SecTrail Certificate Manager

Kullanım Dokümantasyonu

v2.7.0

4 Haziran 2026

İçindekiler

SecTrail Certificate Manager

SecTrail Certificate Manager (CM), kurumsal sınıf SSL/TLS dijital sertifika yaşam döngüsü yönetimi için tasarlanmış kapsamlı bir platformdur.

> **VERSİYON BİLGİSİ**
>
> Bu dokümantasyon **SecTrail CM v2.7.0** için hazırlanmıştır.

Genel Bakış

SecTrail CM, organizasyonların karşılaştığı kritik sertifika yönetimi zorluklarını ele alır:

- **Envanter Boşlukları**: Dağıtık sistemlerde sertifikaların takibi
- **Manuel İşlem Yükü**: Zaman alıcı manuel süreçlerin otomasyonu
- ⏰ **Son Kullanma Tarihi Takibi**: Sertifika süre dolumlarının izlenmesi
- **Operasyonel Yük**: İş yükünün azaltılması ve verimliliğin artırılması

Neden SecTrail CM?

SecTrail Certificate Manager ile organizasyonlar:

- [OK] Reaktif, kriz odaklı yönetimden **proaktif otomasyona** geçiş yapar
- [OK] Tekrarlayan manuel süreçleri **otomatikleştirir**
- [OK] Sertifika envanterinde **tam görünürlük** elde eder
- [OK] Dijital dönüşüm süreçlerinde **operasyonları kolaylaştırır**
- [OK] Beklenmedik servis kesintilerinin **önüne geçer**

Temel Özellikler

Sertifika Keşfi

Altyapınızdaki tüm sertifikaları otomatik olarak keşfedin ve envanterinize ekleyin.

Sertifika Envanteri

Merkezi bir katalogda tüm sertifikalarınızı takip edin ve yönetin.

Sertifika Otoritesi (CA)

Dahili CA altyapınızı yönetin ve kurum içi sertifikalar oluşturun.

Sertifika İzleme

Sertifika durumlarını sürekli izleyin ve proaktif uyarılar alın.

Sertifika İş Akışı

Onay ve talep süreçlerini yönetin. Sürecin tamamen otomatik yönetilmesi ile iş akışlarınızı kolaylaştırın.

Sistem Entegrasyonları

Üçüncü taraf sistemlerle sorunsuz entegrasyon sağlayın.

RBAC Yetkilendirme

Rol tabanlı erişim kontrolü ile güvenli yönetim.

Hızlı Başlangıç

SecTrail CM ile hızlıca başlamak için:

1. **Kurulum Kılavuzu** - Sistemin kurulumu ve yapılandırması
2. **Hızlı Başlangıç** - İlk adımlar ve temel kullanım
3. **Kullanım Kılavuzu** - Detaylı kullanım senaryoları

Sonraki Adımlar

SecTrail CM yolculuğunuza bu adımlarla devam edebilirsiniz:

Başlangıç

Kurulum ve temel yapılandırma

Genel Bakış ->

Özellikler

Tüm özellikleri keşfedin

Sertifika Keşfi ->

Entegrasyonlar

Sistemlerinizle entegre edin

Entegrasyon Rehberi ->

Destek ve Topluluk

Herhangi bir sorunuz veya desteğe ihtiyacınız var mı?

Kanal	Açıklama	Bağlantı
Destek Portalı	Teknik destek ve bilet sistemi	destek.bntpro.com
Ürün Sayfası	Ürün bilgileri ve güncellemeler	www.sectrail.com/cm

SecTrail Certificate Manager ile kesintisiz güvenlik ve maksimum verimlilik.

Genel Bakış

SecTrail Certificate Manager (CM), SSL/TLS sertifikalarının uçtan uca tüm yaşam döngüsünün tek bir portal üzerinden yönetilmesini sağlayan dijital bir platformdur.

SecTrail CM Nedir?

SecTrail Certificate Manager, organizasyonların dijital sertifikalarını merkezi bir platformdan keşfetmesini, izlemesini, yönetmesini ve otomatikleştirmesini sağlayan bir sertifika yaşam döngüsü yönetim sistemidir.

Temel Problem ve Çözüm

Günümüzde organizasyonlar, büyüyen dijital altyapıları ile birlikte yüzlerce hatta binlerce SSL/TLS sertifikası yönetmek zorundadır. Bu sertifikalar, farklı sunucularda, bulut platformlarında, yük dengeleyicilerde ve CDN'lerde dağılmış durumda olabilir. Manuel takip sistemleri, Excel dosyaları veya dağınık araçlar kullanılarak yönetilen sertifikalar, organizasyonlar için ciddi riskler oluşturur:

- **Süre Dolumu Riskleri**: Zamanında yenilenmeyen sertifikalar, kritik servislerin kesintiye uğramasına ve iş kayıplarına neden olabilir
- **Güvenlik Açıkları**: Zayıf algoritmalı, düşük bit uzunluğuna sahip veya güvenilmeyen CA'lar tarafından imzalanmış sertifikalar güvenlik tehdidi oluşturur
- **Uyumluluk Sorunları**: Düzenleyici gereksinimlerin karşılanmaması, audit süreçlerinde sorunlar ve olası cezalarla karşılaşılabilmektedir
- **Görünürlük Eksikliği**: Organizasyonun kaç sertifikası olduğu, nerede kullanıldığı ve ne durumda olduğu belirsizdir
- **Yüksek Operasyonel Yük**: Sertifika yönetimi için ekstra zaman ve insan kaynağı harcanmaktadır

SecTrail CM, bu zorlukları otomatik keşif, merkezi yönetim, proaktif izleme ve akıllı otomasyon özellikleri ile çözerek, organizasyonların sertifika yönetimini güvenli, verimli ve ölçeklenebilir bir şekilde gerçekleştirmesini sağlar.

Zorluk	SecTrail CM Çözümü
Dağınık Altyapı	Otomatik keşif ile tüm sertifikaları tek noktadan görüntüleme
Manuel Süreçler	Sertifika yaşam döngüsünün tamamen otomatikleştirilmesi
Görünürlük Eksikliği	Merkezi envanter ve gerçek zamanlı izleme
Süre Dolumu Riskleri	Proaktif uyarılar ve otomatik yenileme
Uyumluluk Zorlukları	Detaylı raporlama ve audit trail

Temel Faydalar

Kategori	Faydalar
** Operasyonel Verimlilik**	Manuel işlemleri %80'e kadar azaltma, ekip verimliliğini artırma
** Risk Azaltma**	Kesinti önleme, güvenlik açıklarını proaktif tespit, uyumsuzluk riskini minimize etme
** Maliyet Tasarrufu**	Operasyonel maliyet düşürme, kesinti maliyetlerini önleme
** Görünürlük ve Kontrol**	Tam envanter, gerçek zamanlı izleme, detaylı raporlama

Kurulum Kılavuzu

Bu bölümde SecTrail Certificate Manager'ın kurulum adımlarını detaylı olarak bulabilirsiniz.

Kurulum Özeti

SecTrail CM, **sanal bir sunucu (Virtual Appliance)** olarak OVA formatında sunulmaktadır. Bu yaklaşım, kurulumu oldukça basitleştirir:

- [OK] **Kolay Kurulum**: OVA dosyasını sanallaştırma ortamınıza deploy edin
- [OK] **Önceden Yapılandırılmış**: Tüm bileşenler (veritabanı, web sunucusu, vs.) hazır gelir
- [OK] **Hızlı Başlangıç**: Sadece ağ yapılandırması yapın ve kullanmaya başlayın
- [OK] **Manuel Kurulum Yok**: Paket yönetimi, bağımlılık çözümü veya servis yapılandırması gerekmez

Temel Adımlar:

1. OVA imajını sanallaştırma platformuna import edin
2. VM'i başlatın ve `stadmin` kullanıcısıyla giriş yapın
3. `config` komutuyla ağ ayarlarını yapılandırın
4. Web arayüzünden sisteme erişin

Sistem Gereksinimleri

Donanım Gereksinimleri

Minimum Gereksinimler

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

Önerilen Gereksinimler (Üretim Ortamı)

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

Kurulum Öncesi Hazırlık

1. Sanallaştırma Ortamı Gereksinimleri

SecTrail CM, OVA formatında sanal bir makine imajı olarak dağıtılır.

2. Ağ Yapılandırması Hazırlığı

Kurulum öncesinde aşağıdaki ağ bilgilerini hazır bulundurun:

Parametre	Açıklama
IP Adresi	SecTrail CM için statik IP adresi (CIDR notasyonunda)
Gateway	Default gateway IP adresi
DNS Sunucular	Birincil (ve isteğe bağlı ikincil/üçüncül) DNS sunucu adresleri

3. Güvenlik Duvarı ve Port Yapılandırması

SecTrail CM'in düzgün çalışabilmesi için aşağıdaki portların açık olması gerekmektedir:

Port	Protokol	Kullanım	Yön
443	HTTPS	Web Arayüzü	Inbound
22	SSH	Uzaktan yönetim (opsiyonel)	Inbound

Kurulum Adımları

SecTrail CM, sanal bir sunucu (Virtual Appliance) olarak sunulmaktadır ve OVA (Open Virtualization Archive) formatında dağıtılır. Kurulum için manuel paket yönetimine gerek yoktur.

1. OVA İmajının Sanallaştırma Ortamına Deploy Edilmesi

SecTrail CM OVA imajını sanallaştırma ortamınıza deploy edebilirsiniz.

2. İlk Giriş ve Ağ Yapılandırması

VM başlatıldıktan sonra konsol ekranından aşağıdaki adımları takip edin:

Giriş Bilgileri

İlk giriş için aşağıdaki kullanıcı adını kullanın:

- **Kullanıcı Adı**: `stadmin`
- **Şifre**: Şifre sizinle paylaşılacaktır

Ağ Yapılandırması

Giriş yaptıktan sonra ağ yapılandırmasını başlatın:

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

Komut çalıştırıldığında **SecTrail CM Configurator** başlayacaktır.

Adım 1: IP Adresi Yapılandırması

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

IP Address: 10.34.24.56/24
OK
```

- CIDR notasyonunda IP adresi ve subnet mask'ı girin (örn: `10.34.24.56/24`)
- Enter tuşuna basarak onaylayın

Adım 2: Gateway Adresi Yapılandırması

```
Please enter a valid Gateway Address

Gateway IP Address: 10.34.24.1
OK
```

- Default gateway IP adresini girin
- Enter tuşuna basarak onaylayın

Adım 3: DNS Sunucu Yapılandırması

```
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
```

- Yapılandırmak istediğiniz DNS sunucu sayısını girin (1-3 arası)
- Her DNS sunucu için IP adresini girin

Adım 4: Yapılandırma Özeti ve Onay

```
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
```

- Girdiğiniz bilgileri kontrol edin
- Doğruysa `y` tuşuna basarak devam edin

Yapılandırma Aktivasyonu

```
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
```

Ağ yapılandırması başarıyla tamamlandığında yukarıdaki mesajları göreceksiniz.

3. Uygulama Anahtarı Oluşturma (Opsiyonel)

Ağ yapılandırması tamamlandıktan sonra, SecTrail CM uygulama anahtarı oluşturma seçeneği sunulur:

```
SecTrail CM Application Key Generator

regenerate Application Key

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

- Yeni bir uygulama anahtarı oluşturmak için `y` tuşuna basın
- Mevcut anahtarı korumak için `n` tuşuna basın

```
Application key set successfully.
```

4. Yapılandırma Tamamlandı

Yapılandırma tamamlandıktan sonra, web arayüzüne erişim için belirlediğiniz IP adresini kullanabilirsiniz.

Kurulum Sonrası Kontroller

1. Web Arayüzüne Erişim

Ağ yapılandırması tamamlandıktan sonra, tarayıcınızdan aşağıdaki adrese gidin:

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

> **SSL SERTİFİKA UYARISI**
>
> İlk erişimde tarayıcınız self-signed SSL sertifikası nedeniyle güvenlik uyarısı verebilir. Üretim ortamında kurumsal CA tarafından imzalanmış bir sertifika kullanmanız önerilir.

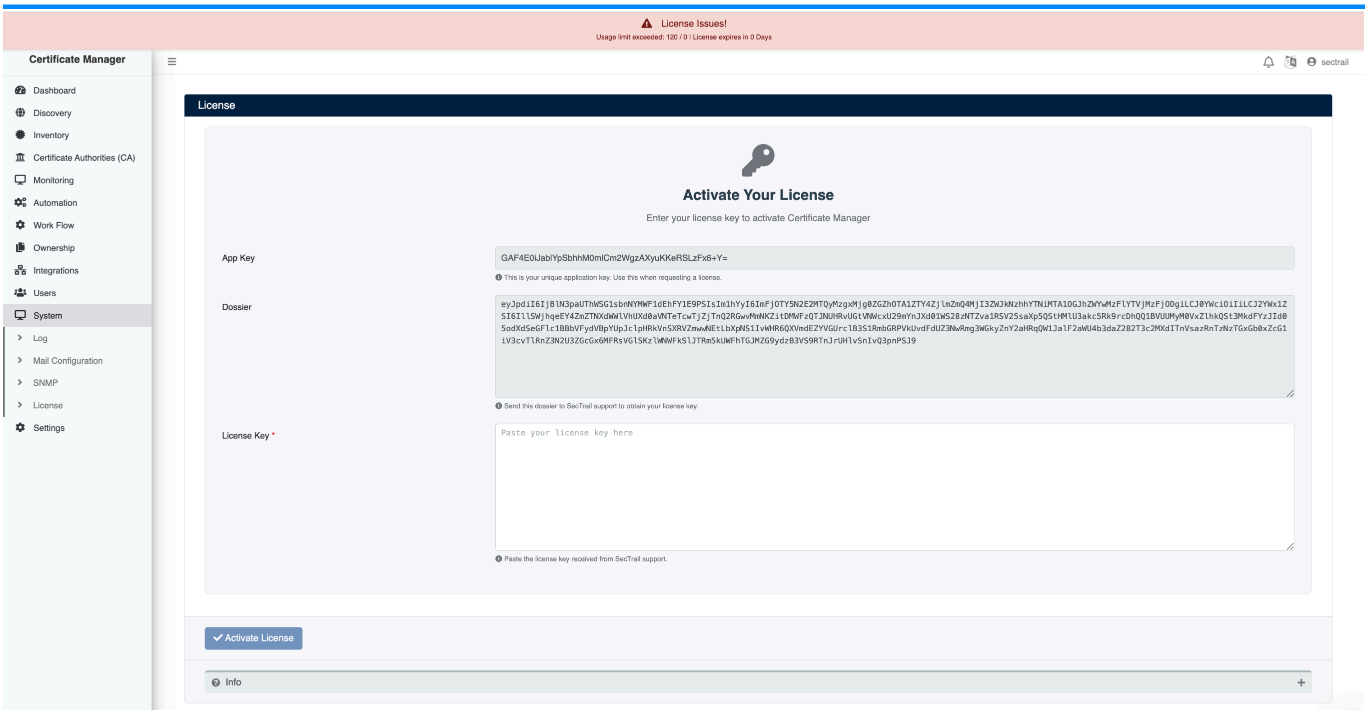
İlk Giriş Bilgileri

Web arayüzü ilk giriş için varsayılan yönetici hesabı:

