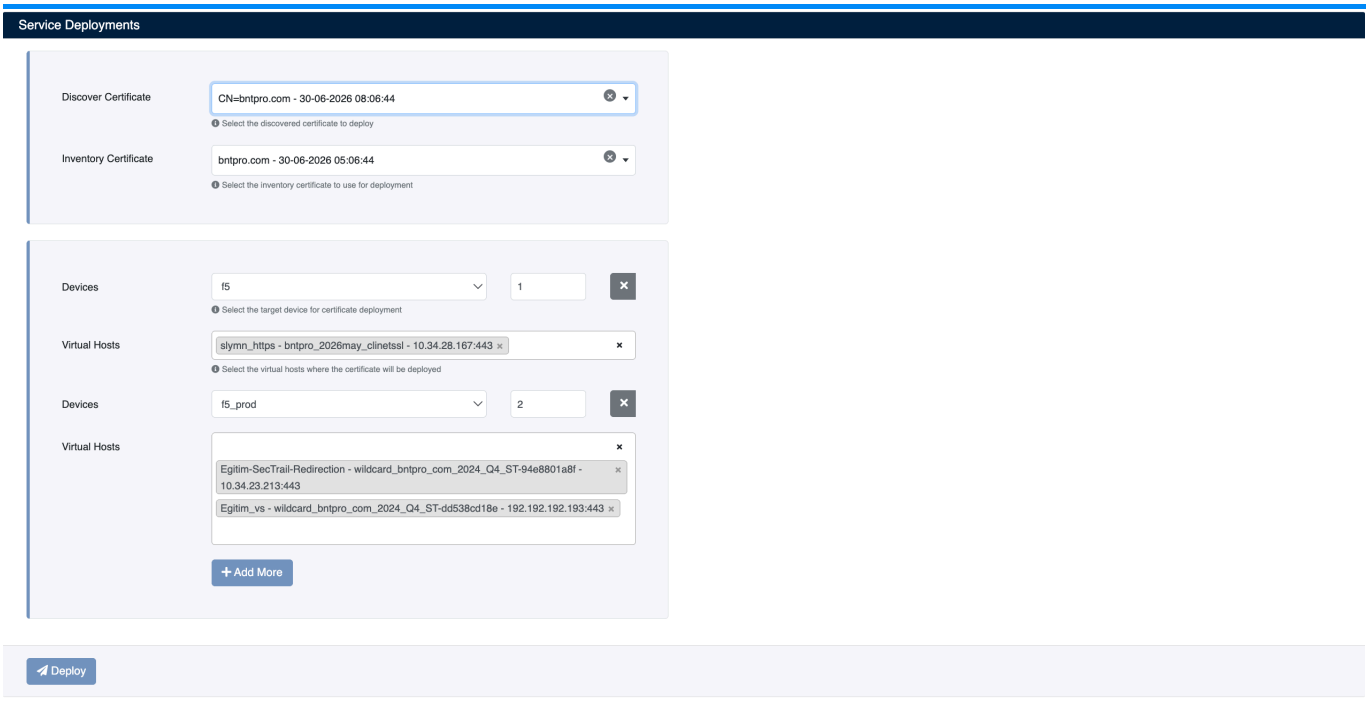
Device Users List



Create New Device User

Service Deployment

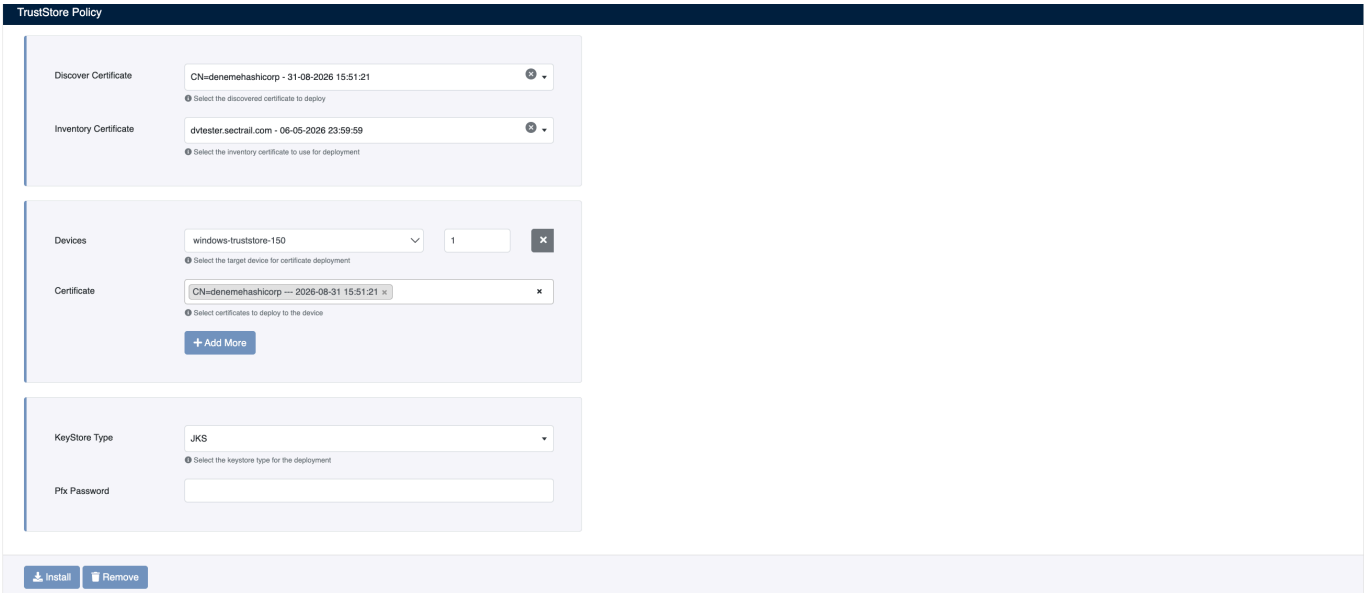
From the **Automation -> Deployments -> Service Deployments** page, you can initiate an instant certificate deployment to selected devices.



Instant Service Certificate Deployment

TrustStore Deployment

From the **Automation -> Deployments -> TrustStore Deployments** page, you can initiate an instant TrustStore deployment to selected devices.



Instant TrustStore Deployment

Workflow Management

This guide explains step by step how to configure certificate lifecycle automation rules, create and manage workflows in SecTrail CM.

ABOUT THE FEATURE

Workflow management enables you to automate certificate renewal, deployment, and notification processes. With server-based automation rules, you can centrally manage certificate lifecycles.

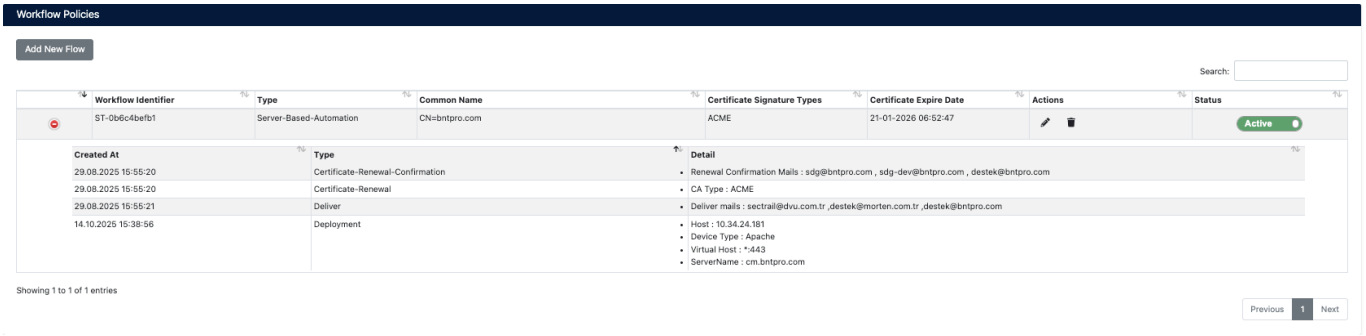
Automatic Operation Principle: Once configured, the system regularly monitors certificate expiration based on your renewal threshold value (e.g., 15 days). As expiration approaches, it automatically initiates the workflow steps you've defined (approval, renewal, deployment) and performs certificate renewal and installation when the time comes.

Workflow Policies List

View and manage all created workflow policies.

ACCESS PATH

To access workflow policies: Go to **Workflow -> Policy** menu.



Workflow Policies - All Automation Rules

List Information

The following details are displayed for each policy in the workflow list:

Column	Description
Workflow Identifier	Automatically generated unique identifier for the workflow (e.g., ST-0b6c4befb1)
Created At	Policy creation date and time
Type	Workflow type (Certificate-Renewal-Confirmation, Certificate-Renewal, Deliver, Deployment)
Common Name	Common name information of the certificate to which the workflow applies
Certificate Signature Types	Certificate signature type (ACME, RSA, ECDSA)
Certificate Expire Date	Expiration date of the associated certificate
Actions	Action buttons for editing and deleting
Status	Workflow status: `Active` or `Inactive`

Workflow Details

Each workflow record can be expanded to view detailed information:

Detail Fields

- **Renewal Confirmation Mails:** Email addresses for renewal approval notifications
- **CA Type:** Certificate authority type used (ACME, Internal CA)
- **Deliver mails:** Email addresses to receive certificate delivery notifications
- **Host:** Server IP address for deployment
- **Device Type:** Target device type (Apache, Nginx, F5, etc.)
- **Virtual Host:** Virtual host configuration
- **ServerName:** Server name information

Available Actions

Top Menu Actions

- **Add New Flow** - Create new workflow policy
- **Search** - Search workflows by identifier number
- **Edit** - Edit existing policy (pencil icon)
- **Delete** - Delete policy (trash icon)
- **Expand/Collapse** - Show/hide detail information

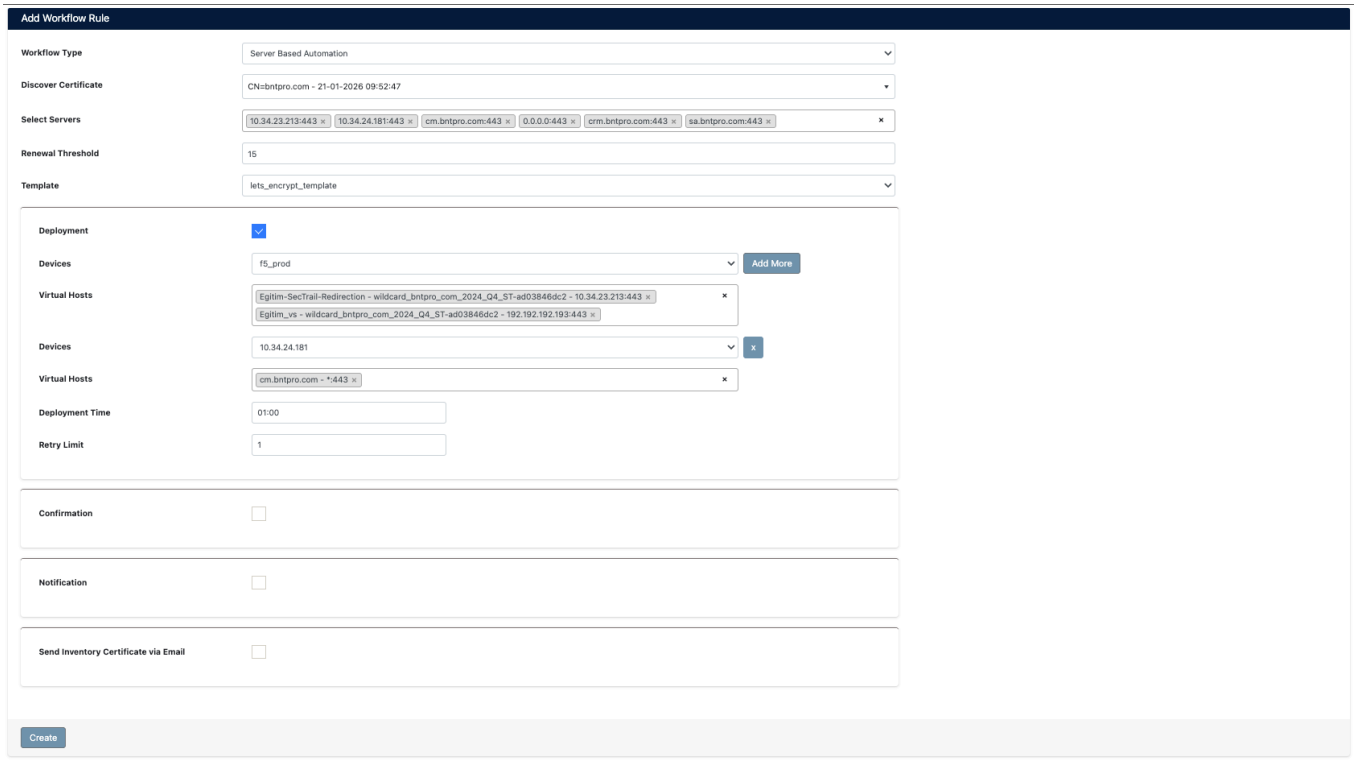
> **CAUTION**
>
> Deleting an active workflow will stop automatic certificate renewal and deployment processes. Make sure before deleting.