- **Kullanıcı Adı**: `admin`
- **Şifre**: `admin`

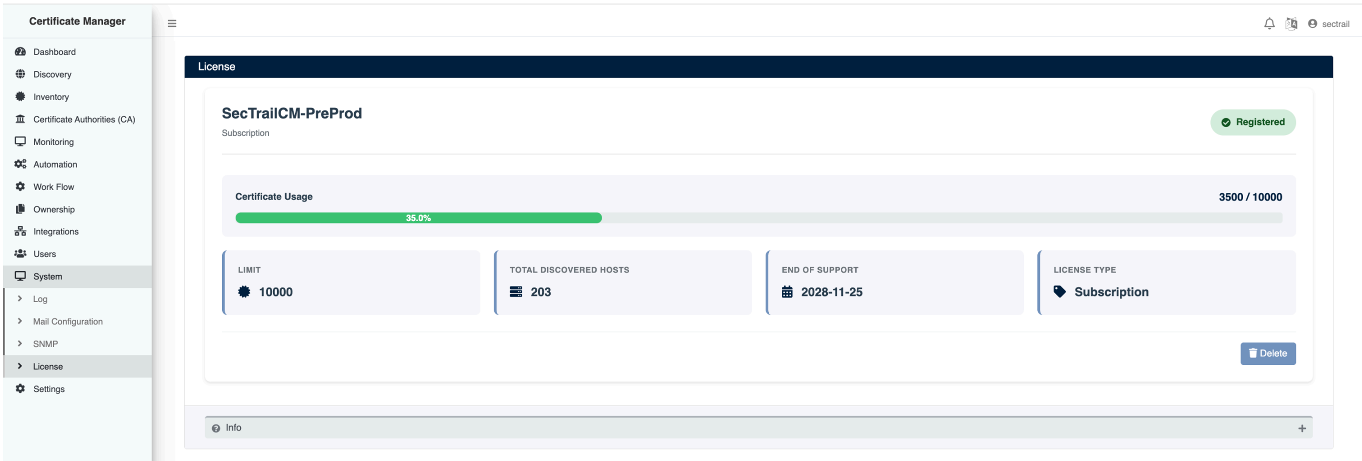
2. Lisans Aktivasyonu

İlk girişte lisans aktivasyonu yapmanız gerekmektedir. Lisans aktivasyonu için aşağıdaki adımları izleyin:



1. Web arayüzüne ilk giriş yaptığınızda lisans aktivasyon ekranı karşınıza gelecektir
2. Ekranda görünen **App Key** ve **Dossier** bilgilerini SecTrail CM destek ekibi ile paylaşın
3. Destek ekibinin size ileteceği **License Key**'i ilgili alana girin
4. Lisans doğrulaması otomatik olarak yapılacaktır

Lisans aktivasyonu tamamlandıktan sonra, lisans detaylarınızı görebilirsiniz:



SERTİFİKA SAYIMI

SecTrail CM, lisans kapsamında sertifikaları **benzersiz (unique)** olarak sayar. Aynı sertifika farklı sistemlerde (örneğin farklı sunucularda veya yük dengeleyicilerde) kullanılsa bile sadece bir kez sayılır. Bu sayede gerçek sertifika sayınızı yönetebilir ve lisansınızı verimli şekilde kullanabilirsiniz.

LİSANS ALMA

App Key ve Dossier bilgilerinizi destek@sectrail.com veya sdg-dev@bntpro.com adreslerine göndererek lisans anahtarınızı temin edebilirsiniz.

Hızlı Başlangıç

SecTrail Certificate Manager'a hoş geldiniz! Bu kılavuz, platformu kullanmaya başlamanız için gereken temel adımları içerir.

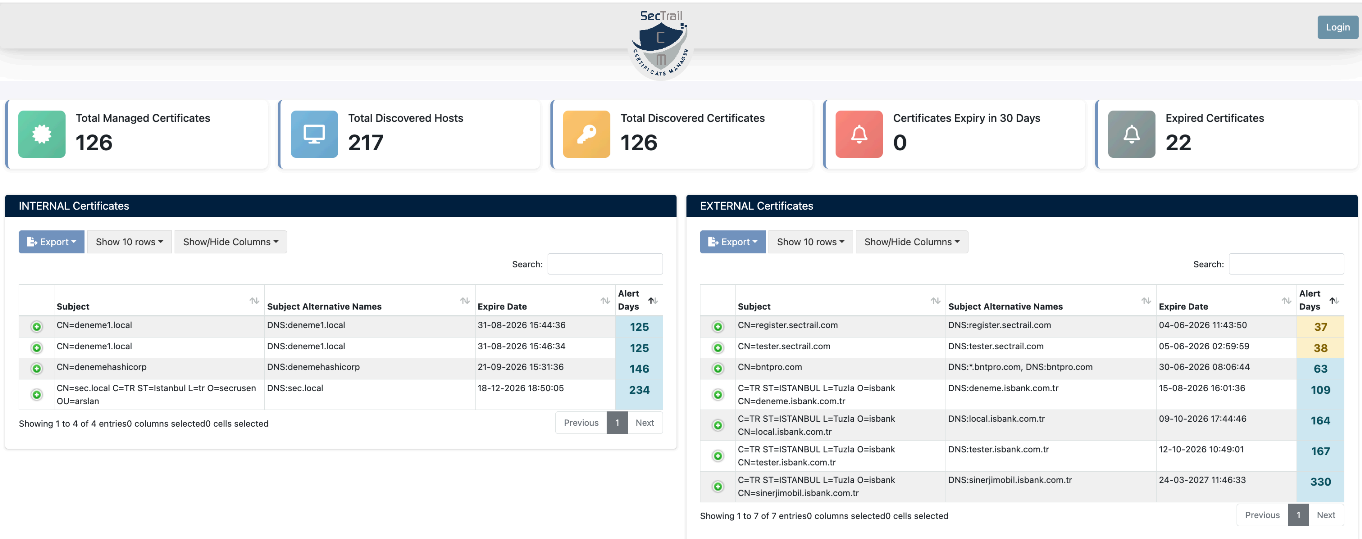
1. Platforma Erişim

Web tarayıcınızdan SecTrail CM adresinize gidin:

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

2. Public Dashboard

> **PUBLİC DASHBOARD**
>
> SecTrail CM'e giriş yapmadan önce **Public Dashboard**'u görüntüleyebilirsiniz. Bu ekran, altyapınızdaki sertifikaların genel durumunu herkese açık olarak gösterir.



SecTrail CM Public Dashboard - Sertifika Genel Durumu

Dashboard Metrikleri

Public Dashboard üzerinde aşağıdaki önemli metrikleri görebilirsiniz:

Metrik	Açıklama
Total Managed Certificates	Yönetilen toplam sertifika sayısı
Total Discovered Hosts	Keşfedilen toplam host sayısı
Total Discovered Certificates	Keşfedilen toplam sertifika sayısı
Certificates Expiry in 30 Days	30 gün içinde süresi dolacak sertifikalar
Expired Certificates	Süresi dolmuş sertifikalar

Sertifika Görünümleri

Dashboard iki ana kategori altında sertifikaları listeler:

- **INTERNAL Certificates**: İç ağdaki (internal) sertifikalar
- **EXTERNAL Certificates**: Dış ağdaki (external) sertifikalar

Sertifika Detayları

Her sertifika için aşağıdaki bilgiler görüntülenir:

- **Subject** - Sertifika konusu
- **Subject Alternative Names** - Alternatif isimler (SAN)
- **Expiry Date** - Son kullanma tarihi
- **Days to Expiry** - Sona erme gün sayısı

> **İPUCU**
>
> - **Show/Hide Columns** butonu ile görmek istediğiniz kolonları özelleştirebilirsiniz
> - **+** tuşuna tıklayarak sertifika detaylarına erişebilirsiniz

3. Giriş Yapma

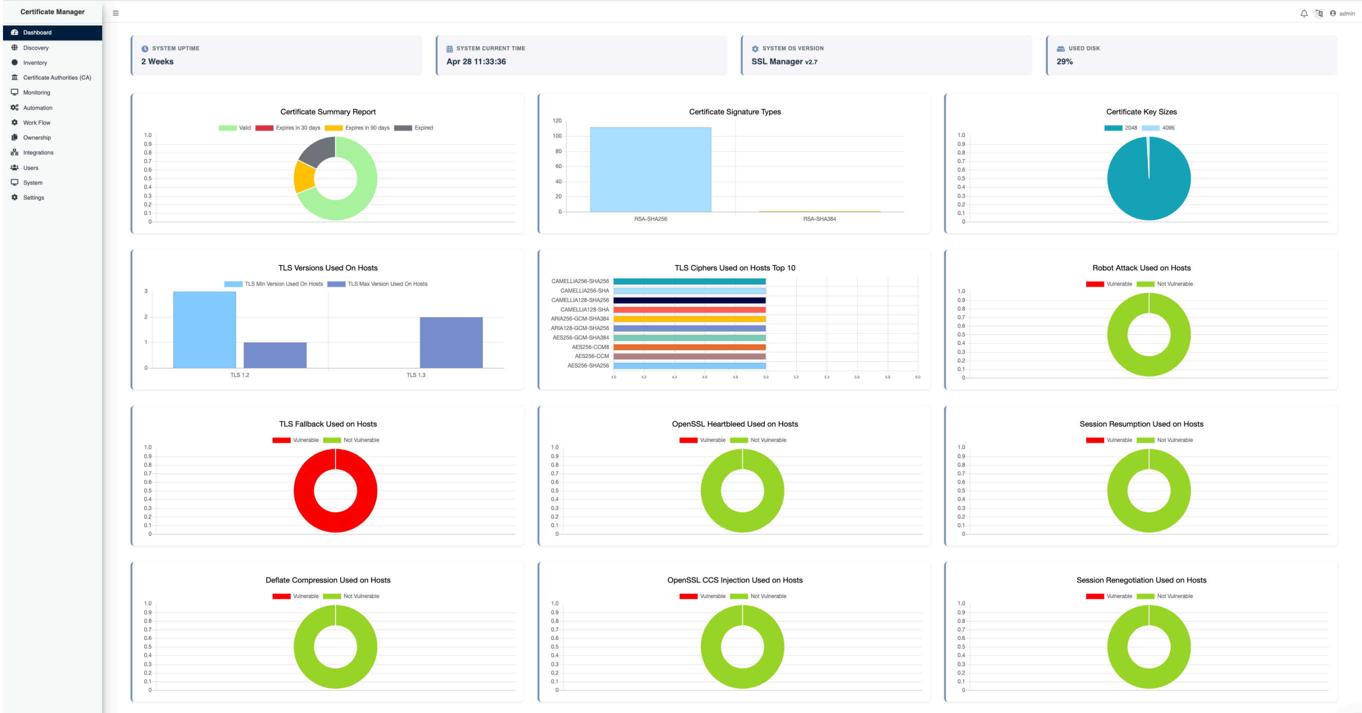
> **VARSAYILAN GİRİŞ BİLGİLERİ**
>
> İlk kurulumda varsayılan giriş bilgileri kullanılır. Güvenlik için bu bilgileri ilk girişten sonra mutlaka değiştirin.

Giriş bilgilerinizi girin:

- **Kullanıcı Adı**: `admin`
- **Şifre**: `admin`

4. Ana Dashboard

Giriş yaptıktan sonra ana dashboard'u göreceksiniz. Bu ekran, sisteminizin kapsamlı bir görünümünü sunar.



SecTrail CM Ana Dashboard - Sistem Genel Bakış

Dashboard'da şunları görebilirsiniz:

- **Sistem Metrikleri**: Uptime, current time, OS version, disk kullanımı
- **Sertifika Durum Grafikleri**: Geçerli/süresi dolacak/dolmuş sertifikalar
- **Güvenlik Grafikleri**: TLS versiyonları, cipher suite'ler, güvenlik açıkları
- **Sol Menü**: Platformun tüm özelliklerine erişim

> **DETAYLI BİLGİ**
>
> Dashboard'daki tüm grafiklerin ve metriklerin detaylı açıklaması için **Dashboard Kullanım Kılavuzu** sayfasını inceleyin.

Sol Menü - Ana Navigasyon

Sol taraftaki menüden platformun tüm özelliklerine erişebilirsiniz:

Dashboard : Ana ekran ve genel sistem durumu

Discovery : Yeni sertifikaları keşfet

Inventory : Sertifika envanteri

Certificate Authorities (CA) : Sertifika otoriteleri yönetimi

Monitoring : Sertifika izleme ve uyarılar

Automation : Otomatik görevleri yönet

Work Flow : İş akışı yönetimi

Ownership : Sertifika sahipliği

Integrations : Entegrasyonlar

Users : Kullanıcı yönetimi

Sertifika Keşfi

Sertifika Keşfi, SecTrail CM'in altyapınızdaki tüm SSL/TLS sertifikalarını otomatik olarak bulup envantere ekleyen güçlü bir özelliktir.

Genel Bakış

> **NEDEN SERTİFİKA KEŞFİ ÖNEMLİDİR?**
>
> Organizasyonlarda sertifikaların nerede kullanıldığının bilinmemesi büyük bir güvenlik riski oluşturur. Süresi dolmuş veya unutulmuş sertifikalar, hizmet kesintilerine ve güvenlik açıklarına yol açabilir.

Temel Özellikler

SecTrail CM'in Sertifika Keşfi özelliği, sertifika yönetimini kolaylaştırır:

Özellik	Açıklama
Otomatik Keşif	Altyapınızdaki tüm sertifikaları otomatik olarak bulur
Merkezi Envanter	Tüm sertifikaları tek bir merkezi sistemde toplar
Düzenli Tarama	Zamanlanmış taramalarla envanteri güncel tutar
Hızlı Tarama	Geniş ağları hızlı ve verimli şekilde tarar
Çoklu Yöntem	Ağ tarama ve CT Logs ile kapsamlı keşif

Keşif Yöntemleri

SecTrail CM, farklı senaryolara uygun iki güçlü keşif yöntemi sunar:

1. Ağ Taraması

> **AĞ TARAMASI NEDİR?**
>
> Ağ Taraması, belirtilen IP aralıklarını veya subnet'leri tarayarak bu ağdaki cihazların SSL/TLS sertifikalarını tespit eder.

Nasıl Çalışır?

Ağ Taraması yöntemi, belirlediğiniz IP aralıklarını ve portları tarayarak aktif SSL/TLS bağlantılarını tespit eder. Bulunan her sertifika otomatik olarak envantere eklenir ve yapılandırdığınız periyotlarda tarama tekrarlanarak yeni sertifikalar keşfedilir.

Kullanım Senaryoları

Ağ Taraması yöntemi aşağıdaki senaryolarda kullanılır:

- ** Sunucu Altyapısı** - Tüm sunucu altyapınızı düzenli olarak tarama
- ** Datacenter Taraması** - Belirli bir datacenter veya subnet'i tarama

- ** Yeni Sunucular** - Yeni eklenen sunucuları otomatik keşfetme
- ** Port Bazlı Tarama** - Standart olmayan portlarda çalışan servisleri bulma

2. Sertifika Şeffaflığı Logları (CT Logs)

SERTİFİKA ŞEFFAFLIĞI LOGLARI NEDİR?

Sertifika Şeffaflığı Logları (Certificate Transparency Logs), public olarak yayınlanan sertifikaların kayıtlarıdır. Sertifika otoriteleri (CA'lar), yayınladıkları sertifikaları bu loglara kaydeder. Bu yöntem, domain bazlı sertifika keşfi için kullanılır.

Nasıl Çalışır?

Sertifika Şeffaflığı Logları yöntemi, belirttiğiniz domain için public sertifika otoritelerinin (CA) kayıtlarını tarar. Bu sayede organizasyonunuza ait ama belki de bilmediğiniz tüm public sertifikaları keşfedebilirsiniz. SecTrail CM, crt.sh ve SSLMate gibi güvenilir CT Log servislerini kullanır.

Avantajları

Avantaj	Açıklama
Public Sertifikalar	Public olarak yayınlanmış tüm sertifikaları bulur
Bilinmeyen Sertifikalar	Organizasyonunuza ait ama bilmediğiniz sertifikaları keşfeder
Gölge BT	Yetkisiz departmanlar tarafından alınan sertifikaları tespit eder
Alt Alan Adı Keşfi	Ana domain'e bağlı tüm alt alan adı sertifikalarını bulur

Kullanım Senaryoları

Sertifika Şeffaflığı Logları yöntemi aşağıdaki senaryolarda kullanılır:

- ** Public Sertifikalar** - İnternet'e açık tüm sertifikalarınızı keşfetme
- ** Organizasyon Envanteri** - Organizasyona ait tüm domain'leri tarama
- ** Gölge BT Tespiti** - Yetkisiz alınan sertifikaları bulma
- ** Alt Alan Adı İzleme** - Tüm alt alan adı sertifikalarını takip etme

3. Entegrasyon Sistemlerinden Keşif

ENTEGRASYON KEŞFİ NEDİR?