Creating New Workflow

Create certificate lifecycle automation rules.

ACCESS PATH

To create a new workflow: Click the **Add New Flow** button on the **Workflow -> Policy** page.



Creating New Workflow Rule

Basic Configuration

1. Workflow Type and Certificate Selection

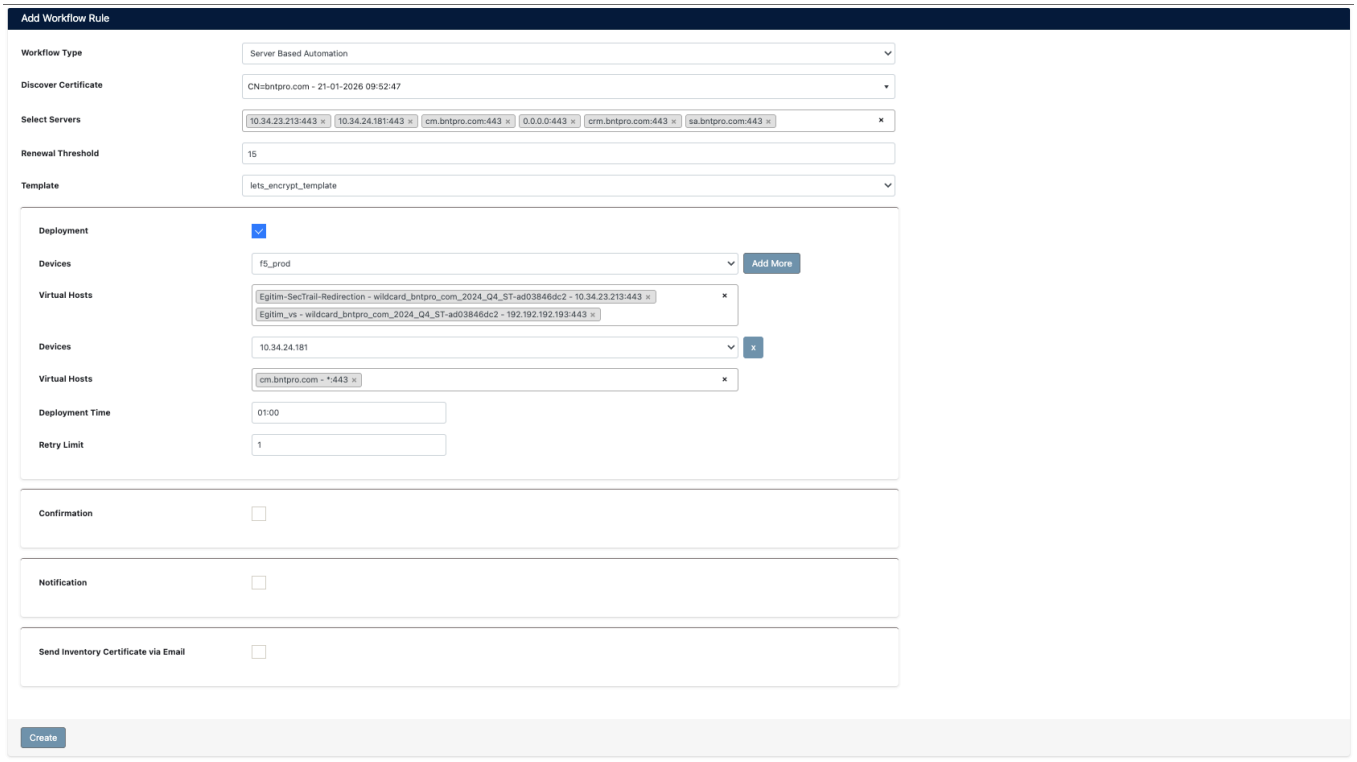
Parameter	Description	Options
Workflow Type	Specify the automation rule type	`Server Based Automation`
Discover Certificate	Select the discovered certificate to which the workflow applies	Certificate selection from discovery list
Select Servers	Specify the servers where automation will run	IP address or hostname selection (supports multiple selection)
Renewal Threshold	Certificate renewal threshold value (days)	How many days before certificate expiration to renew (default: 15)
Template	Certificate template to use	Selection from predefined templates

Steps

1. Select `Server Based Automation` as **Workflow Type**
2. Select the relevant certificate from the **Discover Certificate** dropdown
3. Select target servers in the **Select Servers** field (multiple servers can be selected)
4. Enter the number of days for **Renewal Threshold** (e.g., 15)

5. Select the appropriate template from the **Template** dropdown

2. Deployment Configuration



Deployment Settings

Configure certificate deployment parameters.

Parameter	Description
Deployment	Enable automatic deployment (checkbox)
Devices	Select target device type (F5, Apache, Nginx, etc.)
Virtual Hosts	Select virtual host configurations for deployment
Devices (Secondary)	IP address for secondary devices
Virtual Hosts (Secondary)	Secondary virtual host configurations
Deployment Time	Time when deployment will occur (in HH:MM format)
Retry Limit	Number of retries for failed deployment

Configuration Steps

1. Check the **Deployment** checkbox
2. Select the device type from the **Devices** dropdown
3. Select relevant configurations for **Virtual Hosts**
4. Enter IP address for secondary devices
5. Enter time information in the **Deployment Time** field (e.g., 01:00)
6. Specify the number of retries for **Retry Limit** (e.g., 1)

3. Confirmation Configuration

Approval Notifications Settings

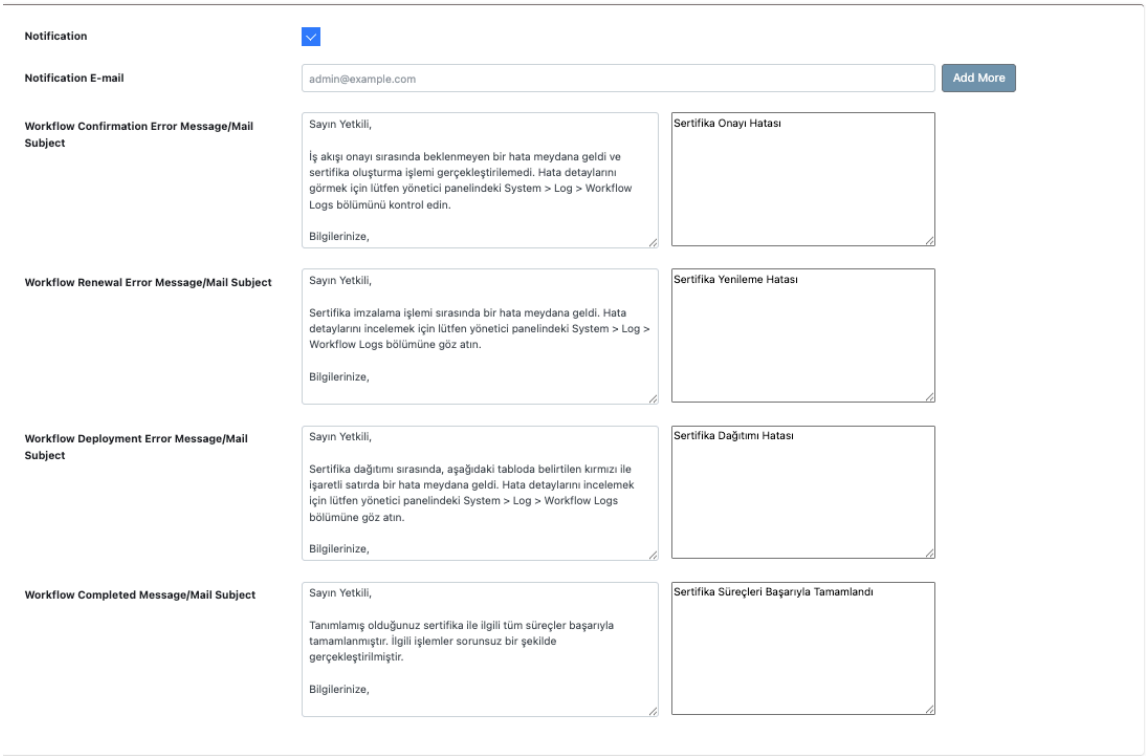
Configure approval processes for certificate renewal and deployment.

Parameter	Description
Confirmation	Enable confirmation mechanism
Renewal Confirmation Emails	Email addresses for renewal approval (comma-separated)
Renewal Confirmation Emails Content	Content of renewal approval email
Deployment Confirmation Emails	Email addresses for deployment approval
Deployment Confirmation Emails Content	Content of deployment approval email

Configuration Steps

1. Check the **Confirmation** checkbox
2. Enter email addresses in the **Renewal Confirmation Emails** field
3. Write the email text in the relevant content field
4. Repeat the same steps for **Deployment Confirmation Emails**
5. Add additional email addresses with the **Add More** button

4. Notification Configuration

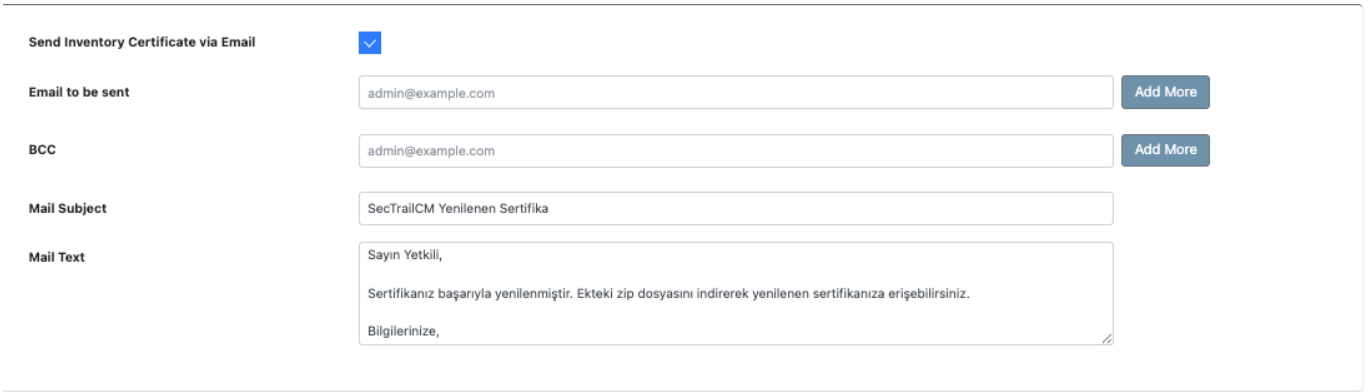


Notification Settings

Configure notification parameters for workflow processes.

Parameter	Description
Notification	Enable notification mechanism
Notification E-mail	Email addresses to receive notifications
Workflow Confirmation Error Message/Mail Subject	Confirmation error email subject and content
Workflow Renewal Error Message/Mail Subject	Renewal error email subject and content
Workflow Deployment Error Message/Mail Subject	Deployment error email subject and content
Workflow Completed Message/Mail Subject	Successful completion email subject and content

5. Send Certificate via Email



Send Certificate via Email

Automatically send renewed certificates via email.