Entegrasyon Keşfi, altyapınızda kullandığınız mevcut sistemlerle (load balancer, web sunucu, keystore vb.) doğrudan entegre olarak bu sistemlerdeki sertifikaları otomatik keşfeder. API veya protokol bazlı bağlantılarla gerçek zamanlı sertifika envanteri sağlar.

Nasıl Çalışır?

SecTrail CM, entegre ettiğiniz sistemlere güvenli API veya protokol bağlantıları kurarak bu sistemlerdeki tüm sertifikaları otomatik olarak keşfeder. Entegrasyon yapılandırıldıktan sonra, belirlediğiniz periyotlarda sistem otomatik olarak tarama yapar ve yeni eklenen veya güncellenen sertifikaları envantere ekler.

Desteklenen Entegrasyon Sistemleri

SecTrail CM aşağıdaki sistemlerden otomatik sertifika keşfi yapabilir:

- **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**

Kullanım Senaryoları

Entegrasyon Keşfi aşağıdaki senaryolarda kullanılır:

- ** Yapılandırma Yönetimi** - Yük dengeleyici ve web sunucularındaki sertifikaları merkezi yönetme
- ** Keystore İzleme** - Java Keystore ve Windows TrustStore'daki sertifikaları takip etme
- ** Otomatik Senkronizasyon** - Üretim sistemlerindeki değişiklikleri anlık yakalama
- ** Gizli Anahtar Yönetimi** - HashiCorp Vault gibi gizli anahtar yönetim sistemlerindeki sertifikaları keşfetme

> **ENTEGRASYON KURULUMU**
>
> Desteklenen sistemlerle entegrasyon kurmak için Entegrasyonlar sayfasını ziyaret edin.

Önerilen Yaklaşımlar

Öneri	Açıklama
⏰ **Düzenli Tarama**	Günlük otomatik tarama yaparak yeni sertifikaları hızlı yakalayın
Test Ortamı	Üretim ortamına geçmeden önce test ortamında deneyin
⏱ **Uygun Zamanlama**	Taramaları iş saatleri dışında (gece) çalıştırın

Dikkat Edilmesi Gerekenler

Konu	Açıklama
Ağ Yükü	Yoğun saatlerde büyük ağ taramaları yapmaktan kaçının
Trafik İzleme	Tarama sırasında ağ trafiğini izleyin
Firewall Kuralları	SecTrail CM'in tarama yapacağı portların açık olduğundan emin olun
⏲ **Hız Sınırlandırma**	Aynı anda çok fazla bağlantı açmayın, hız sınırlandırmaya dikkat edin
İzinler	Tarama yapacağınız ağlar için gerekli izinleri alın

Keşif İşlemleri

SecTrail CM, hem zamanlanmış otomatik keşif hem de anlık manuel keşif imkanı sunar:

Otomatik Keşif (Zamanlanmış)

Belirlediğiniz periyotlarda (günlük veya haftalık) otomatik olarak çalışan keşif görevleri oluşturabilirsiniz. Bu sayede altyapınızdaki yeni sertifikalar sürekli olarak keşfedilir ve envanteriniz güncel kalır.

Manuel Keşif (Anlık)

Zamanlanmış görev oluşturmadan tek seferlik hızlı taramalar yapabilirsiniz. Yeni bir sunucu eklediğinizde veya acil kontrol gerektiğinde kullanışlıdır.

Kullanmaya Başlayın

- **Kullanım Kılavuzu: Keşif** - CA entegrasyonu ve yapılandırma adımları

Sertifika Envanteri

Sertifika Envanteri, tüm sertifikalarınızı merkezi bir yerden görüntülemenizi, yönetmenizi ve organize etmenizi sağlar.

Genel Bakış

Sertifika Envanteri özellikleri:

- Merkezi sertifika kataloğu
- Gelişmiş arama ve filtreleme
- Etiketleme ve gruplama
- Detaylı sertifika bilgileri
- Görselleştirme ve raporlama

Sertifika Envanter Kaynakları

Sertifika Envanteri, farklı kaynaklardan gelen sertifikaları tek bir merkezde toplar ve yönetir. Sisteminiz aşağıdaki kaynaklardan otomatik olarak sertifika keşfi yapar:

Ağ Taraması

Altyapınızda otomatik tarama ile keşfedilen sertifikalar:

- Açık portlar üzerinden erişilebilen TLS/SSL sertifikaları
- Web sunucuları, API gateway'ler, yük dengeleyiciler
- Belirlenen IP aralıkları veya domain'lerde düzenli taramalar
- Belirli port aralıklarında (443, 8443, vb.) otomatik keşif

Sertifika Şeffaflığı Logları Taraması (CT Logs)

Açık sertifika loglarından keşfedilen sertifikalar:

- Organizasyonunuza ait domain'ler için CT log taraması
- Yanlış veya yetkisiz verilen sertifikaların tespiti
- Public CA'lar tarafından verilen tüm sertifikaların izlenmesi

Uygulama Üzerinden İmzalanan Sertifikalar

Platform üzerinde oluşturulan ve imzalanan sertifikalar:

- İmza Talebi (CSR - Certificate Signing Request) ile oluşturulan sertifikalar
- Entegre CA'lar aracılığıyla imzalanan sertifikalar
- Kendinden imzalı (self-signed) sertifikalar
- Internal CA sertifikaları

Import Edilen Sertifikalar

Manuel olarak sisteme eklenen sertifikalar:

- PEM, DER, PFX/P12 formatlarında yüklenen sertifikalar
- Harici sistemlerden aktarılan sertifika zincirleri
- Üçüncü parti CA'lardan alınan sertifikalar

Entegrasyon Sistemlerinden Keşfedilenler

Entegre sistemler üzerinden otomatik olarak keşfedilen sertifikalar:

- **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**

> **ENTEGRASYON EKLEME**
>
> Yeni bir entegrasyon eklemek için Entegrasyonlar sayfasını ziyaret edin ve adım adım kurulum talimatlarını izleyin.

Keşfedilen Sertifikalar Listesi

> **KEŞFEDİLEN SERTİFİKALAR NEDİR?**
>
> Sertifika Keşfi işlemleri sonucunda altyapınızda bulunan tüm sertifikaların detaylı listesidir. Her keşif sonrası bu liste güncellenir ve yeni sertifikalar otomatik olarak eklenir.

Temel Özellikler

Keşfedilen Sertifikalar listesi, sertifika yönetimini kolaylaştıran güçlü özellikler sunar:

Özellik	Açıklama
Detaylı Filtreleme	Her kolon için ayrı arama yapabilme
Özelleştirilebilir Görünüm	Görmek istediğiniz kolonları seçme
Toplu İşlemler	Birden fazla sertifika üzerinde aynı anda işlem yapma
Dışa Aktarma	Seçili sertifikaları farklı formatlarda dışa aktarma
Hızlı Erişim	Son görülme zamanı, port, tip gibi kritik bilgilere anında erişim

Sağladığı Bilgiler

Sertifika envanterinde her sertifika için temel bilgiler liste görünümünde sunulur. Bir sertifikaya tıkladığınızda ise sertifikanın tüm detaylarına erişebilirsiniz.

Liste Görünümünde Görünen Bilgiler

Bilgi	Açıklama
Last Seen	Sertifikanın en son ne zaman görüldüğü
Server	Sertifikanın bulunduğu sunucu adresi
Port	Sertifikanın çalıştığı port numarası
Type	Keşif yöntemi (Ağ Taraması, CT Logları, İçe Aktarma, Entegrasyon, Manuel)
Subject	Sertifika sahibi bilgisi (CN, OU, O)
Not Before	Sertifikanın geçerlilik başlangıç tarihi
Not After	Sertifikanın geçerlilik bitiş tarihi

Detaylı Görünüm

SecTrail CM, sertifikaları parçalayarak tüm bilgileri depolar. Detaylı görünümde X.509 standardındaki tüm alanlar (Subject, Issuer, Serial Number, Public Key, Extensions, Fingerprint, Certificate Chain gibi) ile birlikte keşif kaynağı, ilişkili sistemler ve kullanım geçmişine erişebilirsiniz.

Toplu İşlem Yetenekleri

Liste üzerinden yapılabilecek toplu işlemler:

- [OK] **Durum Değiştirme** - Seçili sertifikaların durumunu toplu güncelleme
- **Dışa Aktarma** - Seçili sertifikaları dışa aktarma (CSV, Excel, PDF)
- **Silme** - Artık kullanılmayan sertifikaları temizleme
- **İmza Talebi Oluşturma** - Yenileme için imza talebi (CSR) oluşturma

Kullanmaya Başlayın

- **Kullanım Kılavuzu: Envanter** - CA entegrasyonu ve yapılandırma adımları

Sertifika İzleme

SecTrail CM, sertifikalarınızı 7/24 kesintisiz izler ve sorunları önceden tespit ederek hizmet kesintilerini önler.

> **NEDEN SERTİFİKA İZLEME ÖNEMLİDİR?**
>
> Süresi dolan bir sertifika, kritik servislerin çökmesine, gelir kaybına ve itibar zedelenmesine neden olabilir. Proaktif izleme ile sorunları önceden tespit edip önleyebilirsiniz.

Genel Bakış

SecTrail CM'in sertifika izleme sistemi, sertifikalarınızın sağlığını sürekli kontrol eder ve kritik durumlar için otomatik alarm oluşturur.

Temel Özellikler

- ⏰ **7/24 İzleme** - Kesintisiz otomatik sertifika durumu kontrolü
- **Proaktif Tespit** - Sorunlar oluşmadan önce erken uyarı
- **Merkezi Dashboard** - Tüm sertifikaların durumunu tek ekrandan görüntüleme
- **Akıllı Alarmlar** - Özelleştirilebilir eşikler ve bildirimler
- **Trend Analizi** - Sertifika yaşam döngüsü ve kullanım istatistikleri

İzleme Metrikleri

SecTrail CM, sertifikalarınız için kapsamlı metrikler toplar ve analiz eder:

Süre Dolumu İzleme

Sertifikaların son kullanma tarihlerini takip ederek zamanında yenileme sağlar:

- **Son Kullanma Tarihi** - Sertifikanın son kullanma tarihi
- **Sona Ermeye Kalan Gün** - Sona ermeye kalan gün sayısı
- **Süre Dolum Durumu** - Geçerli, Yakında Dolacak, Süresi Dolmuş
- **Yenileme Penceresi** - Önerilen yenileme zamanı

> **YENİLEME ÖNERİLERİ**
>
> - 90+ gün: Planlamaya başlayın
> - 30-90 gün: Yenileme sürecini başlatın
> - 7-30 gün: Acil yenileme gerekli
> - 0-7 gün: Kritik durum!

Sertifika Geçerliliği

Sertifikaların teknik geçerliliğini doğrular:

- **İmza Doğrulama** - İmza doğruluğu kontrolü

- **Anahtar Kullanımı** - Anahtar kullanım amacı uygunluğu
- **Genişletilmiş Anahtar Kullanımı** - Genişletilmiş anahtar kullanım kontrolü
- **Temel Kısıtlamalar** - Temel kısıtlamalar doğrulaması

Zincir Doğrulama

Sertifika zincirininin bütünlüğünü kontrol eder:

- **Zincir Bütünlüğü** - Tüm ara sertifikaların varlığı
- **Kök CA Güvenilirliği** - Root CA'nın güvenilir olup olmadığı
- **Zincir Sırası** - Zincir sıralamasının doğruluğu
- **Çapraz İmzalama** - Çapraz imzalama durumu

Güvenlik Skorlaması

Sertifikaların güvenlik seviyesini değerlendirir:

Kriter	Değerlendirme
Anahtar Boyutu	2048+ bit RSA veya 256+ bit ECC önerilir
İmza Algoritması	SHA-256 veya daha güçlü önerilir
TLS Sürümü	TLS 1.2+ önerilir, TLS 1.0/1.1 güvensiz
Şifreleme Paketleri	Güçlü şifreleme paketi kullanımı
Güvenlik Skoru	A+ ile F arası genel güvenlik skoru

GÜVENLİK UYARILARI

- MD5 veya SHA-1 imzalı sertifikalar artık güvensiz kabul edilir
- 1024 bit RSA anahtarlar yetersizdir
- SSL 3.0, TLS 1.0 ve TLS 1.1 protokolleri artık kullanılmamalıdır

Alarm Mekanizması

SecTrail CM, sertifika durumlarını sürekli izleyerek kritik durumlar için otomatik alarm oluşturur.

Alarm Türleri

SecTrail CM, farklı durumlarda farklı alarm seviyeleri oluşturur:

Alarm Seviyesi	Durum	Örnek
Critical	Acil müdahale gerekli	Sertifika süresi dolmuş veya 7 gün içinde dolacak
Warning	Dikkat gerekli	7-30 gün içinde sona erecek sertifika
Info	Bilgilendirme	30-90 gün içinde sona erecek sertifika
OK	Sorun yok	Sertifika geçerli ve sağlıklı

Alarm Tetikleyicileri

Aşağıdaki durumlar alarm oluşturur:

- ⏰ **Süre Dolumu Yaklaşıyor** - Belirlenen eşik değerine göre
- **Güvenlik Sorunu -** Zayıf algoritma veya anahtar boyutu

Bildirim Kanalları

> **ÇOKLU BİLDİRİM KANALLARI**
>
> Alarm durumuna geçmiş sertifikalar için birden fazla bildirim kanalını aynı anda kullanabilirsiniz.

SecTrail CM, aşağıdaki bildirim kanallarını destekler:

E-posta Bildirimleri

En yaygın kullanılan bildirim yöntemi:

- İlgili ekiplere veya kullanıcılara otomatik mail gönderimi
- Doğrudan askıya alma linkleri
- Grup veya bireysel bildirimler
- Özelleştirilebilir e-posta şablonları

SNMP Trap

Kurumsal izleme sistemleri için:

- Merkezi izleme sistemlerine entegrasyon
- SNMPv2c ve SNMPv3 desteği
- Özelleştirilebilir trap mesajları

Sahiplik Yönetimi

> **AKILLI ALARM YÖNLENDİRME**
>
> Alarmların doğru kişi ve ekiplere ulaşması için esnek sahiplik modeli kullanabilirsiniz.

SecTrail CM, iki seviyeli sahiplik modeli sunar:

Sunucu Bazlı Sahiplik

Sunucu seviyesinde sorumluluk ataması:

Avantajlar:

- Tek bir sunucudaki tüm sertifikalar aynı ekibe yönlendirilir
- Altyapı sorumluluğuna göre organizasyon
- Kolay toplu yönetim

Sertifika Bazlı Sahiplik

Her sertifika için özel sahip tanımlama:

Avantajlar:

- Granular kontrol ve sorumluluk
- Domain bazlı organizasyon
- Özel uygulama sahiplikleri

Sahiplik Önceliği

Sahiplik çakışması durumunda öncelik sırası:

1. **Sertifika Bazlı Sahiplik**
2. **Sunucu Bazlı Sahiplik**
3. **Varsayılan Sahiplik**

> **EN İYİ UYGULAMA**
>
> Kritik sertifikalar için hem sertifika bazlı hem de sunucu bazlı sahiplik tanımlayarak çift katmanlı bildirim sağlayabilirsiniz.