Parameter	Description
Send Inventory Certificate via Email	Enable email sending feature
Email to be sent	Email addresses to receive the certificate
BCC	Email addresses to receive blind copy
Mail Subject	Email subject line
Mail Text	Email content text

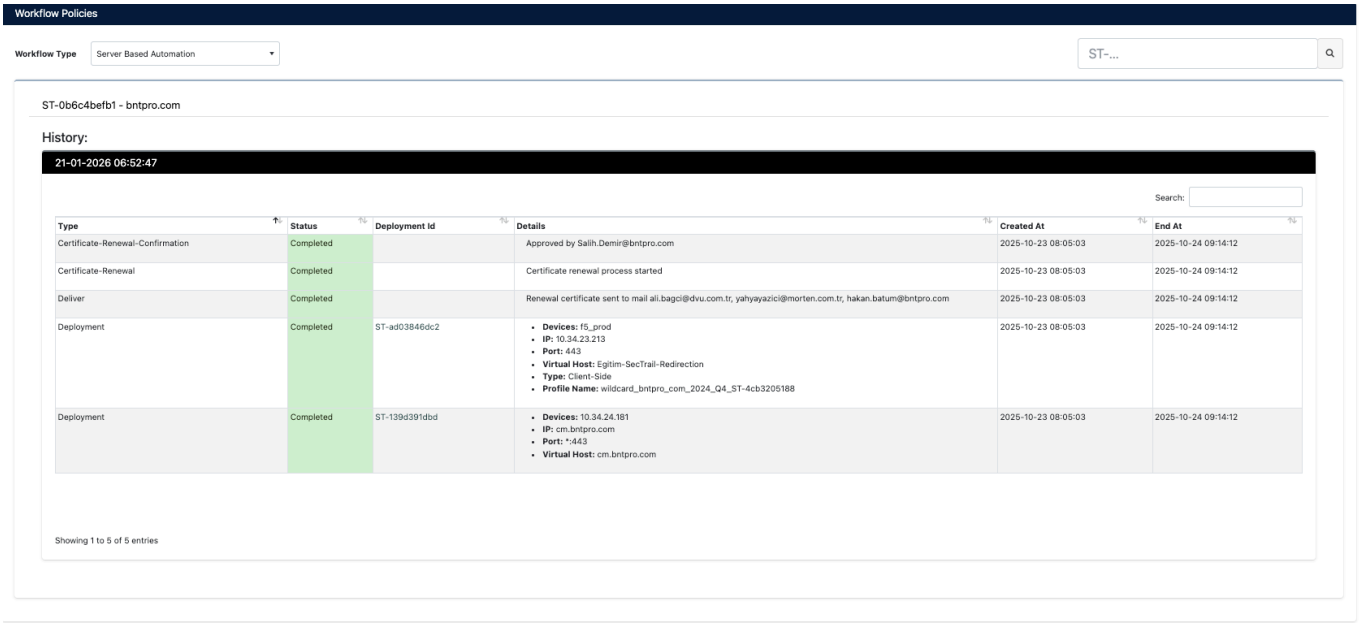
Configuration Steps

1. Check the **Send Inventory Certificate via Email** checkbox
2. Enter recipient email addresses in the **Email to be sent** field
3. Add blind copy recipient addresses in the **BCC** field
4. Write an appropriate subject for **Mail Subject** (e.g., "SecTrailCM Renewed Certificate")
5. Enter the email content in the **Mail Text** field
6. Click the **Create** button to save the workflow

Workflow History

View the execution history and details of created workflows.

> **ACCESS PATH**
>
> To access workflow history: Click on a workflow identifier in the **Workflow -> Processes** list.



Workflow History - Process Steps

History Information

The following information is displayed for each workflow execution:

Column	Description
Type	Operation type (Certificate-Renewal-Confirmation, Certificate-Renewal, Deliver, Deployment)
Status	Operation status (`Completed` , `Failed` , `Pending`)
Deployment Id	Deployment identification number
Details	Operation details and descriptions
Created At	Operation start date and time
End At	Operation completion date and time

Status Indicators

Status	Description
Completed	Operation completed successfully
Failed	Operation failed
Pending	Operation in progress

Deployment Details

When deployment records are expanded, the following details are displayed:

- **Devices:** Target device list (e.g., f5_prod)
- **IP:** Target server IP address
- **Port:** Target port number
- **Virtual Host:** Related virtual host configuration
- **Type:** Deployment type (Client-Side, Server-Side)
- **Profile Name:** Profile name used

Sample Deployment Record

```
- Devices: f5_prod
- IP: 10.34.23.213
- Port: 443
- Virtual Host: Eğitim-SecTrail-Redirection
- Type: Client-Side
- Profile Name: wildcard_bntpro_com_2024_Q4_ST-4cb3205188
```

Search and Filtering

- **Search:** Search by workflow identifier
- **Date Filter:** Filter history records by date range
- **Status Filter:** Filter records by status

PAGINATION

At the bottom of the list, you can navigate through "Showing 1 to 5 of 5 entries" information and page numbers.

Workflow Scenario Example

Below is a step-by-step workflow configuration with a real-world use case scenario.

Scenario: Automatic Wildcard Certificate Renewal and Deployment

Situation: Your company uses a wildcard certificate for `*.bntpro.com`. This certificate is used on multiple servers (Apache, F5 load balancer).

Requirement: The certificate should be automatically renewed before expiration and deployed to all servers.

Step 1: Certificate Discovery

1. Create a certificate discovery rule from the **Discovery -> Discovery List** menu
2. Add target servers (`10.34.23.213` , `10.34.24.181` , `cm.bntpro.com:443`)
3. Start discovery and wait for certificates to be detected

Step 2: Workflow Creation

1. Click the **Add New Flow** button from the **Workflow -> Workflow Policies** page
2. **Workflow Type:** Select `Server Based Automation`
3. **Discover Certificate:** Select `CN=bntpro.com - 21-01-2026 09:52:47`
4. **Select Servers:** Select all servers

- `10.34.23.213:443`
- `10.34.24.181:443`
- `cm.bntpro.com:443`
- `0.0.0.0:443`
- `crm.bntpro.com:443`
- `sa.bntpro.com:443`

5. **Renewal Threshold:** Set to `15` days
6. **Template:** Select `lets_encrypt_template`

Step 3: Deployment Configuration

1. Check the **Deployment** checkbox
2. **Devices (Primary):** Select `f5_prod`
3. **Virtual Hosts (Primary):**

- `Eğitim-SecTrail-Redirection - wildcard_bntpro_com_2024_Q4_ST-ad038846dc2 - 10.34.23.213:443`
- `Eğitim_ss - wildcard_bntpro_com_2024_Q4_ST-ad038846dc2 - 192.192.192.193:443`

4. **Devices (Secondary):** `10.34.24.181`

5. **Virtual Hosts (Secondary):** `cm.bntpro.com -*443`
6. **Deployment Time:** `01:00` (1:00 AM)
7. **Retry Limit:** `1`

Step 4: Confirmation Mechanism

1. Check the **Confirmation** checkbox
2. **Renewal Confirmation Emails:** `admin@example.com, sdg-dev@bntpro.com, destek@bntpro.com`
3. **Deployment Confirmation Emails:** `admin@example.com`

Step 5: Notification Configuration

1. Check the **Notification** checkbox
2. **Notification E-mail:** `admin@example.com`
3. **Workflow Confirmation Error Message**
4. **Workflow Renewal Error Message**
5. **Workflow Deployment Error Message**
6. **Workflow Completed Message**

Step 6: Email Delivery

1. Check the **Send Inventory Certificate via Email** checkbox
2. **Email to be sent:** `admin@example.com, sdg-dev@bntpro.com, destek@bntpro.com`
3. **BCC:** `admin@example.com`
4. **Mail Subject:** `SecTrailCM Renewed Certificate`

Step 7: Save and Activation

1. Click the **Create** button to save the workflow
2. The workflow automatically becomes `Active`
3. The system automatically starts the renewal process 15 days before certificate expiration

Workflow Execution Sequence

The created workflow runs in the following sequence:

1. **Day 0-15:** System checks certificate expiration
2. **Day 15 (Renewal Start):**

- Renewal approval email is sent
- Waits for approval

3. **After Approval:**

- Certificate renewal process begins (ACME/Let's Encrypt)
- New certificate is created

4. **Deployment Approval:**

- Deployment approval email is sent

- Waits for approval

5. **At 01:00 (Deployment):**

- Deployment to F5 load balancer
- Deployment to Apache server
- Retry for each deployment (if failed)

6. **Completion:**

- If all operations succeed, notification email is sent
- New certificate is shared via email

7. **Error State:**

- If an error occurs in any step, relevant error notification is sent
- Detailed log record is created in Workflow Logs

> **BEST PRACTICES**
>
> - **Deployment Time:** Set deployment time to low-traffic hours (1:00 AM-4:00 AM)
> - **Retry Limit:** Increase retry limit for critical systems
> - **Notification:** Add multiple administrator emails
> - **BCC:** Use BCC for archiving in all email notifications
> - **Testing:** Test with a test certificate during initial setup

Pending Approvals

When the confirmation mechanism is enabled, user approval is required before renewal or deployment steps begin. You can view and manage workflows awaiting approval from this screen.

> **NAVIGATION**
>
> To access pending approvals: Go to **Workflow -> Approval** menu.

Pending Workflow Approvals List

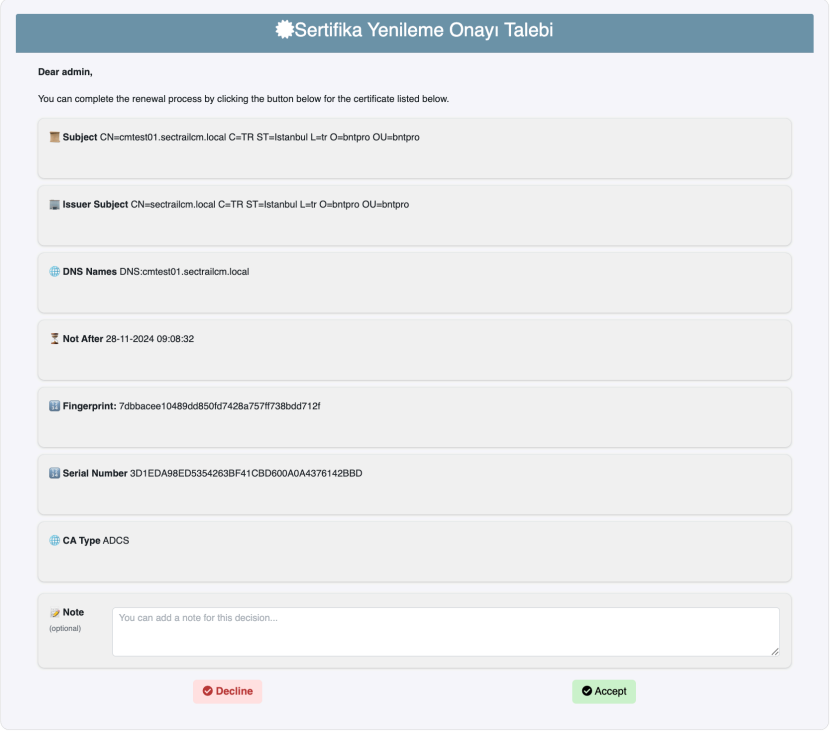
List Information

The following information is displayed for each record in the approval list:

Column	Description
Workflow Identifier	Unique identifier of the workflow
Type	Approval type (Certificate-Renewal-Confirmation, Deployment-Confirmation)
Common Name	Common name of the related certificate
Created At	Date and time the approval request was created
Actions	Approve or reject actions

Approval Process

To approve a pending workflow, click the **Approve** button on the relevant record. Once approved, the workflow continues from where it left off.



Approval Detail Screen

> **NOTICE**
>
> If you reject an approval request, the related workflow step will be cancelled and the process will be stopped.

Ownership Management

SecTrail Certificate Manager provides the ability to automatically assign ownership to certificates based on server or certificate attributes. This ensures alarms and notifications are directed to the right teams and individuals.

Overview

With the ownership management system, you can:

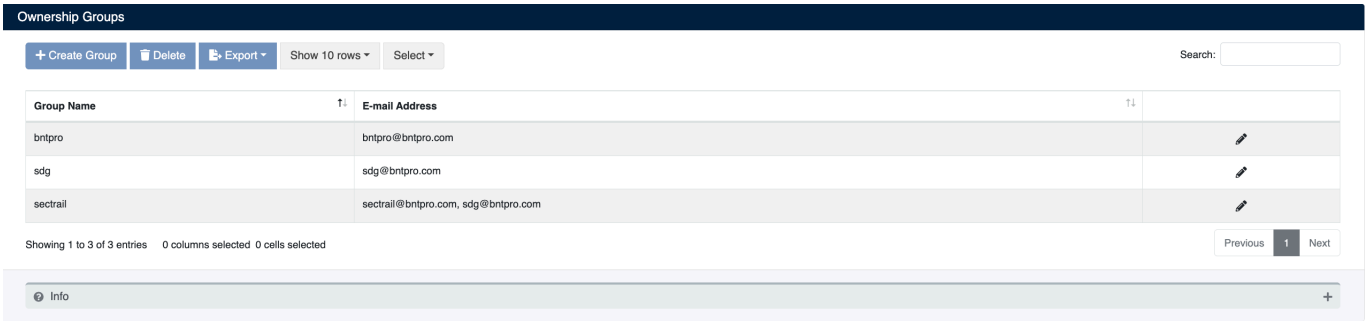
- Assign ownership based on server IP addresses or certificate attributes
- Automatically update discovery lists with ownership information
- Direct alarms to relevant teams
- Integrate with external inventory systems via API
- Define ownership rules using regex patterns

Ownership Components

Ownership Groups

Ownership Groups define the teams or individuals responsible for certificates. Each group consists of:

- **Group Name**: A unique identifier for the group
- **Email Addresses**: One or more email addresses to receive notifications

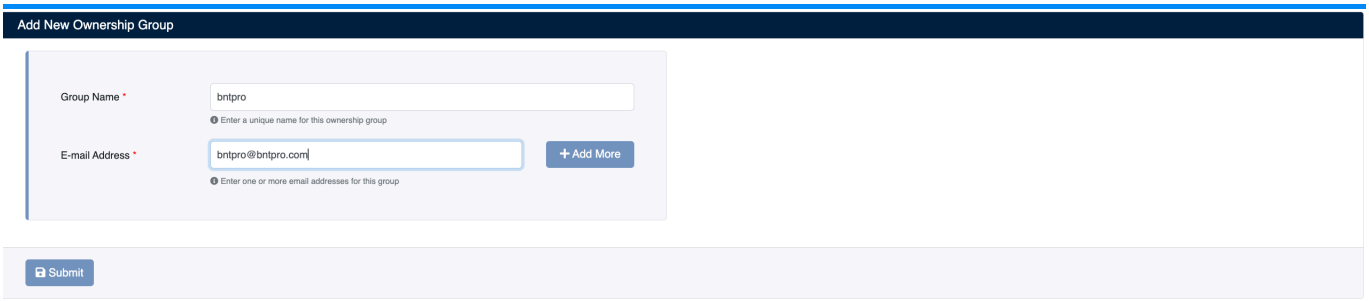


Creating an Ownership Group

1. Go to the **Ownership Groups** section
2. Click the **Create Group** button
3. Enter the following information:

- **Group Name**: A descriptive name for the team or group
- **E-mail Address**: Add one or more email addresses using the "Add More" button

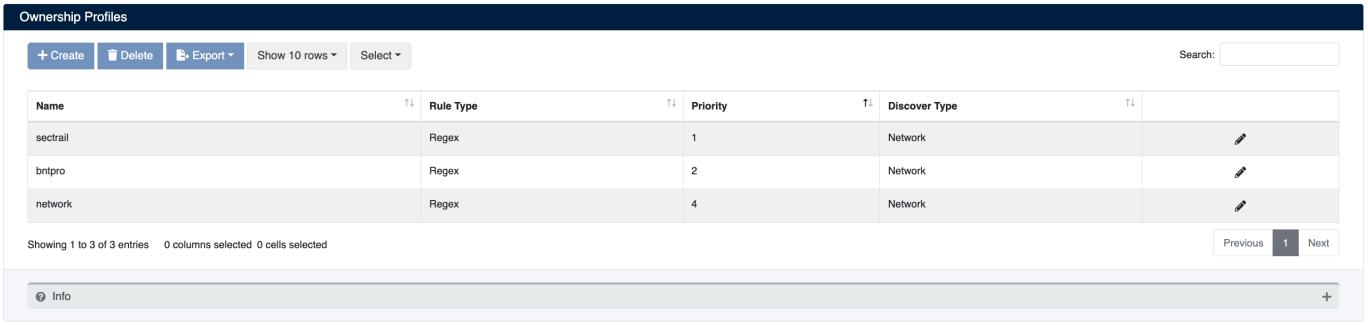
4. Click the **Submit** button to create the group



Ownership Profiles

Ownership Profiles define rules that determine which certificates or servers belong to which ownership group. You can create profiles based on the following criteria:

- Network-based discovery (IP addresses)
- Certificate attributes (subject, issuer, SAN, etc.)



Creating an Ownership Profile

1. Go to the **Ownership Profiles** section
2. Click the **Create** button
3. Configure the following fields:

Basic Information:

- **Name**: A descriptive name for the profile
- **Discover Type**: Select either Network or DataPower
- **Rule Type**: Select the matching method (Regex, Service)
- **Type**: Select the attribute to match (Subject, IP Address)
- **Condition**: Select the matching condition (contains, equals)
- **Regex**: Enter the regex pattern to match. You can add multiple patterns with "Add More"
- Example for certificates: `CN=example.com.tr,OU=Security...`
- Example for IP addresses: `192.168.1..*`

Group Assignment:

- **Ownership Groups**: Select the ownership group to assign when the rule matches

Use Certificate Email:

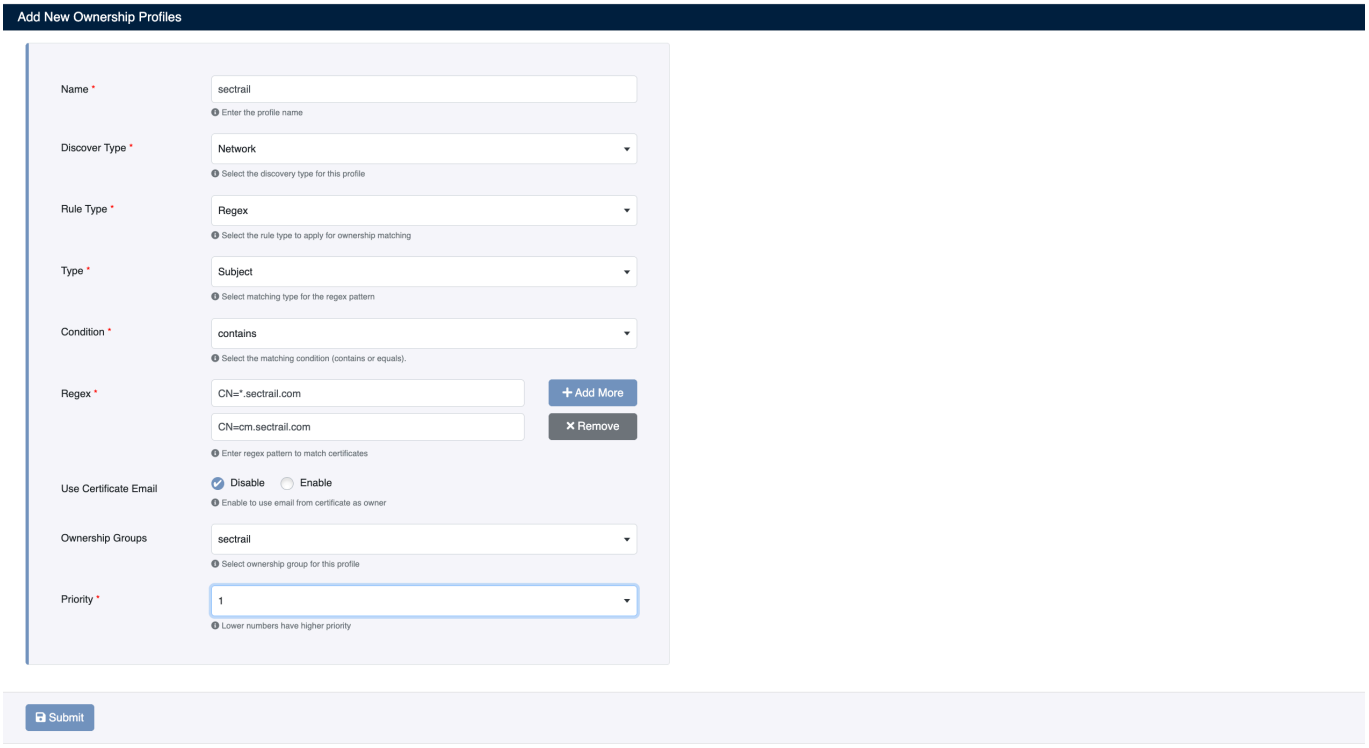
- **Utilize the email address found in the certificate**:
- Enable: Use email addresses found in the certificate

- Disable: Use only ownership group emails

Priority:

- Specify the priority level for this rule (1 = highest priority)
- When multiple rules match, the rule with the highest priority is applied

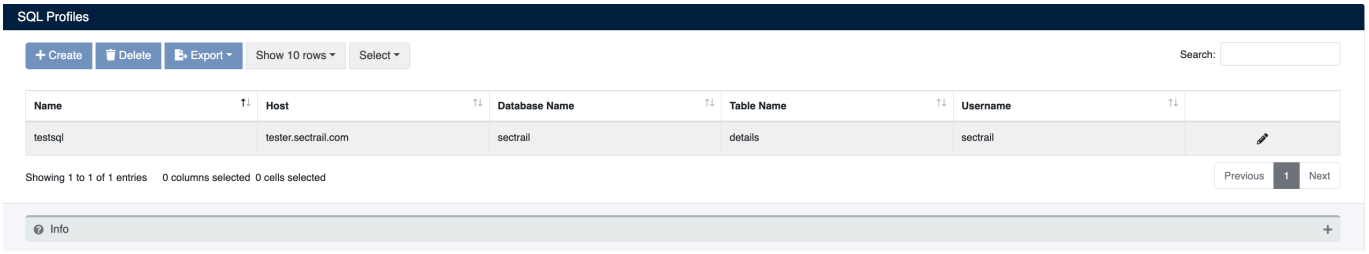
4. Click the **Submit** button to create the profile



Ownership Service Profiles

If your organization has its own inventory system and stores ownership information in that system, you can integrate SecTrail CM with your own API. With this integration:

- SecTrail CM calls the API you provide to automatically query ownership information for discovered certificates
- Your technical team prepares an API endpoint in your own inventory system
- Ownership information is synchronized with SecTrail CM via the API
- No manual ownership assignment is required



Creating an Ownership Service Profile

1. Go to the **Ownership Service Profiles** section
2. Click the **Create** button
3. Enter the following integration information:

- **Name**: A descriptive name for the service profile (e.g., "CMDB API", "Inventory System")
- **URL**: Your inventory system's API endpoint address (e.g., `https://cmdb.yourcompany.com/api/ownership`)
- **Username**: API authentication username (credential information)
- **Password**: API authentication password (credential information)

4. Click the **Submit** button to create the service profile

> **FOR API INTEGRATION**
>
> You need to contact your technical team to prepare an API endpoint in your own inventory system that SecTrail CM can query. The API should receive certificate information and return the relevant ownership group.

Discovery Settings

To reflect ownership information onto certificates in the inventory, discovery scheduling must be configured from the **Ownership -> Discovery Settings** section. This way, SecTrail CM automatically matches ownership profiles with certificates at the defined interval and keeps the inventory up to date.

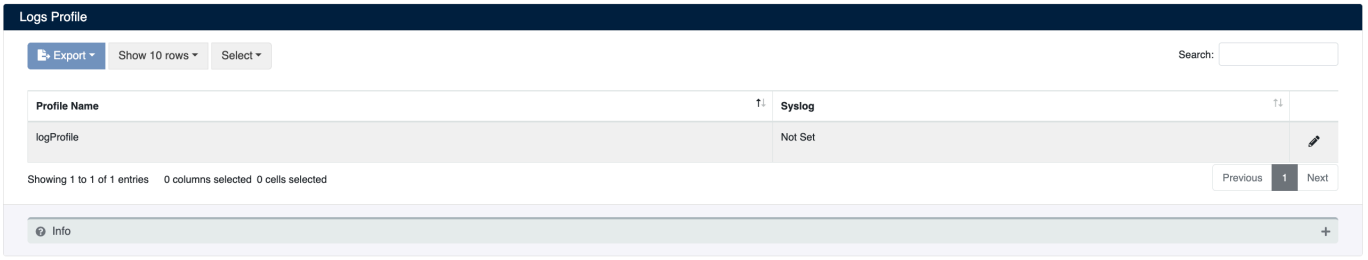
- **Type**: Specifies the discovery type (e.g., `Network`)
- **Working Period**: The period during which ownership matching will run (e.g., `Every week on Friday at 12:00`)

System Logs

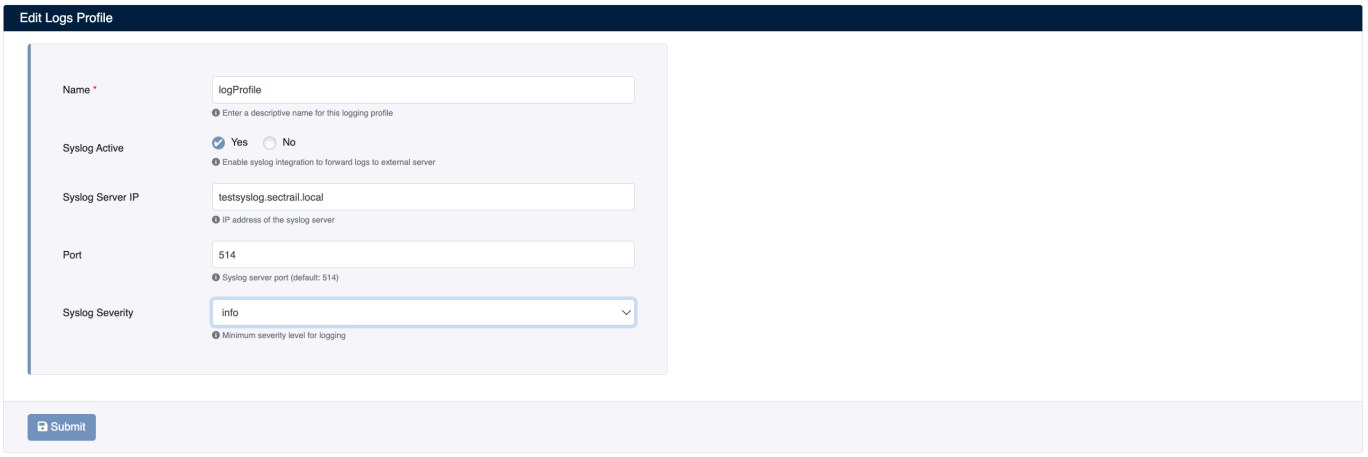
SecTrail CM records all operations performed on the system under different log categories. These logs can be monitored within the system or forwarded to an external Syslog server.