Raporlama ve Analiz

İzleme Raporları

SecTrail CM, düzenli izleme raporları oluşturur:

- **Günlük Durum Raporu** - Her gün sertifika durumu özeti
- **Haftalık Trend Analizi** - Haftalık değişiklikler ve trendler
- **Aylık Compliance Raporu** - Uyumluluk ve güvenlik durumu
- **Özel Raporlar** - İhtiyaca göre özelleştirilmiş raporlar

Dashboard ve Görselleştirme

- **Gerçek Zamanlı Dashboard** - Anlık sertifika durumu
- **Sona Erme Zaman Çizelgesi** - Sona erme takvimi görünümü
- **Alarm Geçmişi** - Geçmiş alarmlar ve müdahaleler

Kullanmaya Başlayın

- **Kullanım Kılavuzu: İzleme** - CA entegrasyonu ve yapılandırma adımları

Sertifika Otoritesi (CA)

SecTrail CM, kuruluşunuzun Certificate Authority (CA) altyapısını merkezi olarak yönetmenizi sağlar.

> **CA YÖNETİMİ NEDEN ÖNEMLİDİR?**
>
> Modern kuruluşlar hem dahili hem de harici CA'ler kullanır. Farklı sistemlerde dağınık CA yönetimi, güvenlik açıkları ve operasyonel karmaşıklık yaratır. SecTrail CM, tüm CA'lerinizi tek bir platformdan yönetmenize olanak tanır.

Temel Özellikler

SecTrail CM'in CA yönetimi özellikleri şunları içerir:

Çoklu CA Yönetimi

Farklı CA sağlayıcılarını tek bir platformdan yönetin:

- **Lokal CA** - Kurum içi sertifika ihtiyaçları için (ADCS, HashiCorp Vault)
- **Harici CA** - İnternet'e açık sistemler için güvenilir sertifikalar (DigiCert, GlobalSign)
- **Hybrid Ortamlar** - Birden fazla CA'yı aynı anda kullanma imkanı
- **Merkezi Kontrol** - Tüm CA'leri tek bir arayüzden yönetme

Sertifika İstek Yönetimi

Sertifika talep süreçlerini otomatikleştirin:

- **İmza Talebi Oluşturma (CSR)** - Otomatik sertifika imza talebi üretimi
- **Şablon Desteği** - Standart sertifika profilleri oluşturma
- **Toplu İşlemler** - Birden fazla sertifikayı aynı anda talep etme
- **Onay Süreçleri** - İş akışı bazlı sertifika onaylama mekanizması

Otomatik Yaşam Döngüsü Yönetimi

Sertifikalarınızı otomatik olarak yönetin:

Otomatik Yenileme Süresi dolmadan sertifikaları otomatik yenileme. Sistem, belirlediğiniz eşik değerlere göre yenileme işlemlerini otomatik olarak başlatır.

Esnek Eşikler Yenileme zamanlamasını özelleştirme imkanı. Her sertifika tipi veya ortam için farklı yenileme politikaları tanımlayabilirsiniz.

Akıllı Bildirimler Kritik olaylarda otomatik uyarı alma. Yenileme başarısızlıkları, yaklaşan süre dolumları ve diğer önemli durumlar için anlık bildirimler.

Kesintisiz Geçiş Zero-downtime sertifika güncellemeleri. Üretim ortamlarınızda kesinti yaşamadan sertifika yenileme işlemlerini gerçekleştirin.

Güvenli Anahtar Yönetimi

Özel anahtarlarınızı (private key) güvenle saklayın:

- **Donanım Güvenlik Modülü Desteği (HSM)** - Donanım güvenlik modülü entegrasyonu ile en yüksek güvenlik seviyesi
- **Şifreli Depolama** - Beklemede ve iletimde şifreleme ile kapsamlı veri koruması
- **Anahtar Rotasyonu** - Periyodik anahtar yenileme ile güvenlik standartlarını koruma
- **Erişim Kontrolü** - Rol bazlı anahtar erişimi ile yetkisiz kullanımı engelleme

Merkezi İzleme ve Raporlama

Tüm CA işlemlerini takip edin:

- **Detaylı Denetim Günlüğü (Audit Log)** - Her işlemin kayıt altına alınması ve geçmiş takibi
- **Performans Metrikleri** - CA kullanım istatistikleri ve analizleri
- **Alarm ve Bildirimler** - Anormal durumlar için otomatik uyarılar

Desteklenen CA Sağlayıcıları

GENİŞ CA DESTEĞİ

SecTrail CM, endüstri standardı CA sistemleri ile entegre çalışır. İster kurumsal, ister public, ister ACME protokollü CA kullanın - hepsini tek platformdan yönetin.

Kategori	CA Sağlayıcısı	Kullanım Alanı	Temel Özellikler
** Kurumsal CA**	Microsoft AD CS	Enterprise Windows PKI	Windows entegrasyonu, şablon desteği, auto-enrollment
	HashiCorp Vault PKI	Cloud-native & DevOps	Dynamic secrets, short-lived sertifikalar, Kubernetes desteği
** Harici CA**	DigiCert	Public SSL/TLS sertifikaları	OV/EV/DV sertifikalar, CertCentral API, IoT/code signing
	GlobalSign	Uluslararası güvenilir CA	SSL/TLS, code signing, Atlas Platform entegrasyonu
** ACME CA**	Let's Encrypt	Ücretsiz otomatik SSL	Domain doğrulama, wildcard desteği, 90 günlük otomatik yenileme
	ZeroSSL	Let's Encrypt alternatifi	Ücretsiz SSL, otomatik doğrulama
	Buypass	Ücretsiz CA seçeneği	ACME protokolü, Norveç merkezli güvenilir CA
	Google Trust Services	GCP optimize	Google Cloud Platform için optimize edilmiş
	SSL.com	ACME ticari CA	Çeşitli sertifika tipleri, ACME desteği

Güvenlik ve Uyumluluk

GÜVENLİK VE UYUMLULUK

SecTrail CM, sertifika yönetiminde en yüksek güvenlik ve uyumluluk standartlarını destekler.

Entegrasyon ve Otomasyon

API VE OTOMASYON

SecTrail CM'in güçlü API'si ile tüm CA işlemlerinizi otomatikleştirebilir, DevOps süreçlerinize entegre edebilirsiniz.

API Özellikleri

SecTrail CM, CA yönetimi için kapsamlı API desteği sunar.

Otomasyon Senaryoları

- **Otomatik Sertifika Talep** - İmza talebi (CSR) oluşturma ve CA'ya gönderme
- **Otomatik Yenileme** - Süresi dolmadan sertifika yenileme
- **Otomatik Dağıtım** - Yeni sertifikaların otomatik dağıtımı
- **Otomatik İptal** - Gerektiğinde sertifika iptali
- **Otomatik İzleme** - Sertifika durumlarının izlenmesi

Kullanmaya Başlayın

- **Kullanım Kılavuzu: CA Yönetimi** - CA entegrasyonu ve yapılandırma adımları

Sistem Entegrasyonları

SecTrail CM, kurumsal altyapınızdaki kritik sistemlerle doğrudan entegre olarak sertifika yönetimini otomatikleştirir.

> **NEDEN SİSTEM ENTEGRASYONU ÖNEMLİDİR?**
>
> Manuel sertifika dağıtımı zaman alıcı, hata eğilimli ve risklidir. Otomatik entegrasyonlar sayesinde sertifika değişimi süreçleri insan müdahalesi olmadan güvenli ve hızlı bir şekilde gerçekleştirilir.

Genel Bakış

SecTrail CM'in Sistem Entegrasyonları modülü, sertifika yaşam döngüsü yönetiminin en kritik aşamalarından biri olan **sertifika dağıtımı ve değişimi** süreçlerini otomatikleştirir. Platform, hedef sistemlere **ajansız** bağlantı kurarak sertifikaların güvenli bir şekilde güncellenmesini sağlar.

Temel Özellikler

Özellik	Açıklama
Otomatik Dağıtım	Yenilenen sertifikalar otomatik olarak ilgili sistemlere dağıtılır
Ajansız Mimari	Hedef sistemlere ajan kurulumu gerektirmeden entegrasyon
Güvenli İletişim	SSH, HTTPS, WinRM gibi güvenli protokoller üzerinden bağlantı
⏮ Geri Alma Desteği	Hata durumunda önceki sertifikaya otomatik geri dönme
Çoklu Platform	Yük dengeleyici, güvenlik duvarı, web sunucu ve uygulama sunucusu desteği

Desteklenen Entegrasyonlar

SecTrail CM, sektördeki önde gelen yük dengeleyici, güvenlik duvarı, web sunucu ve uygulama sunucusu platformları ile entegre çalışır.

Yük Dengeleyici ve Uygulama Dağıtım Kontrolcüsü (ADC)

Platform	Kullanım Alanları
F5 BIG-IP	Yük dengeleme, SSL boşaltma, yüksek erişilebilirlik
Citrix NetScaler (ADC)	Uygulama dağıtımı, uzaktan erişim ağ geçidi, SSL boşaltma

Güvenlik Duvarı ve Güvenlik

Platform	Kullanım Alanları
Palo Alto Networks	SSL inspection, forward proxy, GlobalProtect
Fortinet FortiWeb	Web application firewall, OWASP koruma

Web Sunucuları

Platform	Kullanım Alanları
NGINX	Reverse proxy, API gateway, microservices
Apache HTTP Server	Geleneksel web sunucu, PHP uygulamaları
IIS	Windows ortamları, ASP.NET, SharePoint

Uygulama Sunucusu

Platform	Kullanım Alanları
Apache Tomcat	Java web uygulamaları, Spring Boot
Java Keystore (JKS)	Java uygulamaları, Kafka, Elasticsearch

Certificate Store

Platform	Kullanım Alanları
Windows Certificate Store	Windows sunucular, domain ortamları, Active Directory

Otomatik Sertifika Değişimi Süreci

SecTrail CM, sertifika değişim sürecini tamamen otomatikleştirir ve her adımda **hata kontrolü** ile **geri alma desteği** sağlar:

Adım	Aşama	İşlem	Hata Durumunda
1⃣	**Bağlantı**	Hedef sisteme güvenli bağlantı (SSH/WinRM/API) ve erişim kontrolü	[!] **İşlem iptal**, bildirim gönder
2⃣	**Yedekleme**	Mevcut sertifikanın yedeği alınır (certificate + key + config)	[!] **İşlem durdur**, güvenli çıkış
3⃣	**Dağıtım**	Yeni sertifika dosyalarının hedef sisteme güvenli transferi	**Eski sertifika geri yükle**
4⃣	**Yapılandırma**	Sertifika yapılandırma güncellemesi	**Yedekten geri yükle**
5⃣	**Servis Güncelleme**	Servis yenilenmesi	**Eski sertifika ile geri başlat**
6⃣	**[x] Doğrulama**	SSL/TLS bağlantı ve erişilebilirlik testi	**Tam geri alma**
7⃣	**Bildirim**	Başarı/hata durumu raporlama, denetim günlüğü kaydı, dashboard güncelleme	[OK] **Geri alma bildirimi gönderilir**

OTOMATİK GERİ ALMA GARANTİSİ

Her adımda hata tespit edilirse, sistem otomatik olarak önceki çalışan duruma geri döner. Eski sertifika korunur ve servis kesintisi yaşanmaz.

Entegrasyon Avantajları

Operasyonel Verimlilik

Avantaj	Açıklama
⏱ **Zaman Tasarrufu**	Manuel işlemleri otomatikleştirerek saatler yerine dakikalar
Hata Minimizasyonu	İnsan hatalarını ortadan kaldırarak %99.9+ başarı oranı
7/24 Çalışma	İş saatleri dışında da otomatik sertifika yenileme
Ölçeklenebilirlik	Yüzlerce sistem için eşzamanlı sertifika dağıtımı

Güvenlik

Avantaj	Açıklama
⏰ **Zamanında Yenileme**	Süresi dolmuş sertifika riskini ortadan kaldırma
Merkezi Kontrol	Tüm sertifikaların tek noktadan yönetimi
Güvenli İletişim	SSH, TLS, WinRM gibi güvenli protokoller
Denetim İzi	Her işlemin detaylı kayıt altına alınması

Kullanmaya Başlayın

- **Kullanım Kılavuzu: CA Yönetimi** - CA entegrasyonu ve yapılandırma adımları

Sertifika İş Akışı

SecTrail CM'in Sertifika İş Akışı modülü, sertifika yaşam döngüsünü baştan sona otomatize ederek manuel müdahaleyi minimuma indirir.

> **NEDEN İŞ AKIŞI OTOMASYONU ÖNEMLİDİR?**
>
> Manuel sertifika yenileme ve dağıtım süreçleri, unutulan yenileme tarihleri, kesinti riski ve operasyonel yük oluşturur. Otomatik iş akışları sayesinde sertifikalar süre dolmadan yenilenir ve sistemlere kesintisiz dağıtılır.

Genel Bakış

SecTrail CM'in İş Akışı modülü, sertifikaların **otomatik yenilenmesi**, **onaylanması** ve **hedef sistemlere dağıtılması** süreçlerini yönetir. Keşfedilen her sertifika için özelleştirilebilir iş akışı tanımlanabilir ve tüm süreç baştan sona otomatize edilebilir.

Otomatik İş Akışı Süreci

```
┌─────────────────────────────────────────┐
│ Sertifika İş Akışı Senaryosu │
└─────────────────────────────────────────┘

 Sertifika Tespiti
 v
 ⏰ Yenileme Zamanı (30 gün kala)
 v
 CA Belirleme
 v
 [OK] Onay Süreci
 v
 Yeni Sertifika Alma
 v
 Hedef Sistemlere Kurulum
 v
 [x] Test ve Bildirim
```

SecTrail CM, sertifika yenileme sürecini tamamen otomatikleştirir ve her adımı kayıt altına alır:

Aşama	Açıklama
Keşif ve İzleme	Sertifika Keşfi modülü ile tespit edilen sertifikalar sürekli izlenir
⏰ **Otomatik Tetikleme**	Belirlenen eşik değerlere göre iş akışı başlatılır
Otorite Seçimi	Mevcut otorite veya politikalara göre CA seçimi ve entegrasyon durumu kontrolü
[OK] **Onay Mekanizması**	İsteğe bağlı manuel kontrol noktası (production için önerilir)
Sertifika Talebi	CA ile otomatik iletişim ve sertifika alımı
Otomatik Dağıtım	Hedef sistemlere dağıtım (web sunucuları, yük dengeleyiciler, güvenlik duvarları, cloud platformları)
[x] **Doğrulama & Bildirim**	SSL/TLS testleri, erişilebilirlik kontrolü ve raporlama

GERİ ALMA DESTEĞİ

Her adımda hata kontrolü yapılır ve gerekirse otomatik geri alma işlemi gerçekleştirilir.

İş Akışı Avantajları

Operasyonel Verimlilik

Avantaj	Açıklama
⏱ **Zaman Tasarrufu**	Manuel süreçleri otomatikleştirerek işgücü maliyetini azaltma
Hata Minimizasyonu	İnsan hatalarını ortadan kaldırarak %99.9+ başarı oranı
7/24 Otomatik İşlem	İş saatleri dışında da kesintisiz sertifika yönetimi
Ölçeklenebilirlik	Yüzlerce sertifika için eşzamanlı iş akışı yönetimi

Güvenlik ve Uyumluluk

Avantaj	Açıklama
⏰ **Zamanında Yenileme**	Süresi dolmuş sertifika riskini tamamen ortadan kaldırma
Tam Denetim İzi	Her işlemin detaylı kayıt altına alınması
Merkezi Kontrol	Tüm iş akışlarının tek noktadan yönetimi

İş Akışı Yapılandırması

SecTrail CM, farklı sertifika grupları için özelleştirilmiş iş akışı şablonları oluşturmanıza olanak tanır:

- **Yenileme Eşikleri**: Sertifika tipine göre özel tetikleme süreleri
- **Onay Kuralları**: Kritik sistemler için çok katmanlı onay mekanizmaları
- **Dağıtım Hedefleri**: Otomatik dağıtım yapılacak sistem grupları

- **Bildirim Ayarları**: E-posta, SNMP Trap
- **Geri Alma Politikaları**: Hata durumunda otomatik veya manuel geri alma

Kullanmaya Başlayın

- **Kullanım Kılavuzu: İş Akışı** - CA entegrasyonu ve yapılandırma adımları

RBAC ve Yetkilendirme

SecTrail CM, kurumsal düzeyde **rol tabanlı erişim kontrolü (RBAC - Role-Based Access Control)** ile güvenli ve esnek bir yetkilendirme sistemi sunar. Kullanıcı yönetiminden izin kontrolüne kadar tüm güvenlik katmanlarını merkezi olarak yönetin.