Syslog Configuration

To forward logs to an external Syslog server, edit the existing profile under **System > Log > Logging Profiles**.



Click the pencil icon on the profile and fill in the following fields:

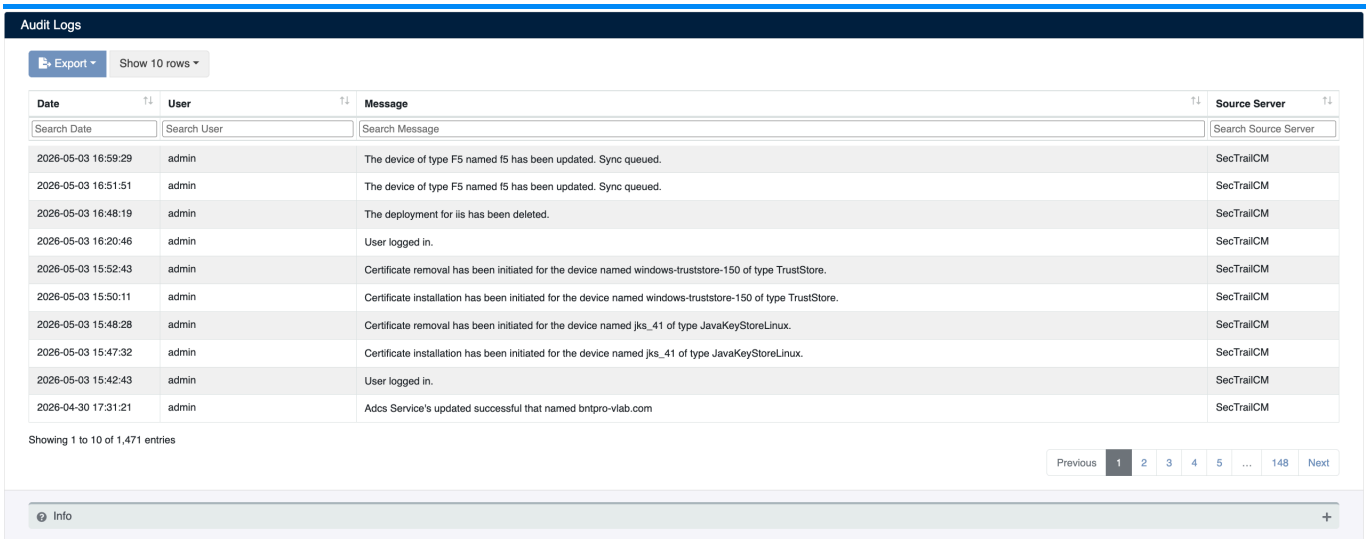


- **Name**: A descriptive name for the log profile
- **Syslog Active**: Select `Yes` to enable Syslog forwarding
- **Syslog Server IP**: IP address or hostname of the Syslog server
- **Port**: Port of the Syslog server (default: `514`)
- **Syslog Severity**: Minimum log severity level to forward (e.g. `info`, `warning`, `error`)

Log Categories

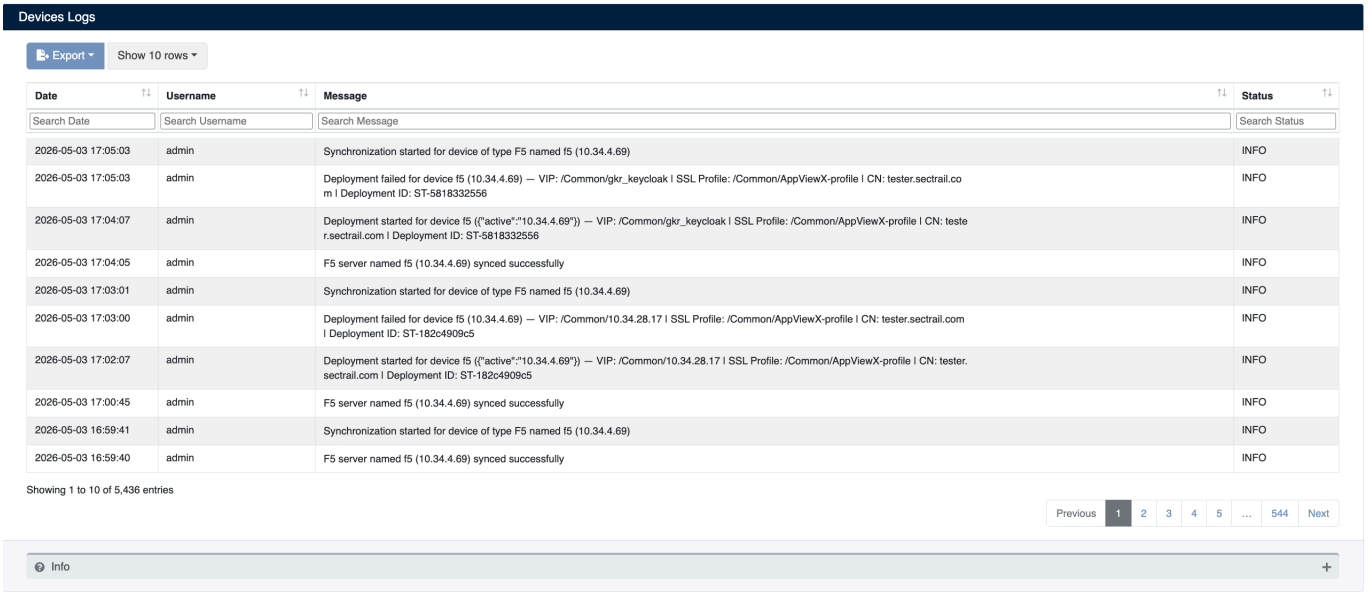
Audit Logs

Records user actions and system events. Used to track who performed which operation and when.



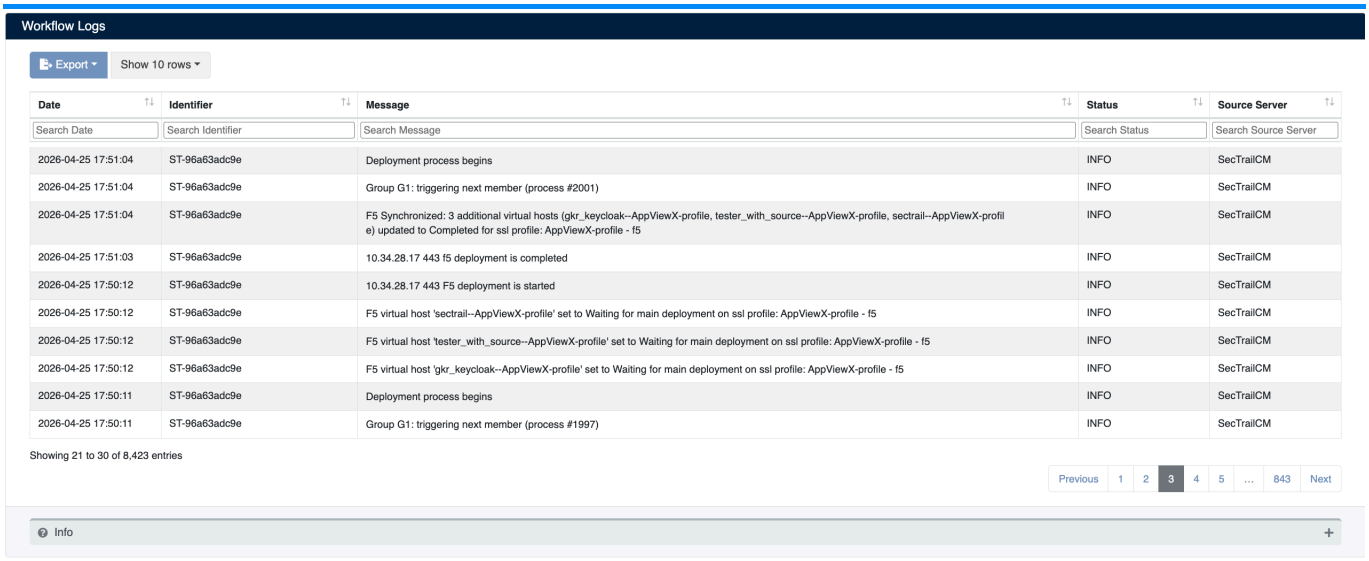
Device Logs

Contains detailed logs of certificate deployment and synchronization operations performed on devices.



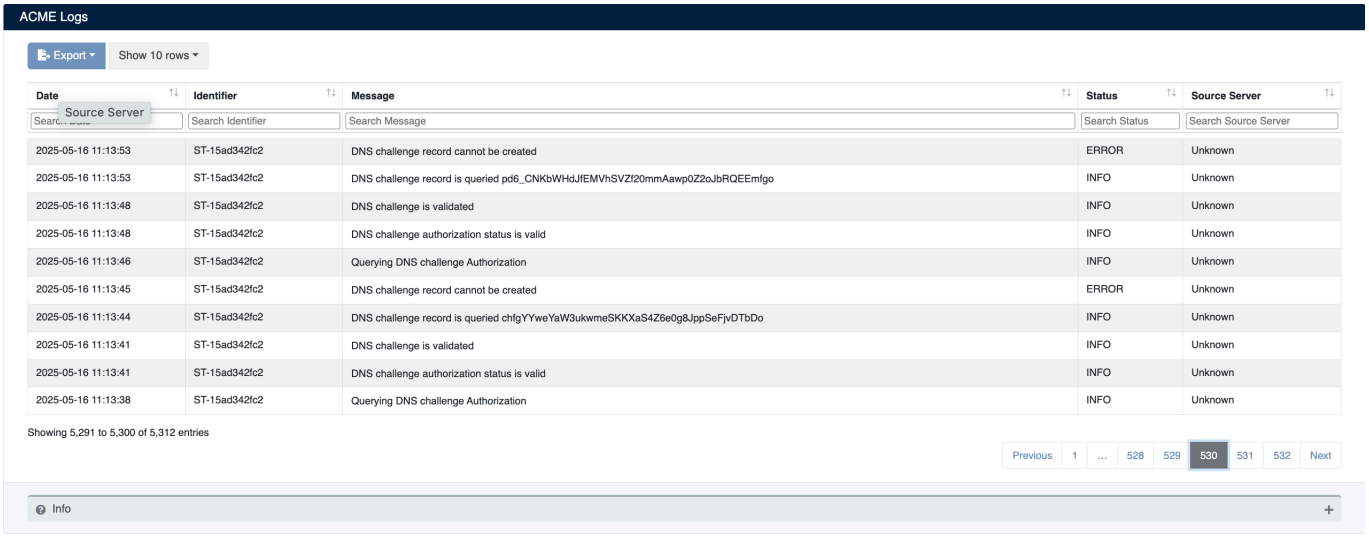
Workflow Logs

Contains step-by-step logs of deployment processes triggered within automation workflows.