NEDEN RBAC?

Sertifika yönetimi hassas bir işlemdir. Yanlış kişilerin kritik işlemleri gerçekleştirmesi, güvenlik ihlallerine yol açabilir. RBAC ile her kullanıcının sadece görevine uygun yetkilere sahip olmasını sağlarsınız.

TEMEL PRENSİPLER

- **En Az Yetki -** Kullanıcılara sadece ihtiyaç duydukları minimum yetkiler verilir
- **Görev Ayrımı -** Kritik işlemler farklı roller arasında bölüştürülür
- **Katmanlı Savunma -** Çok katmanlı güvenlik kontrolü sağlanır

Temel Özellikler

Esnek Kullanıcı Yönetimi

SecTrail CM, farklı kurumsal ihtiyaçlara yanıt verebilecek şekilde çoklu kullanıcı kaynağını destekler:

Active Directory (AD) / LDAP Entegrasyonu

Mevcut kurumsal kimlik altyapınızı kullanın:

- **Otomatik Senkronizasyon** - Kullanıcı bilgileri otomatik güncellenir
- **Grup Bazlı Yönetim** - AD gruplarını doğrudan roller ile eşleştirin
- **Merkezi Kullanıcı Yönetimi** - Kullanıcı ekleme/çıkarma AD'de yapılır

Lokal Kullanıcı Hesapları

Bağımsız kullanıcı yönetimi:

- Harici danışmanlar ve geçici kullanıcılar için
- AD erişimi olmayan kullanıcılar için alternatif
- Özelleştirilebilir parola politikaları
- Manuel kullanıcı oluşturma ve yönetim

Hibrit Yönetim

Her iki yöntemi aynı anda kullanabilirsiniz. Örneğin, çalışanlar AD ile giriş yaparken, dış danışmanlar lokal hesap kullanabilir.

Rol Tabanlı Erişim Kontrolü (RBAC)

Güçlü ve esnek rol yönetimi sistemi:

Hiyerarşik Rol Yapısı

- **Sistem Rolleri** - Değiştirilemeyen önceden tanımlı roller
- **Özel Roller** - Kuruluşunuza özel roller oluşturun
- **Rol Kalıtımı** - Rollerin birbirinden izin alması

Granüler İzin Kontrolü

Her işlem için ayrı izin tanımı (CRUD + Execute modeli):

İzin	Açıklama	Örnek
Oluşturma	Yeni kaynak ekleme	Yeni sertifika talebi oluşturma
Okuma	Bilgileri görüntüleme	Sertifika detaylarını görme
Güncelleme	Mevcut kaynağı değiştirme	Sertifika bilgilerini güncelleme
Silme	Kaynağı kaldırma	Sertifika veya CA silme
Çalıştırma	İşlem tetikleme	Sertifika yenileme, dağıtım

Organizasyon ve Grup Yönetimi

Kullanıcı Grupları

Kullanıcıları organize edin:

- **Departman Bazlı** - IT, DevOps, Security, Network ekipleri
- **Proje Bazlı** - Belirli projelere ait ekipler
- **Bölge/Lokasyon Bazlı** - İstanbul, Ankara, İzmir ofisleri
- **Toplu Rol Ataması** - Gruplara otomatik rol dağıtımı

Dinamik Üyelik

Otomatik grup üyeliği yönetimi:

- **AD Grup Senkronizasyonu** - Active Directory grupları otomatik senkronize edilir
- **Kural Bazlı Atama** - Kullanıcı özelliklerine göre otomatik grup üyeliği
- **Özellik Filtreleme** - Departman, unvan, lokasyon gibi özelliklere göre filtreleme

Detaylı Audit ve İzleme

Tüm yetkilendirme işlemlerini kayıt altına alın ve uyumluluk gereksinimlerini karşılayın:

Kullanıcı Aktivite Günlüğü

Tüm kullanıcı etkileşimlerini izleyin:

- [OK] Kimler ne zaman sisteme giriş yaptı?
- [OK] Hangi işlemler gerçekleştirildi?
- [OK] Hangi kaynaklara erişildi?
- [OK] Başarısız giriş denemeleri
- [OK] IP adresi ve kullanıcı aracısı bilgileri

Rol ve İzin Değişiklikleri

Yetkilendirme değişikliklerini takip edin:

- **Rol Atama/Kaldırma** - Kim, kime, ne zaman rol atadı/kaldırdı?
- **İzin Değişiklikleri** - Hangi izinler eklendi/kaldırıldı?
- **Grup Üyelik Değişiklikleri** - Grup üyeliklerinin tam geçmişi
- **Değişiklik Yapan Bilgisi** - Her değişikliği yapan kişi kaydedilir

Uyumluluk Raporları

Denetim ve uyumluluk raporları:

- **Kullanıcı Erişim Hakları** - Her kullanıcının sahip olduğu izinlerin raporu
- **Aktif/Pasif Kullanıcı Listesi** - Kullanım durumuna göre kullanıcı analizi
- **Son Giriş Zamanları** - Kullanıcı aktivite takibi
- **Yetki Değişiklik Geçmişi** - Belirli tarih aralığında yapılan değişiklikler
- **Ayrıcalıklı Kullanıcı Raporu** - Yüksek yetkili kullanıcıların listesi

---

Önceden Tanımlı Roller

SecTrail CM, hızlı kurulum için hazır roller sunar:

Rol	Açıklama	Temel İzinler	Kullanım Senaryosu
Admin	Tüm yetkilere sahip sistem yöneticisi	- Tüm modüller: tam erişim - Kullanıcı yönetimi - Sistem ayarları - Rol tanımlama	Sistem yöneticileri ve IT liderleri için
API	API erişimi için sistem kullanıcısı	- Sertifikalar: okuma, çalıştırma - Entegrasyonlar: çalıştırma - API: tam erişim	Otomasyon ve entegrasyon sistemleri için

> **ÖZEL ROL TANIMLAMA**
>
> Bu roller temel ihtiyaçları karşılar. Kuruluşunuzun özel gereksinimlerine göre yeni roller oluşturabilir veya mevcut rolleri klonlayarak özelleştirebilirsiniz.

Kullanım Senaryoları

Senaryo 1: Departman Bazlı Erişim

Durum: IT departmanı tüm sertifikaları yönetirken, DevOps ekibi sadece kendi projelerine ait sertifikaları görür ve yenileyebilir.

Çözüm:

- IT ekibine `Certificate Manager` rolü atanır
- DevOps ekibine özel `DevOps Certificate Operator` rolü oluşturulur
- Proje bazlı tag'ler ile erişim kısıtlanır

```
Roller:
├── IT Team -> Certificate Manager (tüm sertifikalar)
└── DevOps Team -> DevOps Certificate Operator (sadece tag:project=devops)
```

[OK] Senaryo 2: Onay Mekanizması

Durum: Junior çalışanlar sertifika talebi oluşturabilir ancak manager onayı olmadan üretim ortamına sertifika deploy edemez.

Çözüm:

- Junior'lara `Certificate Requester` rolü (create, read izinleri)
- Manager'lara `Certificate Approver` rolü (execute, deploy izinleri)
- Workflow sistemi ile onay mekanizması kurulur

```
İş Akışı:
1. Junior -> Sertifika talebi oluşturur (create)
2. Manager -> Talebi inceler ve onaylar (approve)
3. Sistem -> Onaylanan sertifikayı deploy eder (execute)
```

Senaryo 3: Dış Danışman Erişimi

Durum: Geçici çalışan danışmanlara sınırlı süreli ve belirli sertifikalar için salt okunur erişim verilebilir.

Çözüm:

- Lokal kullanıcı hesabı oluşturulur (AD dışı)
- `External Auditor` rolü atanır (sadece read izinleri)
- Hesap sona erme tarihi belirlenir
- Belirli sertifika gruplarına erişim kısıtlanır

```
Danışman Profili:
├── Kullanıcı Tipi: Lokal (AD dışı)
├── Rol: Certificate Viewer (read-only)
├── Erişim Süresi: 90 gün
└── Kısıtlama: Sadece "Production-Web" sertifikaları
```

Senaryo 4: Multi-Tenant Yapı

Durum: Farklı şirket veya iş birimleri aynı platformu kullanabilir, ancak birbirlerinin verilerine erişemez.

Çözüm:

- Her şirket/birim için ayrı organizasyon tanımlanır
- Organizasyon bazlı veri izolasyonu sağlanır
- Kullanıcılar sadece kendi organizasyonlarının verilerine erişir

```
Organizasyon Yapısı:
├── 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
```

DAHA FAZLA BİLGİ

Kullanıcı yönetimi ve rol yapılandırması için Kullanım Kılavuzu: RBAC Yönetimi sayfasını inceleyin.

Giriş

SecTrail CM, sertifika yaşam döngüsünün her aşamasını otomatikleştirmek için iki temel entegrasyon kategorisi sunar: **Sertifika Otoriteleri (CA)** ile entegrasyon ve **Sistem Entegrasyonları**.

Entegrasyon Tipleri

Sertifika Otoritesi (CA) Entegrasyonları

CA entegrasyonları, sertifika **edinme** ve **yenileme** süreçlerini otomatikleştirir. SecTrail CM, hem genel (public) hem de özel (private) sertifika otoriteleri ile entegre çalışarak sertifika taleplerini, onay süreçlerini ve sertifika alımını tamamen otomatik hale getirir.

Temel Özellikler:

- Otomatik sertifika talebi ve onay süreci
- Otomatik yenileme
- Çoklu CA desteği
- Template-based talep yönetimi
- API-based güvenli iletişim

Desteklenen CA Türleri:

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

Sistem Entegrasyonları

Sistem entegrasyonları, CA'den alınan sertifikaların hedef sistemlere **dağıtımını** ve **yönetimini** otomatikleştirir. Load balancer'lar, firewall'lar, web sunucular ve application server'lara ajansız mimari ile güvenli bağlantı kurarak sertifika değişimini otomatik gerçekleştirir.

Temel Özellikler:

- Ajansız mimari (agent-less architecture)
- Güvenli protokoller (SSH, WinRM, HTTPS API)
- Otomatik rollback desteği
- Dağıtım sonrası doğrulama
- Detaylı audit log

Desteklenen Sistem Kategorileri:

Kategori	Entegrasyonlar
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, GlobalSign ManagedSSL servisi ile entegrasyon sağlayarak SSL/TLS sertifikalarının sipariş edilmesini, yenilenmesini ve iptal edilmesini merkezi olarak yönetmenizi sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	SOAP API (HTTPS)	GlobalSign ManagedSSL API'si kullanılır
API Endpoint	`https://system.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl`	ManagedSSL SOAP servisi
Kimlik Doğrulama	Basic Authentication	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	ManagedSSL API Erişimi	Sertifika sipariş, sorgulama ve yönetim yetkisi

Otomatik İşlemler

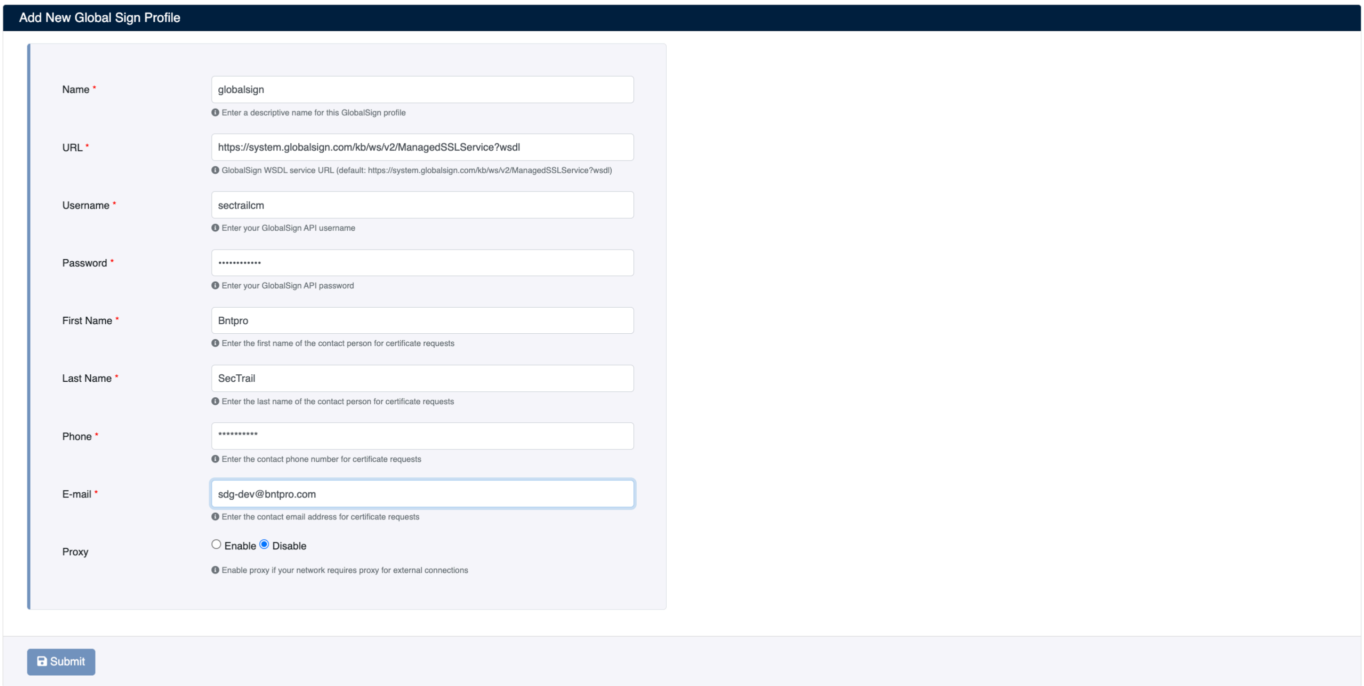
SecTrail CM, GlobalSign üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika Siparişi**: Yeni SSL/TLS sertifikası talebi oluşturma
2. **Sipariş Sorgulama**: Mevcut sertifika siparişlerinin durumunu görüntüleme
3. **Sertifika Yenileme**: Süresi dolmak üzere olan sertifikaların yenilenmesi
4. **Sertifika İptali**: Artık kullanılmayan veya güvenliği tehlikeye girmiş sertifikaların iptal edilmesi

Yapılandırma Adımları

1. GlobalSign Profili Ekleme

Certificate Authorities (CA) > GlobalSign > Accounts bölümüne gidin ve **Add New Global Sign Profile** butonuna tıklayın:



Aşağıdaki bilgileri girin:

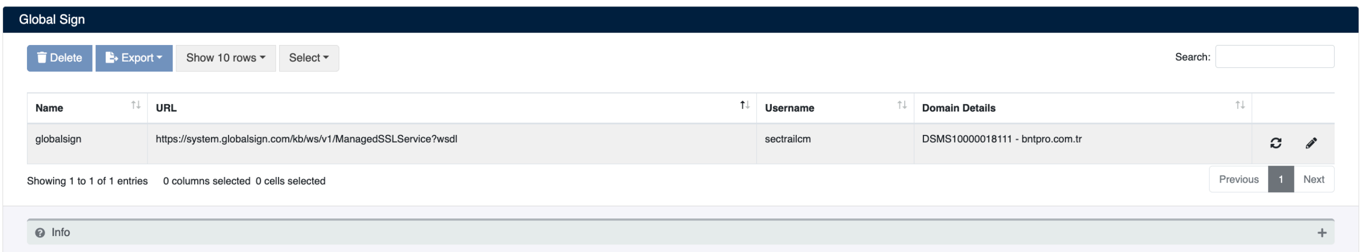
- **Name**: Profil için tanımlayıcı isim verin
- **URL**: GlobalSign ManagedSSL API endpoint adresi
- `https://system.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl`
- **Username**: GlobalSign API kullanıcı adınız
- **Password**: GlobalSign API şifreniz
- **Proxy**: Proxy kullanımı (Etkinleştir/Devre Dışı Bırak). Proxy'yi etkinleştirdikten sonra **Settings -> Proxy** ayarlarından proxy yapılandırmanızı tamamlayın.

Submit butonuna tıklayarak profili kaydedin.

> **İLETİŞİM BİLGİLERİ**
>
> GlobalSign, sertifika işlemleri için belirtilen iletişim bilgilerini kullanacaktır. Bu bilgilerin doğru ve güncel olduğundan emin olun.

2. GlobalSign Hesaplarını Görüntüleme

Profil eklendikten sonra **Certificate Authorities (CA) > GlobalSign > Accounts** listesinde görüntülenecektir:



Liste ekranında aşağıdaki bilgiler gösterilir:

- **Name**: Profil ismi

- **URL**: API endpoint adresi
- **Username**: Kullanıcı adı
- **Domain Details**: İlişkili domain bilgileri

Hesap İşlemleri

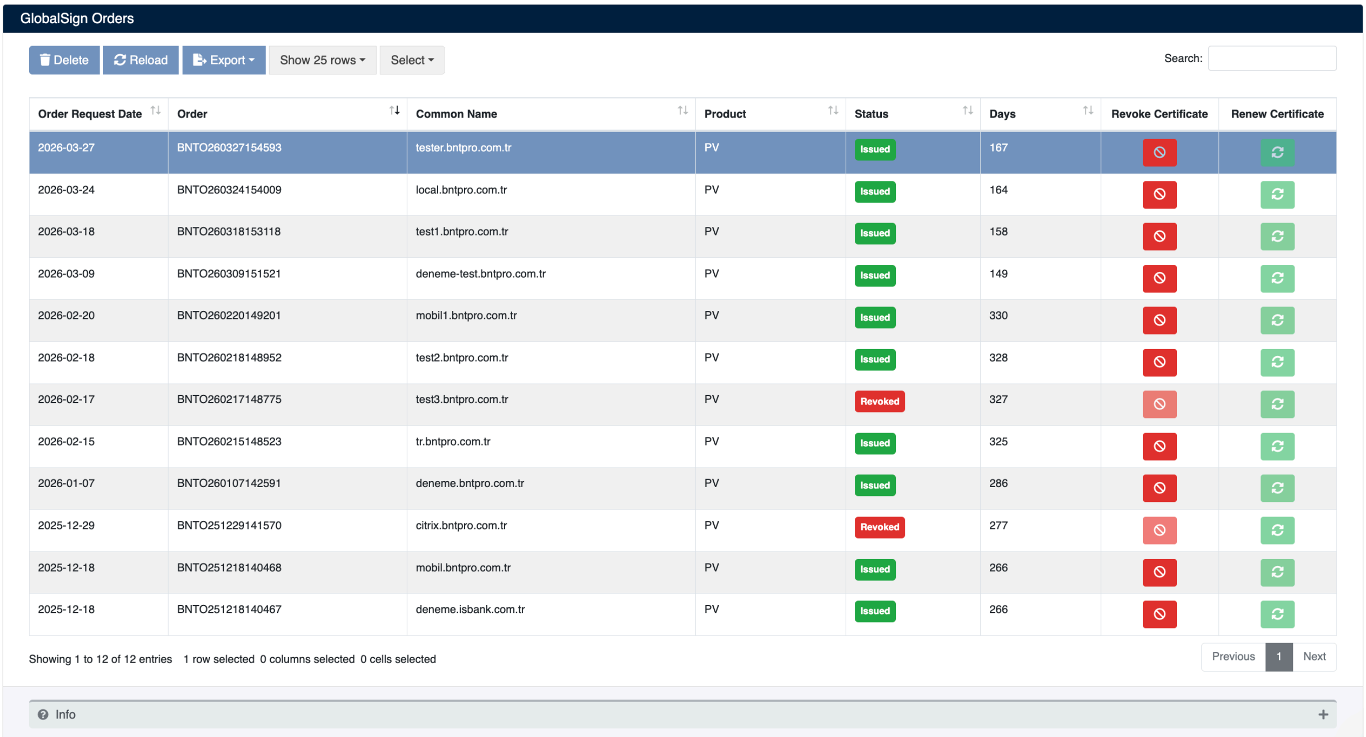
Her profil için aşağıdaki işlemler yapılabilir:

- **Refresh** (): Profil bilgilerini yenile
- **Edit** (): Profil ayarlarını düzenle
- **Delete** (): Profili sil

Sertifika Siparişlerini Görüntüleme

GlobalSign entegrasyonu sonrasında tüm sertifika siparişlerinizi görüntüleyebilirsiniz:

Certificate Authorities (CA) > GlobalSign > Orders bölümüne gidin:



Order Request Date	Order	Common Name	Product	Status	Days	Revoke Certificate	Renew Certificate
2026-03-27	BNTO260327154593	tester.bntpro.com.tr	PV	Issued	167		
2026-03-24	BNTO260324154009	local.bntpro.com.tr	PV	Issued	164		
2026-03-18	BNTO260318153118	test1.bntpro.com.tr	PV	Issued	158		
2026-03-09	BNTO260309151521	deneme-test.bntpro.com.tr	PV	Issued	149		
2026-02-20	BNTO260220149201	mobil1.bntpro.com.tr	PV	Issued	330		
2026-02-18	BNTO260218148952	test2.bntpro.com.tr	PV	Issued	328		
2026-02-17	BNTO260217148775	test3.bntpro.com.tr	PV	Revoked	327		
2026-02-15	BNTO260215148523	tr.bntpro.com.tr	PV	Issued	325		
2026-01-07	BNTO260107142591	deneme.bntpro.com.tr	PV	Issued	286		
2025-12-29	BNTO251229141570	citrix.bntpro.com.tr	PV	Revoked	277		
2025-12-18	BNTO251218140468	mobil.bntpro.com.tr	PV	Issued	266		
2025-12-18	BNTO251218140467	deneme.isbank.com.tr	PV	Issued	266		

Sipariş Bilgileri

Alan	Açıklama
Order Request Date	Sertifika talep tarihi
Order	GlobalSign sipariş numarası
Common Name	Sertifikanın kullanılacağı domain adı
Product	Sertifika ürün tipi
Status	Sertifika durumu (Issued, Pending, vb.)
Days	Kalan geçerlilik süresi (gün)

Sertifika Durumları

- **Issued** : Sertifika başarıyla düzenlenmiş ve aktif
- **Pending** : Sipariş işleniyor
- **Revoked** : Sertifika iptal edilmiş
- **Expired** : Sertifika süresi dolmuş

Sertifika Yönetimi

Sertifika Yenileme (Renew)

Süresi dolmak üzere olan sertifikaları yenilemek için:

1. **Certificate Authorities (CA) > GlobalSign > Orders** bölümüne gidin
2. Yenilemek istediğiniz sertifikayı bulun
3. **Renew Certificate** butonuna (yeşil ikon) tıklayın
4. Yenileme işlemini onaylayın

> **YENİLEME ZAMANLAMASI**
>
> Sertifikaları son kullanma tarihinden en az 30 gün önce yenilemeye başlamanız önerilir.

Sertifika İptali (Revoke)

Güvenliği tehlikeye girmiş veya artık kullanılmayan sertifikaları iptal etmek için:

1. **Certificate Authorities (CA) > GlobalSign > Orders** bölümüne gidin
2. İptal etmek istediğiniz sertifikayı bulun
3. **Revoke Certificate** butonuna (kırmızı ikon) tıklayın
4. İptal işlemini onaylayın

> **İPTAL İŞLEMİ**
>
> Sertifika iptal edildikten sonra bu işlem geri alınamaz. İptal edilen sertifika artık kullanılamaz.

DigiCert

SecTrail CM, DigiCert API servisi ile entegrasyon sağlayarak SSL/TLS sertifikalarının sipariş edilmesini, yenilenmesini ve iptal edilmesini merkezi olarak yönetmenizi sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	REST API (HTTPS)	DigiCert REST API kullanılır
API Endpoint	`https://www.digicert.com/services/v2/`	DigiCert API v2 servisi
Kimlik Doğrulama	API Key Authentication	API Key ile kimlik doğrulama
Kullanıcı Yetkisi	DigiCert API Erişimi	Sertifika sipariş, sorgulama ve yönetim yetkisi

Otomatik İşlemler

SecTrail CM, DigiCert üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika Siparişi**: Yeni SSL/TLS sertifikası talebi oluşturma
2. **Sipariş Sorgulama**: Mevcut sertifika siparişlerinin durumunu görüntüleme
3. **Sertifika Yenileme**: Süresi dolmak üzere olan sertifikaların yenilenmesi
4. **Sertifika İptali**: Artık kullanılmayan veya güvenliği tehlikeye girmiş sertifikaların iptal edilmesi
5. **Sertifika İndirme**: Düzenlenmiş sertifikaların otomatik olarak indirilmesi

Yapılandırma Adımları

1. DigiCert Profili Ekleme

Certificate Authorities (CA) > DigiCert > Accounts bölümüne gidin ve **Add New DigiCert Profile** butonuna tıklayın:

Aşağıdaki bilgileri girin:

- **Name**: Profil için tanımlayıcı isim verin

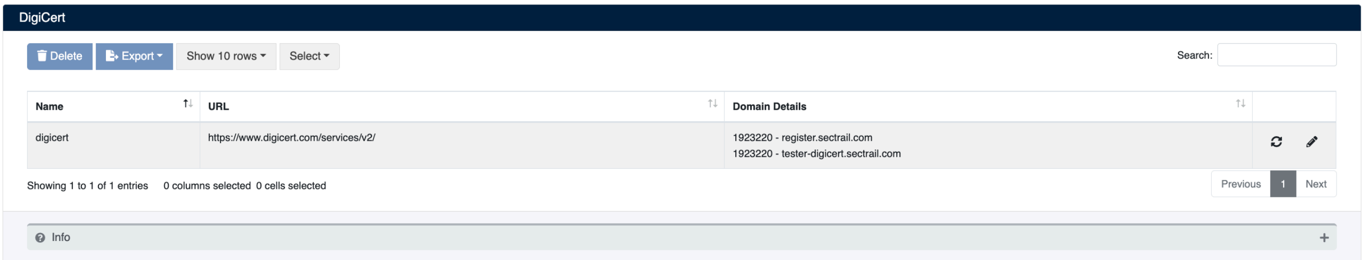
- **URL**: DigiCert API endpoint adresi
- `https://www.digicert.com/services/v2/`
- **API Key**: DigiCert API anahtarınız
- **Proxy**: Proxy kullanımı (Etkinleştir/Devre Dışı Bırak). Proxy'yi etkinleştirdikten sonra **Settings -> Proxy** ayarlarından proxy yapılandırmanızı tamamlayın.

Submit butonuna tıklayarak profili kaydedin.

> **API KEY**
>
> DigiCert API anahtarınızı DigiCert hesap yönetim panelinden oluşturabilirsiniz. API anahtarının yeterli izinlere sahip olduğundan emin olun.

2. DigiCert Hesaplarını Görüntüleme

Profil eklendikten sonra **Certificate Authorities (CA) > DigiCert > Accounts** listesinde görüntülenecektir:



Liste ekranında aşağıdaki bilgiler gösterilir:

- **Name**: Profil ismi
- **URL**: API endpoint adresi
- **Domain Details**: İlişkili domain bilgileri

Hesap İşlemleri

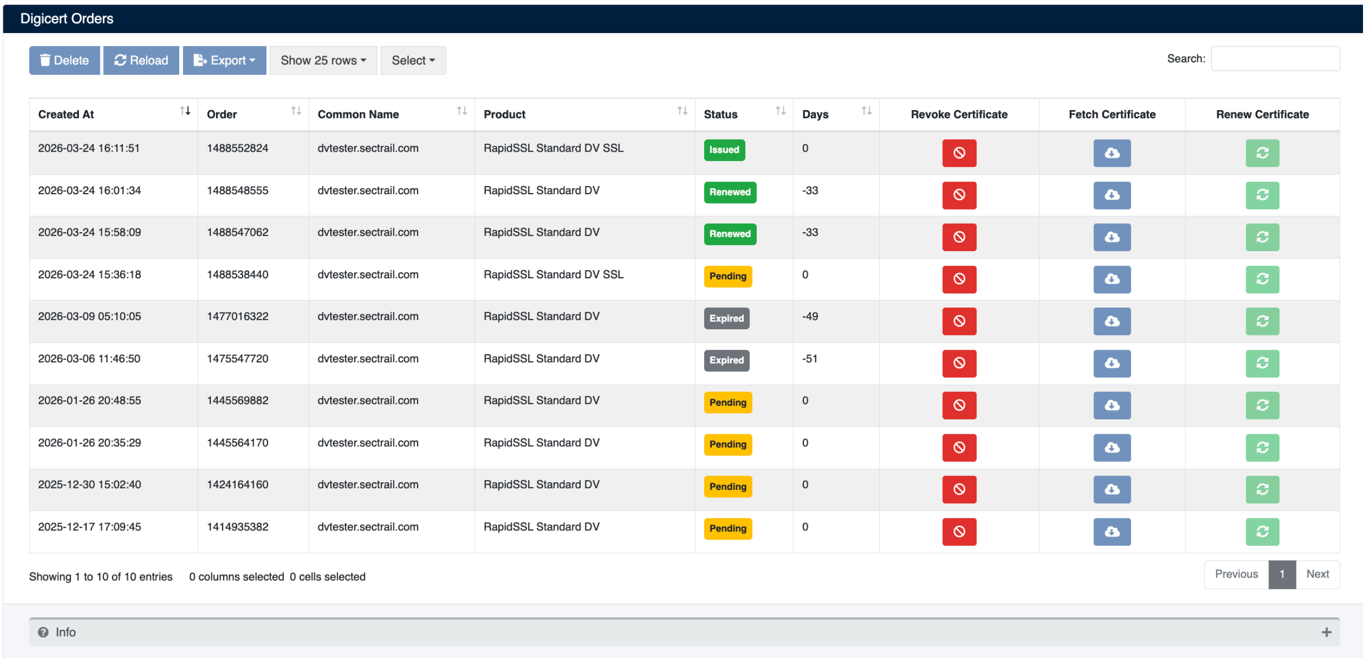
Her profil için aşağıdaki işlemler yapılabilir:

- **Refresh**: Profil bilgilerini yenile
- **Edit**: Profil ayarlarını düzenle
- **Delete**: Profili sil

Sertifika Siparişlerini Görüntüleme

DigiCert entegrasyonu sonrasında tüm sertifika siparişlerinizi görüntüleyebilirsiniz:

Certificate Authorities (CA) > DigiCert > Orders bölümüne gidin:



Digicert Orders

Delete | Reload | Export | Show 25 rows | Select | Search:

Created At	Order	Common Name	Product	Status	Days	Revoke Certificate	Fetch Certificate	Renew Certificate
2026-03-24 16:11:51	1488552824	dvtester.sectrail.com	RapidSSL Standard DV SSL	Issued	0			
2026-03-24 16:01:34	1488548555	dvtester.sectrail.com	RapidSSL Standard DV	Renewed	-33			
2026-03-24 15:58:09	1488547062	dvtester.sectrail.com	RapidSSL Standard DV	Renewed	-33			
2026-03-24 15:36:18	1488538440	dvtester.sectrail.com	RapidSSL Standard DV SSL	Pending	0			
2026-03-09 05:10:05	1477016322	dvtester.sectrail.com	RapidSSL Standard DV	Expired	-49			
2026-03-06 11:46:50	1475547720	dvtester.sectrail.com	RapidSSL Standard DV	Expired	-51			
2026-01-26 20:48:55	1445569882	dvtester.sectrail.com	RapidSSL Standard DV	Pending	0			
2026-01-26 20:35:29	1445564170	dvtester.sectrail.com	RapidSSL Standard DV	Pending	0			
2025-12-30 15:02:40	1424164160	dvtester.sectrail.com	RapidSSL Standard DV	Pending	0			
2025-12-17 17:09:45	1414935382	dvtester.sectrail.com	RapidSSL Standard DV	Pending	0			

Showing 1 to 10 of 10 entries 0 columns selected 0 cells selected

Previous 1 Next

Info

Sipariş Bilgileri

Alan	Açıklama
Created At	Sertifika talep tarihi ve saati
Order	DigiCert sipariş numarası
Common Name	Sertifikanın kullanılacağı domain adı
Product	Sertifika ürün tipi (örn: RapidSSL Standard DV)
Status	Sertifika durumu (Issued, Expired, Renewed, Revoked)
Days	Kalan/geçen geçerlilik süresi (gün cinsinden)

Sertifika Durumları

- **Renewed**: Sertifika yenilenmiş ve aktif
- **Expired**: Sertifika süresi dolmuş (negatif gün değeri)
- **Revoked**: Sertifika iptal edilmiş
- **Issued**: Sertifika başarıyla düzenlenmiş ve aktif

Sertifika Yönetimi

Sertifika İndirme (Fetch)

Düzenlenmiş sertifikaları indirmek için:

1. **Certificate Authorities (CA) > DigiCert > Orders** bölümüne gidin
2. İndirmek istediğiniz sertifikayı bulun
3. **Fetch Certificate** butonuna tıklayın
4. Sertifika otomatik olarak indirilir ve sisteme eklenir

OTOMATİK İNDİRME

DigiCert'ten düzenlenen sertifikalar otomatik olarak sisteme indirilebilir. Bu özellik sayesinde manuel indirme işlemine gerek kalmaz.