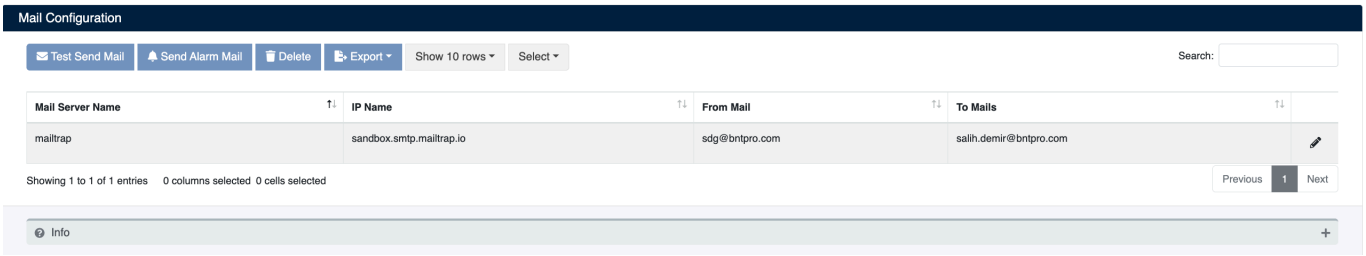
ACME Logs

Contains logs of DNS challenge and certificate renewal operations performed via the ACME protocol.



Mail Configuration

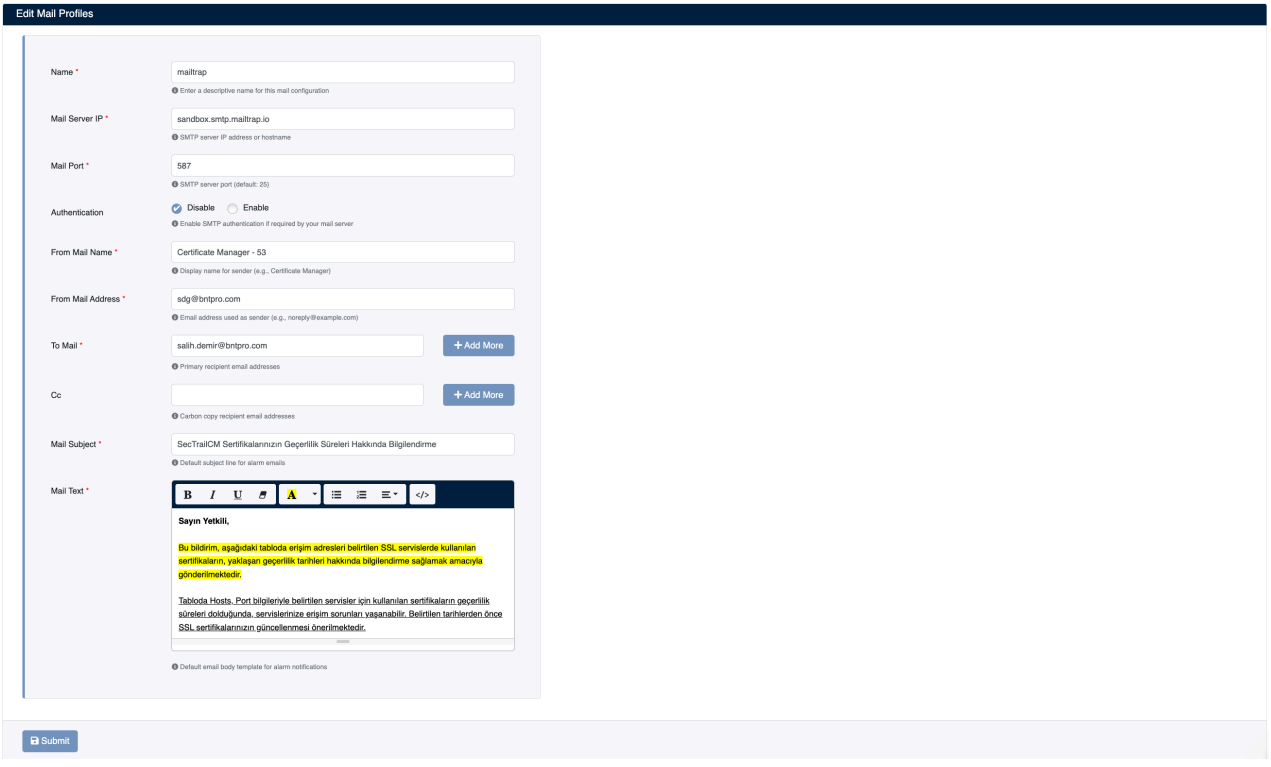
SecTrail CM provides SMTP-based mail configuration to deliver certificate alarms and notifications via email. Defined profiles can be viewed and edited under **System > Mail Configuration**.



The list displays **Mail Server Name**, **IP Name**, **From Mail**, and **To Mails** columns. The **Test Send Mail** button can be used to verify the configuration, and the **Send Alarm Mail** button sends an alarm mail immediately.

Editing Mail Profile

Click the pencil icon on the profile and fill in the following fields:

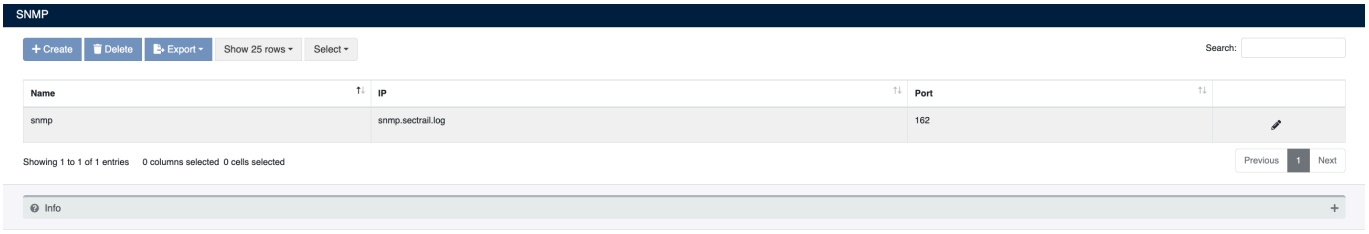


- **Name**: A descriptive name for the mail profile
- **Mail Server**: IP address or hostname of the SMTP server
- **Mail Port**: SMTP port (default: `25`)
- **Authentication**: Select `Enable` if SMTP authentication is required
- **From Mail Name**: Sender display name (e.g. `Certificate Manager - S5`)
- **From Mail Address**: Sender email address
- **To Mail**: Primary recipient address for notifications; click **+ Add More** to add multiple recipients

- **Cc**: Carbon copy email addresses; click **+ Add More** to add multiple addresses
- **Mail Subject**: Subject line for alarm emails
- **Mail Text**: Default body template for alarm emails (editable via rich text editor)

SNMP Configuration

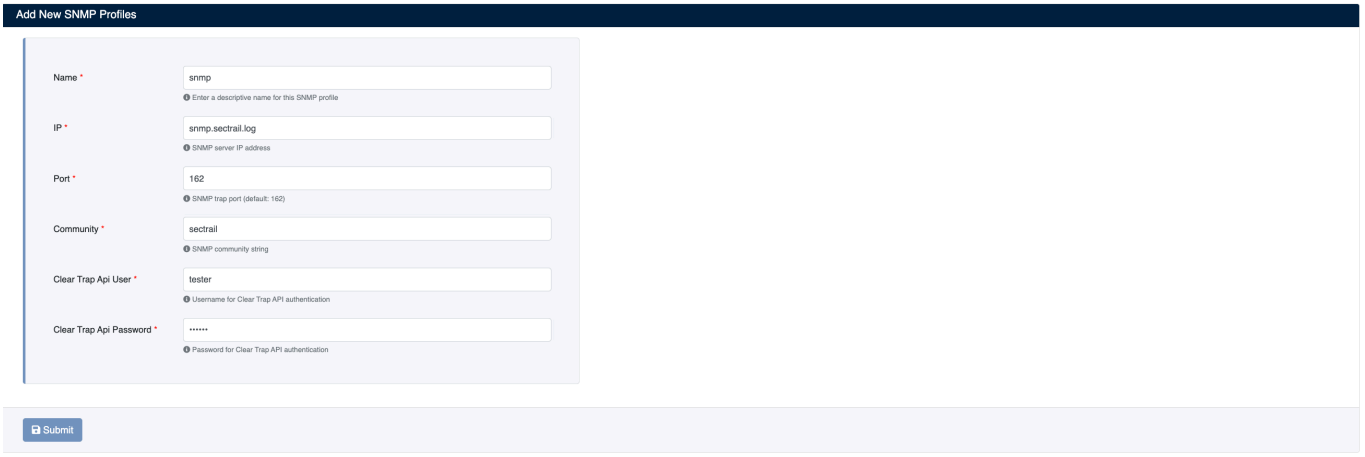
SecTrail CM can forward certificate alarms as SNMP traps to an external SNMP server. SNMP profiles can be created and managed under **System > SNMP**.



The list displays the **Name**, **IP**, and **Port** information of defined profiles.

Creating a New SNMP Profile

Click the **+ Create** button to add a new SNMP profile:



- **Name**: A descriptive name for the SNMP profile
- **IP**: IP address or hostname of the SNMP trap receiver
- **Port**: SNMP trap port (default: `162`)
- **Community**: SNMP community string (e.g. `sectrail`)
- **Clear Trap Api User**: Username for Clear Trap API authentication
- **Clear Trap Api Password**: Password for Clear Trap API authentication

> **INFO**
>
> Once a profile is created, when certificate alarms are triggered, the corresponding SNMP traps are automatically forwarded to the configured server.

User Management

SecTrail CM provides both local user management and enterprise identity management support with LDAP/Active Directory integration. This allows you to easily manage your users and integrate with your corporate directory services.

User Types

SecTrail CM supports two different types of users:

1. Local Users

Local users are users defined and managed in SecTrail CM's own database.

Features:

- Created and managed within SecTrail CM
- Defined with username, password, and email address
- Role-based authorization support
- Ability to create dedicated users for API access

2. LDAP/Active Directory Users

Provides centralized identity management by integrating with your corporate Active Directory or LDAP servers.

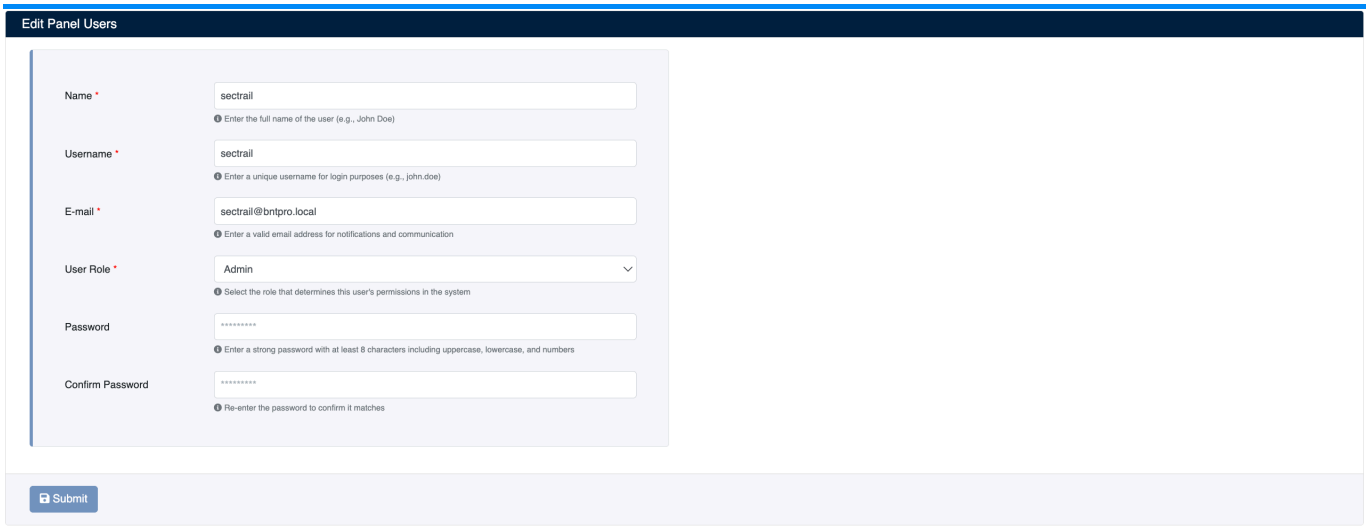
Features:

- Centralized user management
- Login with existing corporate credentials
- Group-based authorization
- User-based authorization

Local User Management

Creating a New User

1. Navigate to the **Local Users** tab from the **Users** menu
2. Click the **Create** button
3. Fill in the following information in the **Add New Panel Users** form:



Form Fields

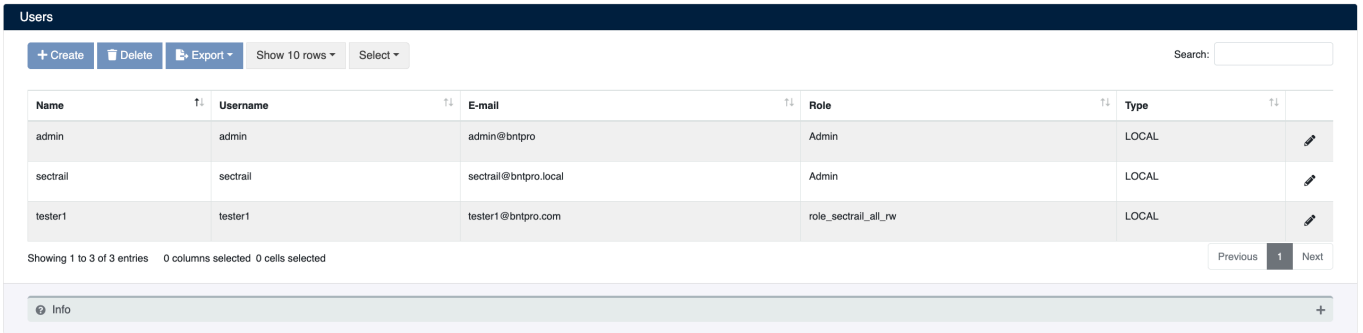
- **Name**: User's first and last name
- **Username**: Username to be used for system login (must be unique)
- **E-mail**: User's email address (valid format: `name@mail.com`)
- **User Role**: Role to be assigned to the user
- **Password**: User password
- **Confirm Password**: Password confirmation

1. Click the **Submit** button to create the user

> **TIP**
>
> Create users with dedicated API roles for API integrations. These users should only be used for API access.

User List

The **Users** screen displays all users in the system in table format.



On this screen:

Column Information:

- **Name**: User's full name
- **Username**: Username used for system login
- **E-mail**: User's email address
- **Role**: Role assigned to the user

User Operations

Action buttons are located on the right side of each user row:

- **Edit ()**: Edit user information
- **Delete ()**: Remove user from the system

> **WARNING**
>
> Be careful when deleting users with active sessions. User deletion is irreversible.

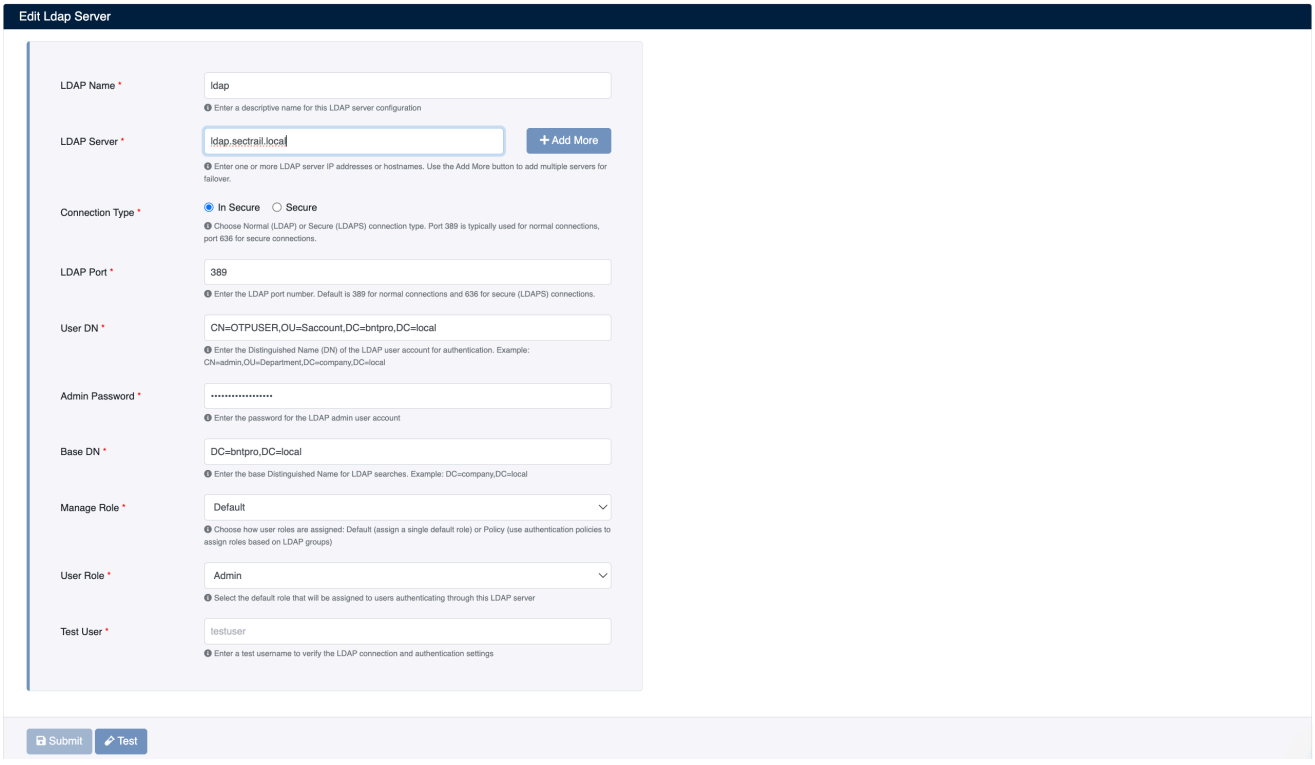
LDAP/Active Directory Integration

SecTrail CM provides enterprise identity management by integrating with your Active Directory or LDAP servers.

LDAP Server Configuration

Creating a New LDAP Profile

You can create a new LDAP/AD profile using the **Add New Ldap Server** form.



Form Fields

- **LDAP Name**: Unique name for the LDAP profile
- **LDAP Server**: IP address or hostname of the LDAP/AD server. Multiple servers can be added using the **Add More** button
- **Connection Type**: Connection type selection
- **In Secure**: Unencrypted connection (Port 389, for testing/development)
- **Secure**: SSL/TLS encrypted connection (Port 636, for production)
- **LDAP Port**: Connection port number (default: `389` or `636`)

- **User DN**: Administrator DN for LDAP connection
- **Admin Password**: Password for the administrator specified in User DN
- **Base DN**: Base DN where user searches will begin
- **Manage Role**: Default role for LDAP administrators
- **User Role**: Default role for LDAP users
- **Test User**: Username to test the connection

> **WARNING**
>
> Always test your LDAP connections. Incorrect configuration can prevent user logins and make system access impossible.

> **TIP**
>
> Before configuring your first LDAP setup, ensure you have a local admin account that can log into the system. This way, you can access the system in case of LDAP issues.

LDAP Profile Management

The **LDAP Profiles** table displays all defined LDAP servers.

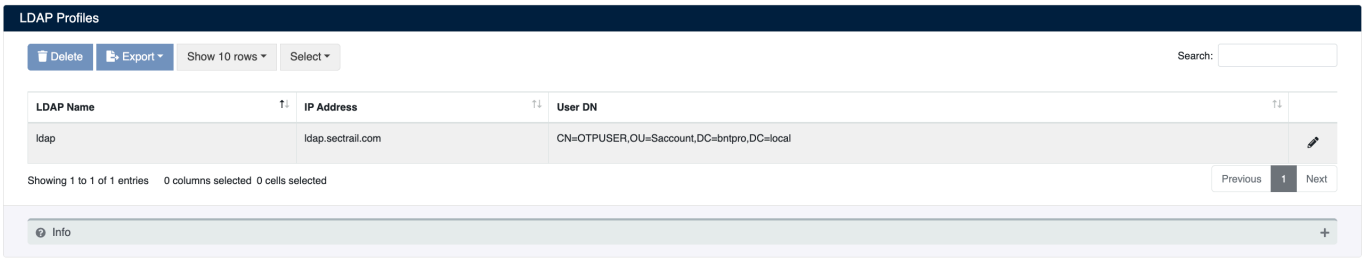


Table Columns:

- **LDAP Name**: Profile name
- **IP Address**: LDAP server IP address
- **User DN**: Administrator DN used for connection

Profile Operations:

Two action buttons are located on the right side of each profile row:

- **Edit ()**: Edit LDAP profile settings
- You can update all configuration fields
- Server address, port, DN information can be changed
- You may need to re-enter the password
- **Delete ()**: Delete LDAP profile
- Deletion is irreversible
- Remote Authentication Policies associated with this profile may be affected

> **CAUTION**

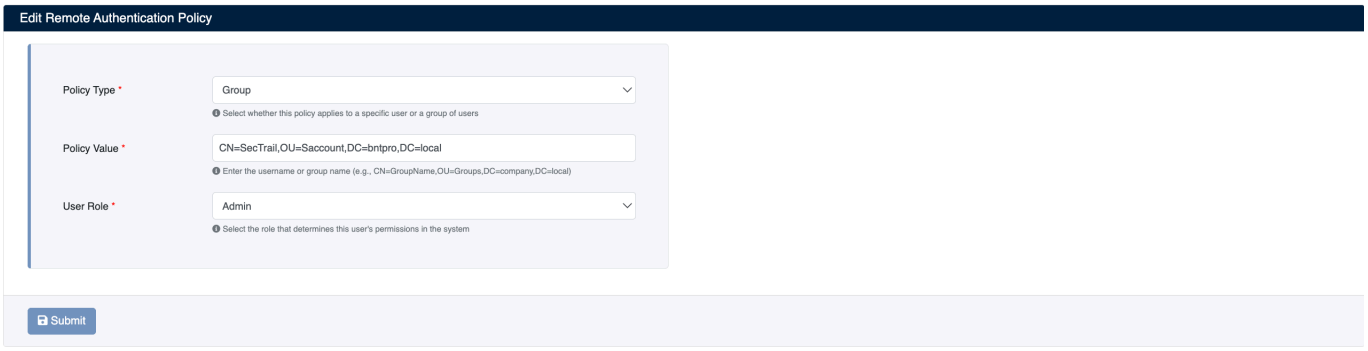
> Before deleting an actively used LDAP profile, ensure that users logging in with that profile can access the system through another method.

Remote Authentication Policies

Remote Authentication Policy allows you to assign custom roles to LDAP/AD users on a group or user basis. This way, you can assign different roles based on AD group memberships.

Creating a New Policy

You can create a new policy using the **Add New Remote Authentication Policy** form.



Form Fields

- **Policy Type**: Type of policy
- **Group**: AD group-based policy
- **User**: Individual user-based policy
- **Policy Value**: Policy value (varies based on Policy Type)
- **If Group is selected**: AD group DN is entered
- **If User is selected**: Only username is entered
- **User Role**: Role to be assigned to users matching this policy

Policy List

The **Remote Authentication Policy** table displays all defined policies.

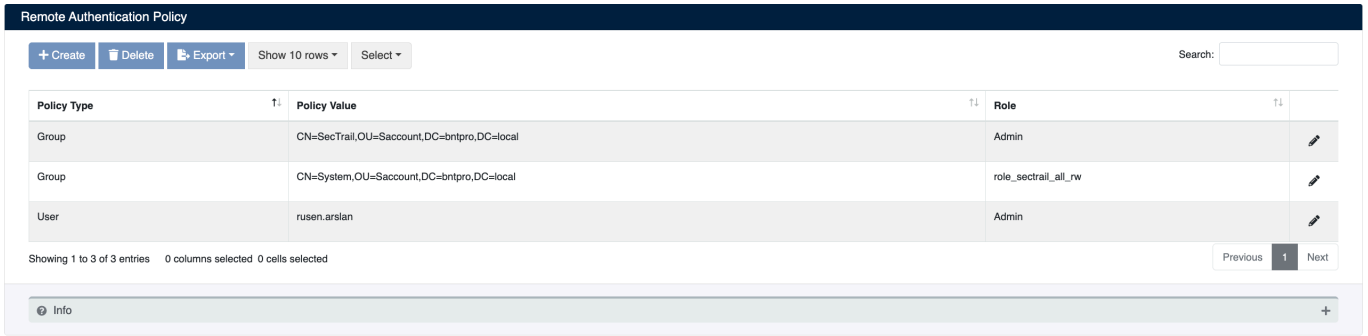


Table Columns:

- **Policy Type**: Type of policy (`Group` or `User`)
- **Policy Value**: Group DN or username
- **Role**: Assigned role

Policy Operations:

Two action buttons are located on the right side of each policy row:

- **Edit ()**: Edit policy settings
- Policy type, value, or role can be changed
- Edit carefully for active users
- **Delete ()**: Delete policy
- When a policy is deleted, users return to the default role in the LDAP profile
- Active sessions are not affected, applies to new logins

Policy Priority Order

If multiple policies apply to a user, the priority order is as follows:

1. **User Policies**: Highest priority
2. **Group Policies**: Second priority

> **TIP**
>
> Use group-based policies whenever possible. This simplifies management and works in harmony with your AD structure.