Sertifika Yenileme (Renew)

Süresi dolmak üzere olan sertifikaları yenilemek için:

1. **Certificate Authorities (CA) > DigiCert > Orders** bölümüne gidin
2. Yenilemek istediğiniz sertifikayı bulun
3. **Renew Certificate** butonuna tıklayın
4. Yenileme işlemini onaylayın

YENİLEME ZAMANLAMASI

Sertifikaları son kullanma tarihinden en az 30 gün önce yenilemeye başlamanız önerilir. "Days" sütununda negatif değerler süresi dolmuş sertifikaları gösterir.

Sertifika İptali (Revoke)

Güvenliği tehlikeye girmiş veya artık kullanılmayan sertifikaları iptal etmek için:

1. **Certificate Authorities (CA) > DigiCert > Orders** bölümüne gidin
2. İptal etmek istediğiniz sertifikayı bulun
3. **Revoke Certificate** butonuna tıklayın
4. İptal işlemini onaylayın

İPTAL İŞLEMİ

Sertifika iptal edildikten sonra bu işlem geri alınamaz. İptal edilen sertifika artık kullanılamaz.

Microsoft ADCS

SecTrail CM, Microsoft Active Directory Certificate Services (ADCS - Sertifika Hizmetleri) ile entegrasyon sağlayarak kurumsal SSL/TLS sertifikalarının otomatik olarak talep edilmesini ve yönetilmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	HTTPS	Sertifika Kayıt Web Servisi kullanılır
Port	`443` (varsayılan)	Standart HTTPS portu
Kimlik Doğrulama	NTLM / Kerberos kimlik doğrulama	Windows kimlik doğrulama
Kullanıcı Yetkisi	Sertifika talep ve kayıt	Sertifika talep ve kayıt yetkisi

Otomatik İşlemler

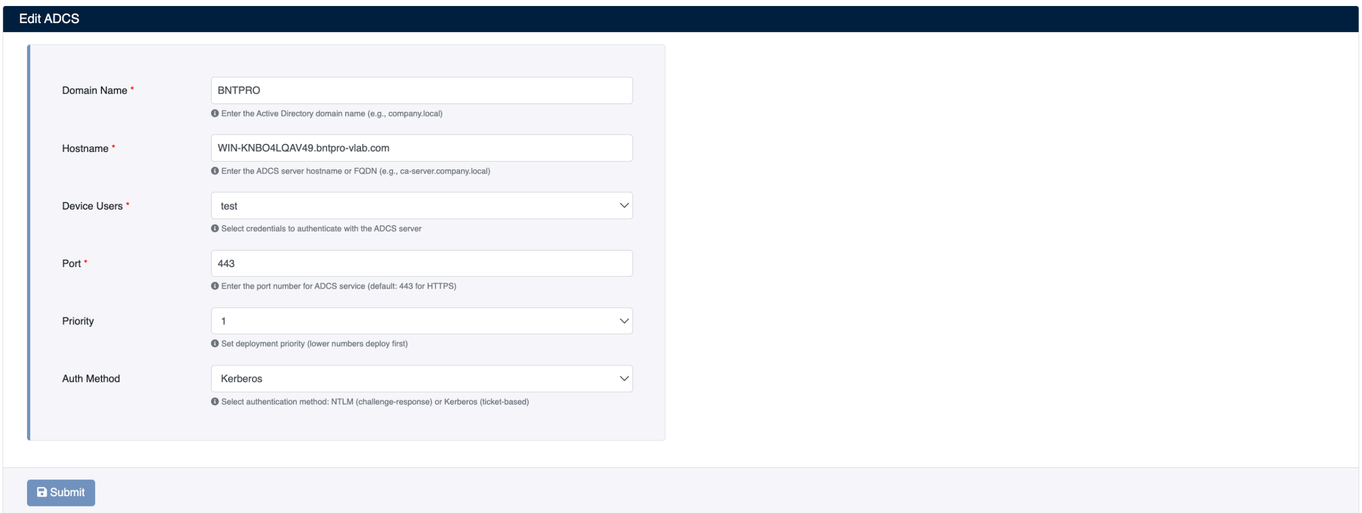
SecTrail CM, Microsoft ADCS üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika Talebi**: CSR gönderimi
2. **Sertifika Kayıt**: ADCS üzerinden sertifika düzenleme
3. **Şablon Yönetimi**: Farklı sertifika şablonlarını kullanma
4. **Otomatik Onay**: Yapılandırılmış şablonlar için otomatik onay
5. **Bekleyen Sipariş Takibi**: CA yöneticisi onayı bekleyen sertifika taleplerini izleme

Yapılandırma Adımları

1. ADCS Servisi Ekleme

Certificate Authorities (CA) > ADCS > Accounts bölümüne gidin ve **Add New ADCS Service** butonuna tıklayın:



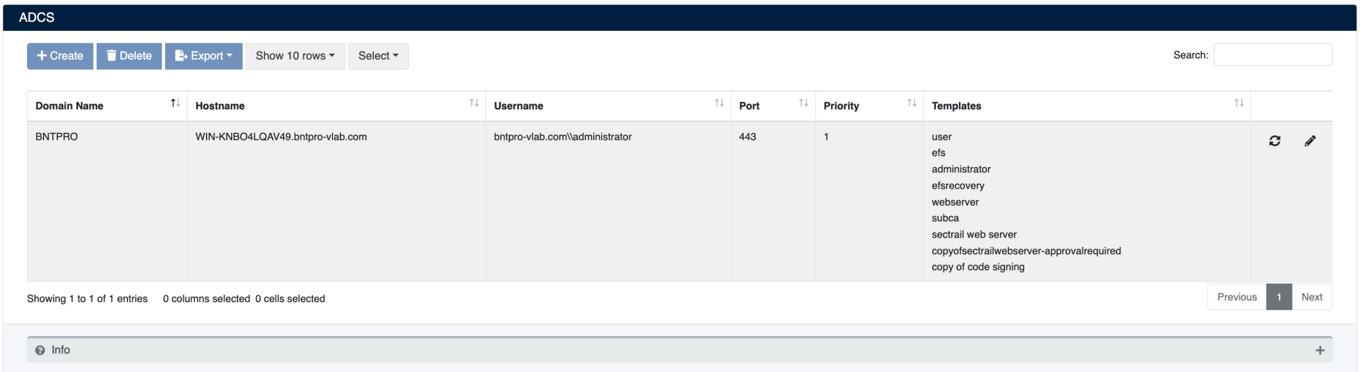
Aşağıdaki bilgileri girin:

- **Domain Name**: Active Directory domain adı
- **Hostname**: ADCS sunucusunun hostname'i
- **Username**: ADCS erişimi için kullanıcı adı. **Automation > Device Users** bölümünden kullanıcı oluşturabilir ve buradan seçebilirsiniz.
- **Password**: Kullanıcı parolası
- **Port**: ADCS Web Enrollment servisi portu (varsayılan: 443)
- **Priority**: Servis öncelik seviyesi (1-10 arası)
- **Auth Method**: Kimlik doğrulama yöntemi (NTLM / Kerberos)

Submit butonuna tıklayarak servisi kaydedin.

2. ADCS Servislerini Görüntüleme

Servis eklendikten sonra **Certificate Authorities (CA) > ADCS > Accounts** listesinde görüntülenecektir:



Liste ekranında aşağıdaki bilgiler gösterilir:

Domain Name: Bağlantının gerçekleştirileceği Active Directory domain adıdır. SecTrail CM, sertifika taleplerini bu domain üzerindeki ADCS sunucusuna iletir.

Hostname: ADCS sunucusunun ağ adresi.

Username: ADCS sunucusuna bağlanmak için kullanılan hesap adı.

Port: ADCS Web Enrollment servisinin dinlediği port numarası (varsayılan: 443).

Priority: Birden fazla ADCS servisi tanımlıysa hangi sunucunun öncelikli kullanılacağını belirler (1-10 arası, düşük değer yüksek öncelik).

Templates: Bu ADCS sunucusundan çekilen ve sertifika imzalamada kullanılabilecek şablon listesi.

Servis İşlemleri

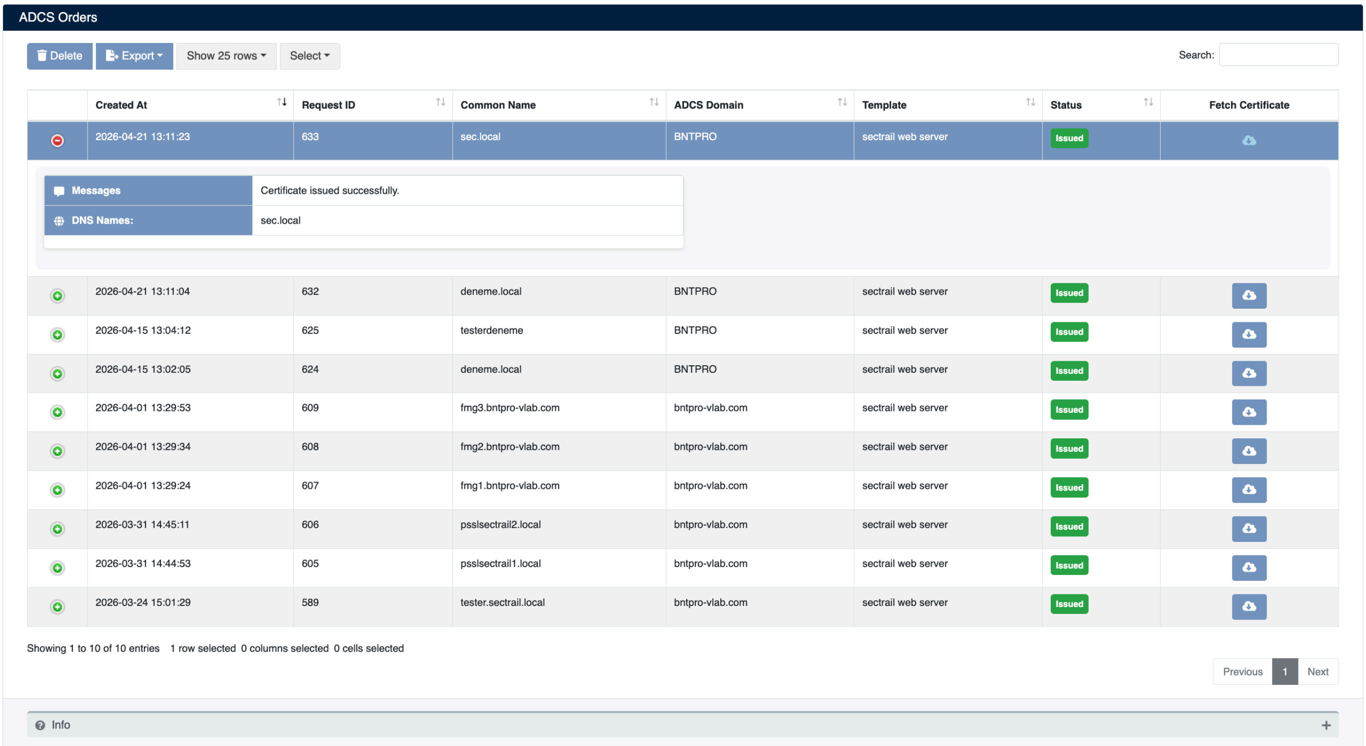
Her servis için aşağıdaki işlemler yapılabilir:

- **Refresh**: Servis bilgilerini ve şablon listesini ADCS sunucusundan yeniden çeker
- **Edit**: Servis bağlantı ayarlarını düzenle
- **Delete**: Servisi sil

Orders (Siparişler)

ADCS'e sertifika talebi gönderildikten sonra tüm bekleyen ve tamamlanan siparişleri şu adresten takip edebilirsiniz:

Certificate Authorities (CA) > ADCS > Orders



Onay Mekanizmalı Şablonlar Hakkında

Bazı ADCS sertifika şablonları, sertifikanın düzenlenmesi için **CA yöneticisi onayı** gerektirir. Bu tür şablonlar kullanılarak sertifika talebinde bulunulduğunda, sertifika hemen düzenlenmez — talep kuyruğa alınır ve ADCS sunucusundaki bir CA yöneticisi tarafından manuel olarak onaylanması gerekir.

> **BEKLEYEN TALEPLERİN TAKİBİ**
>
> Onay gerektiren bir şablonla sertifika talebi gönderdiniz ve sertifika henüz düzenlenmediyse, **Certificate Authorities (CA) > ADCS > Orders** sayfasına giderek durumunu kontrol edebilirsiniz. CA yöneticisi ADCS tarafında talebi onayladıktan sonra, düzenlenen sertifikayı SecTrail CM'e almak için **Fetch** işlemini kullanabilirsiniz.

Sipariş Alanları

Alan	Açıklama
Created At	Talebin ADCS sunucusuna gönderildiği tarih ve saat
Request ID	Talep gönderildikten sonra ADCS tarafından dönen istek ID'si
Common Name	Sertifikanın düzenleneceği domain adı
ADCS Domain	Talebin iletildiği Active Directory domain adı
Template	Sertifika imzalamada kullanılan ADCS şablonu
Status	Siparişin mevcut durumu (Issued, Pending, Denied)
Fetch Certificate	Düzenlenmiş sertifikayı SecTrail CM envanterine almak için kullanılan işlem butonu

Sipariş Durumları

- **Issued** : Sertifika onaylanmış ve düzenlenmiş — almak için **Fetch** kullanın
- **Pending** : ADCS sunucusundaki CA yöneticisinin onayı bekleniyor
- **Denied** : Talep CA yöneticisi tarafından reddedildi

Sipariş İşlemleri

- **Fetch**: Düzenlenmiş sertifikayı SecTrail CM envanterine al
- **Delete**: Sipariş kaydını sil

> **ONAY MEKANİZMALI İŞ AKIŞI**
>
> Organizasyonunuz onay gerektiren ADCS şablonları kullanıyorsa, bekleyen taleplerin onaylanması için CA yöneticinizle koordine edin. Onaydan sonra **Certificate Authorities (CA) > ADCS > Orders** sayfasına dönüp **Fetch** ile sertifikayı içe aktarın.