> **WARNING**
>
> Policy changes take effect in new sessions. Active users may need to log in again.

User Roles

In SecTrail CM, users are managed through role-based authorization. One or more roles can be assigned to each user.

Default Roles

- **Admin**: Full administrator privileges
- **API**: Dedicated role for API access

For detailed information about roles and permissions, see the Role and Permissions section.

Role and Permissions

SecTrail CM manages user permissions using role-based access control (RBAC). This system allows you to assign appropriate permissions to users based on their job definitions and provides secure access management.

Role-Based Access Control

Role-based access control is a security model that enables permission assignment through roles rather than directly assigning permissions to users.

Basic Concepts

- **Role**: A logical group of specific permissions
- **Permission**: Authorization for a specific operation that can be performed in the system
- **User**: A system user assigned to one or more roles

Advantages

- **Centralized Management**: Permissions are managed at the role level
- **Easy Maintenance**: User permissions are updated collectively through role changes
- **Security**: Facilitates the application of the principle of least privilege
- **Flexibility**: Role definitions suitable for organizational structure
- **Auditability**: Role-based permission control and reporting

Default Roles

SecTrail CM comes with the following default roles:

Admin

This role has full administrator privileges and can perform all operations on the system.

Use Cases:

- System administrators
- Fully privileged super users
- Initial setup and configuration

API

This role is specifically designed for API access and is used for operations via REST API.

Use Cases:

- System integrations
- Automation scripts
- Third-party applications

Role Management

Viewing Role List

The **Role Management** screen displays all roles in the system in a simple table format.

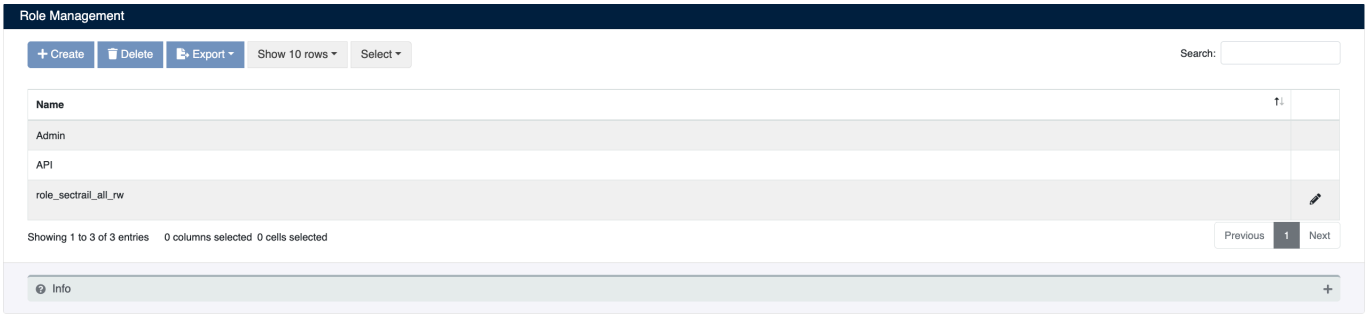
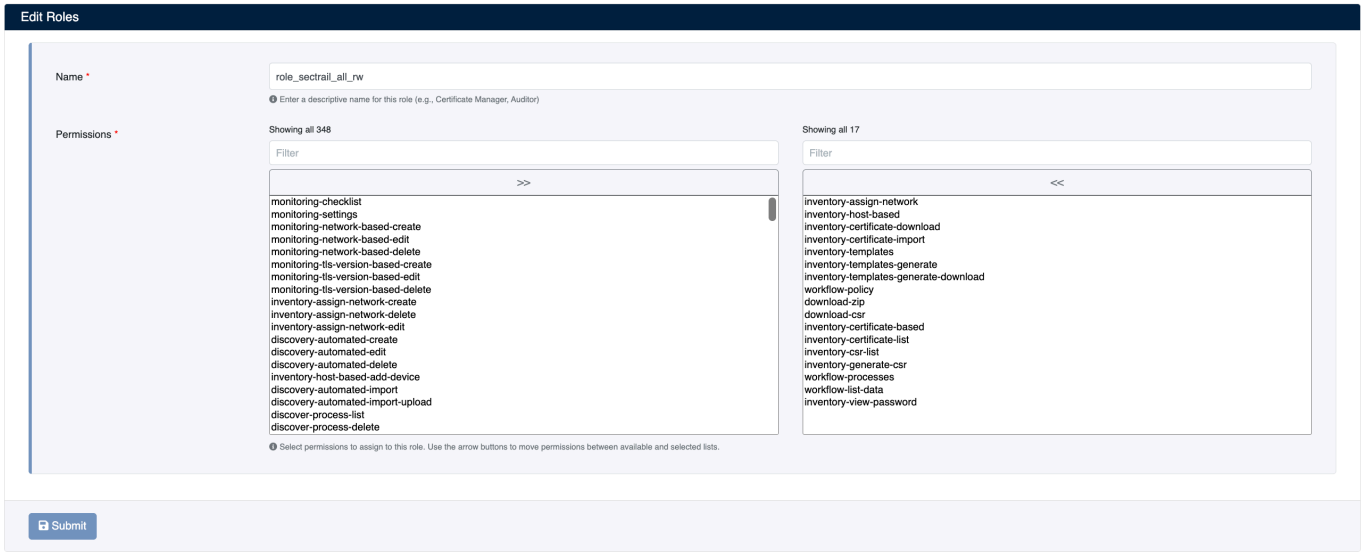


Table Columns:

- **Name**: Role name
- **Actions**: Action buttons

Creating a New Role

You can create a new role and assign permissions to it using the **Add New Roles** form.



Form Fields

- **Name**: Unique name for the role (lowercase and hyphen characters are recommended, e.g., `sign`, `certificate-viewer`, `deployment-operator`)
- **Permissions**: Permission selection is made through a two-panel transfer box

Permission Selection Interface:

The form contains two panels, left and right:

- **Left Panel**: Displays all available permissions in the system. You can quickly search for permissions using the Filter box.

- **Transfer Buttons**: You can move permissions from the left panel to the right panel with the `>>` button, and from the right panel to the left panel with the `<<` button
- **Right Panel (Selected Permissions)**: Shows the list of permissions to be assigned to the role

> **USING FILTERS**
>
> - `sign` -> Find signing operations
> - `delete` -> Find deletion permissions
> - `create` -> Find creation permissions
> - `edit` -> Find editing permissions
> - `download` -> Find download permissions

Editing a Role

1. Click the **Edit ()** button next to the role you want to edit in the role list
2. Update the role name and permissions
3. Click the **Submit** button to save the changes

Deleting a Role

1. Click the **Delete ()** button next to the role you want to delete in the role list
2. Confirm the deletion

> **WARNING**
>
> Before deleting roles assigned to active users, ensure that you have assigned other roles to these users. Otherwise, users may not be able to access the system.

Assigning Roles to Users

After creating roles, you need to assign these roles to users.

Local Users

1. Navigate to **Users** > **Local Users**
2. When creating or editing a user, select the relevant role from the **User Role** field
3. Save the changes

LDAP/AD Users

For LDAP or Active Directory users, roles are assigned through Remote Authentication Policy:

1. Navigate to the **Remote Authentication Policy** section
2. Create a group or user-based policy
3. Select the role you want to assign in the **User Role** field

For detailed information, see the User Management section.

API Documentation

SecTrail Certificate Manager provides a powerful RESTful API that enables you to automate your certificate management operations.

Overview

The SecTrail CM API provides comprehensive endpoints for certificate lifecycle management. Using the API, you can:

- Perform certificate signing operations
- Upload and manage certificates
- Manage discovery lists in bulk
- Query the certificate inventory

API Documentation Interface

SecTrail CM offers an interactive Swagger/OpenAPI documentation interface for you to explore and test all API endpoints:

```
https://your-sectrailcm-server/documentation
```

Through this interface, you can:

- View all available endpoints
- Review request/response schemas
- Test API calls directly

Authentication

Before you start using the API, you need to authenticate with a Bearer token. For detailed information, refer to the Authentication section.

Getting Started

1. Create a user with API role
2. Obtain an authentication token
3. Start using API endpoints

For all endpoints and usage examples, please review the Endpoints page.

Authentication

The SecTrail CM API uses Bearer token-based authentication. To use the API endpoints, you must first obtain an access token.

Creating an API User

Before you start using the API, you should create a user with API role:

Steps

1. Navigate to **Users** > **Local Users** in the SecTrail CM interface
2. Create a new user
3. Assign the **API** role to the user
4. Save the username and password

> **TIP**
>
> Use strong passwords for API users and store these credentials securely.

Obtaining an Authentication Token

After creating your API user, you need to obtain an authentication token.

Endpoint

```
POST /api/login
```

Request Body

```
{
 "username": "api-user",
 "password": "your-secure-password"
}
```

Response

```
{
 "user": "apiuser",
 "access_token": "eyJ0eXAiOiJKV1QiLCJhbGci..."
}
```

Example cURL Command

```
curl -X POST https://your-sectrailcm-server/api/login \
 -H "Content-Type: application/x-www-form-urlencoded" \
 -d "username=api-user&password=your-secure-password"
```

Using the Token

You must use the obtained authentication token in the `Authorization` header for all your API requests:

```
curl -X GET https://your-sectrailcm-server/api/endpoint \
 -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."
```

Token Expiration

- Authentication tokens expire after a certain period
- When your token expires, you need to obtain a new token
- The response contains the username (`user`) and access token (`access_token`) information

Security Recommendations

- Never store tokens in your source code
- Use environment variables or a secure vault
- Secure all API requests by using HTTPS
- Renew tokens regularly
- Grant only necessary permissions to API users

API Endpoints

The SecTrail CM API provides various endpoints to automate your certificate management operations. For detailed documentation of all endpoints, you can use the Swagger interface:

```
https://your-sectrailcm-server/documentation
```

Primary Use Cases

1. Certificate Signing

You can perform certificate signing operations in various formats through the API:

Supported Signing Types:

- CSR (Certificate Signing Request) signing
- Self-Signed certificate creation
- Template-based certificate generation
- JKS (Java KeyStore) format certificate creation

Endpoint:

```
POST /api/generate
```

> **INFO**
> For certificate signing operations, the operation type is determined using the `requestType` parameter. Please review the Swagger documentation for a detailed parameter list.

2. Certificate Upload and Distribution

You can automatically distribute your certificates to target servers and devices through the API:

Features:

- Distribution to multiple target devices (F5, Apache, Nginx, IIS, etc.)
- Virtual host-based distribution
- Scheduled distribution support
- Retry mechanism for failed distributions
- Distribution status querying and monitoring

Endpoint:

```
POST /api/deployment
```

3. Discovery List Management

You can manage your discovery lists in bulk through the API:

Features:

- Discovery list creation
- Bulk domain/IP addition
- Querying discovery results
- Scheduling discovery plans

Endpoint:

```
POST /api/discoverList
```

4. Certificate Inventory

You can query certificates in the inventory and retrieve their information:

Features:

- Retrieving bulk certificate list
- Viewing certificate details
- Querying certificate status

Endpoint:

```
POST /api/getCertificates
```

API Usage Examples

Authentication

You must use an authentication token in all API requests:

```
curl -X POST https://your-sectrailcm-server/api/endpoint \
 -H "Authorization: Bearer YOUR_TOKEN" \
 -H "Content-Type: application/json" \
 -d '{"key": "value"}'
```

Error Handling

The API uses standard HTTP status codes:

- `200 OK` - Request successful
- `201 Created` - Resource created
- `400 Bad Request` - Invalid request
- `401 Unauthorized` - Authentication error
- `403 Forbidden` - Authorization error
- `404 Not Found` - Resource not found
- `500 Internal Server Error` - Server error

Swagger Documentation

Use the Swagger interface for detailed descriptions of all endpoints, parameter definitions, and example request/response structures:

```
https://your-sectrailcm-server/documentation
```

Through the Swagger interface, you can:

- Explore all endpoints
- View request/response schemas
- Test API calls interactively

> **TIP**
>
> You can use the "Try it out" feature in the Swagger documentation to test your API calls directly and see the results.