> **SERTİFİKA İMZALAMA**
>
> ADCS entegrasyonu sayesinde, istediğiniz şablon ile sertifika imzalama işlemini gerçekleştirebilirsiniz. Şablon seçimi, sertifikanın geçerlilik süresi, kullanım amacı ve güvenlik seviyesini belirler.

ACME - Otomatik Sertifika Yönetimi

SecTrail CM, ACME (Automatic Certificate Management Environment - Otomatik Sertifika Yönetim Ortamı) protokolünü destekleyen tüm Sertifika Otoritesi sistemleri ile entegrasyon sağlayarak SSL/TLS sertifikalarının otomatik olarak sipariş edilmesini, yenilenmesini ve yönetilmesini sağlar.

Desteklenen ACME Sağlayıcılar

SecTrail CM, ACME protokolünü destekleyen aşağıdaki Sertifika Otoriteleri ile uyumludur:

- **Let's Encrypt** - Ücretsiz DV sertifikalar için en popüler ACME sağlayıcı
- **Let's Encrypt Staging** - Test ve geliştirme ortamı için test sunucusu
- **ZeroSSL** - Ücretsiz SSL sertifikalar sağlayan ACME servisi
- **Buypass** - Norveç merkezli ücretsiz Sertifika Otoritesi
- **Buypass Staging** - Buypass test ortamı
- **SSL.com RSA** - RSA algoritması ile SSL.com ticari sertifikaları
- **SSL.com ECC** - ECC (Elliptic Curve) algoritması ile SSL.com sertifikaları
- **Google Trust Services** - Google'ın kurumsal ACME servisi
- **Google Trust Services Staging** - Google test ortamı
- **DigiCert** - DigiCert ACME servisi (kurumsal)

> **ACME PROTOKOLÜ**
>
> ACME protokolü, sertifika yaşam döngüsünün otomasyonunu sağlayan açık bir standarttır (RFC 8555). Bu dokümantasyonda **Let's Encrypt** örneği üzerinden entegrasyon adımları anlatılacaktır.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	ACME v2 (HTTPS)	RFC 8555 standardı
Kimlik Doğrulama	Email	ACME account registration
Doğrulama Yöntemleri	DNS-01, HTTP-01	Domain ownership doğrulama
DNS-01 Port	53 (DNS)	Domain Delegasyonu için gerekli (opsiyonel)
HTTP-01 Port	80 (HTTP)	HTTP doğrulama için gerekli (opsiyonel)
DNS Integration	PowerDNS, Akamai	DNS-01 otomasyonu için önerilen

Otomatik İşlemler

SecTrail CM, ACME protokolü üzerinden aşağıdaki işlemleri otomatik gerçekleştirir:

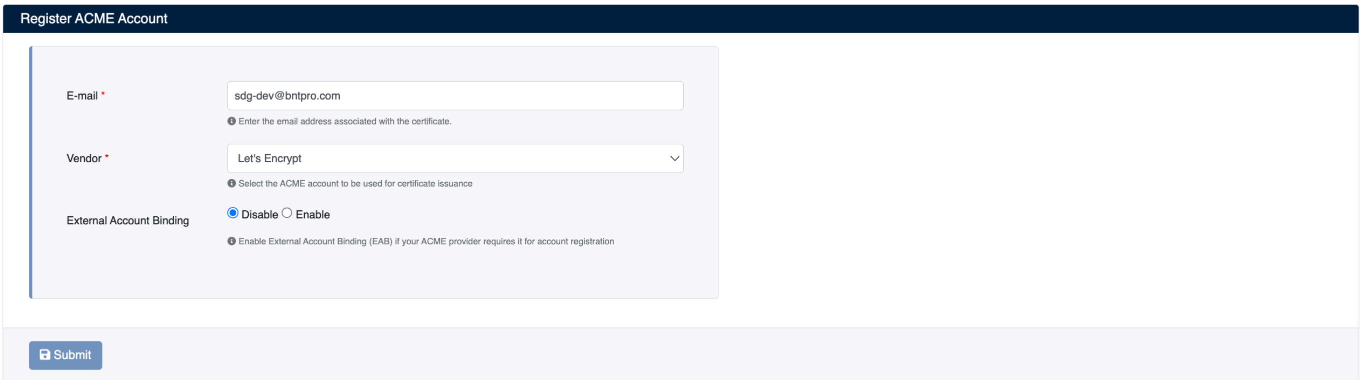
1. **ACME Hesap Kaydı**: Sertifika siparişi için ACME hesabı oluşturma

2. **Sertifika Siparişi**: Yeni SSL/TLS sertifikası talebi oluşturma
3. **Domain Doğrulama**: DNS-01 veya HTTP-01 challenge ile domain doğrulama
4. **Otomatik DNS Kayıt Yönetimi**: DNS doğrulama kayıtlarının otomatik oluşturulması ve silinmesi
5. **Sertifika Düzenleme**: Sertifikanın otomatik olarak alınması
6. **Sertifika Yenileme**: Süresi dolmak üzere olan sertifikaların otomatik yenilenmesi
7. **Sertifika Dağıtımı**: Düzenlenmiş sertifikaların sisteme otomatik eklenmesi

Yapılandırma Adımları

1. ACME Account Oluşturma

Certificate Authorities (CA) > ACME > Accounts bölümüne gidin ve **Register** butonuna tıklayın:



Aşağıdaki bilgileri girin:

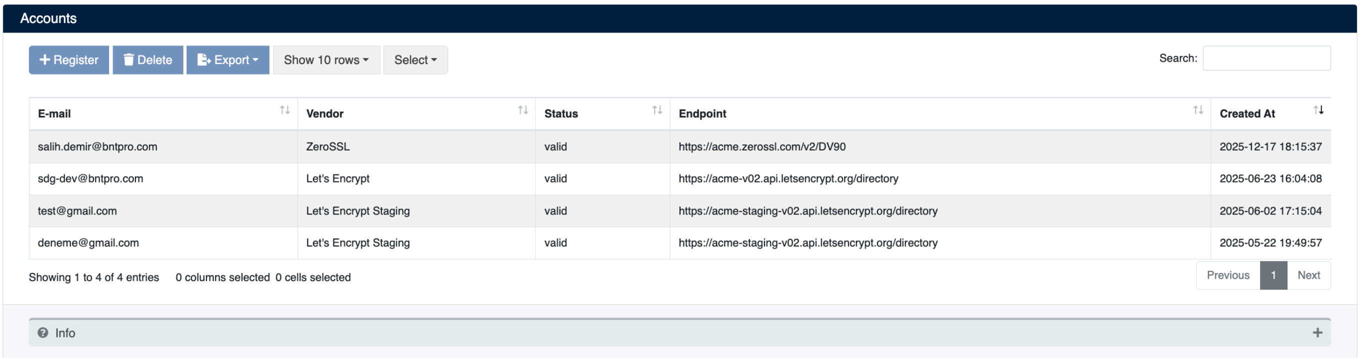
- **E-mail**: ACME account için e-posta adresi
- **Vendor**: ACME sağlayıcı seçimi
- Let's Encrypt
- Let's Encrypt Staging
- ZeroSSL
- Buypass
- Buypass Staging
- SSL.com RSA
- SSL.com ECC
- Google Trust Services
- Google Trust Services Staging
- DigiCert
- **Use External Account Binding**: Bazı sağlayıcılar için gerekli (varsayılan: Disable)

Submit butonuna tıklayarak ACME account'u oluşturun.

> **HESAP KAYDI**
>
> ACME account oluşturulurken otomatik olarak bir anahtar çifti oluşturulur ve kayıt işlemi gerçekleştirilir. Account bilgileri güvenli şekilde saklanır.

2. ACME Hesaplarını Görüntüleme

Account eklendikten sonra **Certificate Authorities (CA) > ACME > Accounts** listesinde görüntülenecektir:



Liste ekranında aşağıdaki bilgiler gösterilir:

- **E-mail**: ACME account e-posta adresi
- **Vendor**: Kullanılan ACME sağlayıcı
- **Status**: Account durumu (valid/invalid)
- **Endpoint**: ACME directory endpoint URL
- **Created At**: Account oluşturulma tarihi

Hesap İşlemleri

Her account için aşağıdaki işlemler yapılabilir:

- **Delete**: Account'u sil

> **ACCOUNT SİLME**
>
> ACME account silindiğinde bu account ile oluşturulmuş tüm siparişler görüntülenemez hale gelir. Ancak düzenlenmiş sertifikalar sistemde kalır.

3. Doğrulama Yöntemleri (Doğrulama Yöntemleri)

ACME protokolü ile sertifika imzalarken iki farklı doğrulama yöntemi kullanılır:

DNS-01 Doğrulama (DNS Doğrulama)

Wildcard sertifika imzalamak için DNS doğrulama yöntemini kullanmanız gerekmektedir.

DNS doğrulama için iki farklı yöntem bulunmaktadır:

Yöntem 1: Domain Delegasyonu (Önerilen)

Gereksinimler:

- SecTrail CM uygulamasının **53 (DNS) portundan** internete erişime açık olması
- Sertifika imzalanacak domainin `_acme-challenge` subdomaininin SecTrail CM sunucusuna delege edilmesi

Yapılandırma:

Domain DNS kaydınızda aşağıdaki NS kaydını oluşturun:

```
_acme-challenge.domainadi NS 3600 sectrailcm.sunucu.adresi
```

Avantajlar:

- Tamamen otomatik süreç
- Manuel müdahale gerektirmez
- Sürekli sertifika yenileme için idealdir

Yöntem 2: Manuel TXT Kaydı

Yapılandırma:

Her sertifika talebi için domain DNS kaydınızda manuel olarak TXT kaydı oluşturmanız gerekir:

```
_acme-challenge.domainadi TXT 3600 TOKEN_DEGERI
```

Dezavantajlar:

- Her sertifika talebi için manuel müdahale gerektirir
- Token değeri her sipariş için değişir
- Otomatik yenileme için uygun değildir

> **MANUEL TXT KAYDI**
>
> Bu yöntem manuel müdahale gerektirdiği için tavsiye edilmemektedir. Otomatik sertifika yenileme süreçleri için Domain Delegasyonu veya External DNS entegrasyonu kullanılmalıdır.

Yöntem 3: External DNS Entegrasyonu (Önerilen)

Desteklenen DNS Sağlayıcılar:

Certificate Authorities (CA) > External DNS bölümünden aşağıdaki DNS sağlayıcılardan birini yapılandırabilirsiniz:

- **PowerDNS -** Açık kaynak DNS sunucusu
- **Akamai** - Kurumsal DNS yönetimi

Yapılandırma:

1. **Certificate Authorities (CA) > External DNS** bölümüne gidin
2. DNS sağlayıcınızı seçin
3. API credentials bilgilerini girin
4. Test edin ve kaydedin

Avantajlar:

- Tamamen otomatik DNS kayıt yönetimi
- TXT kayıtları otomatik oluşturulur ve silinir
- Wildcard ve çoklu domain sertifikalar için ideal
- Sertifika yenileme tam otomasyonu

> **DNS ENTEGRASYONU**

> PowerDNS ve Akamai entegrasyonları ile DNS doğrulama kayıtları tamamen otomatik yönetilir. Manuel müdahale gerekmez ve sertifika yenileme süreçleri kesintisiz çalışır.

HTTP-01 Doğrulama (HTTP Doğrulama)

Kullanım Alanı: Sadece tek domain (tek domain) sertifikalar için kullanılabilir. Wildcard sertifikalar için **desteklenmez**.

Gereksinimler:

1. **Port 80 Erişimi:** İmzalanacak domain 80 portundan HTTP isteğine cevap verebilmeli
2. **Public IP:** Domain'in public IP adresi istekleri alabilmeli
3. **Web Sunucu:** Domain için web sunucusu yapılandırması olmalı

F5 Yük Dengeleyici Kullanıyorsanız:

- Domain'in public IP'si istekleri F5'e geliyor olmalı
- Hangi virtual server'a indiğini biliyor olmalınız
- Port 80 üzerinden `/.well-known/acme-challenge/` path'ine erişim sağlanmalı

ACME Challenge Süreci:

1. ACME server, `http://domainadi/.well-known/acme-challenge/TOKEN` adresine HTTP GET isteği gönderir
2. Web sunucunuz bu isteğe doğrulama token'ı ile cevap vermelidir
3. Token doğrulandığında sertifika düzenlenir

> **HTTP-01 KISITLAMALARI**
>
> - **Wildcard sertifikalar için kullanılamaz**
> - Port 80 üzerinden erişilebilir olmalı (HTTPS değil)
> - Her domain için ayrı doğrulama gerekir
> - Load balancer veya firewall yapılandırması gerektirebilir

> **DOĞRULAMA YÖNTEMİ SEÇİMİ**
>
> - **Wildcard Sertifikalar için:** DNS-01 doğrulama kullanılmalıdır (zorunlu)
> - **Tek Domain için:** HTTP-01 veya DNS-01 kullanılabilir
> - **Otomatik Yenileme için:** DNS-01 with External DNS önerilir
> - **Manuel Süreç için:** HTTP-01 kullanılabilir

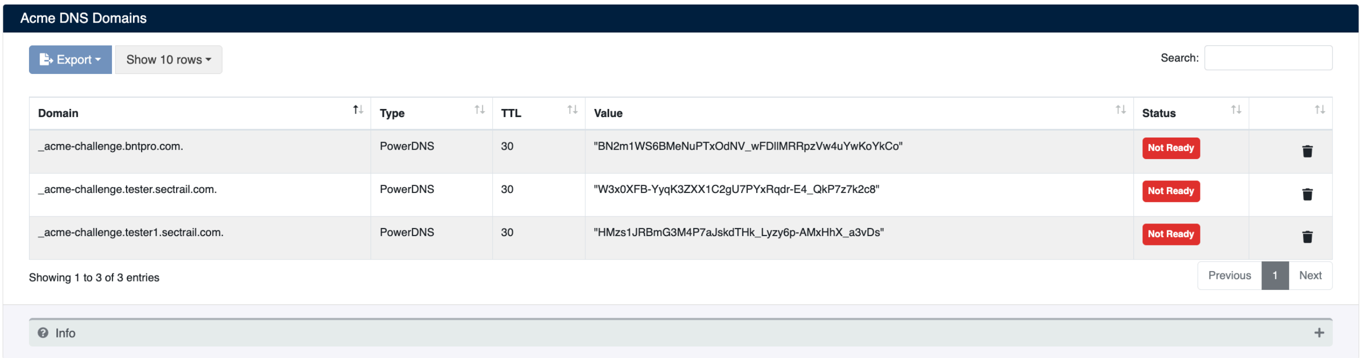
4. DNS Entegrasyonu Yapılandırması

DNS-01 doğrulama kullanmak için External DNS entegrasyonu yapılandırılmalıdır.

DNS Challenge Kayıtları

ACME sertifika siparişi oluşturulduğunda, DNS doğrulama için otomatik olarak TXT kayıtları oluşturulur:

Certificate Authorities (CA) > ACME > Acme DNS Domains bölümünde challenge kayıtlarını görüntüleyebilirsiniz:



DNS Kayıt Bilgileri

- **Domain**: Challenge kaydının oluşturulacağı domain (_acme-challenge.example.com)
- **Type**: DNS kayıt tipi (PowerDNS, Akamai, vb.)
- **TTL**: Time to Live değeri (saniye)
- **Value**: ACME challenge token değeri
- **Status**: Kayıt durumu (Not Ready, Ready, Valid)

> **OTOMATİK DNS YÖNETİMİ**
>
> DNS doğrulama kayıtları sertifika siparişi oluşturulduğunda otomatik olarak eklenir ve doğrulama tamamlandıktan sonra otomatik olarak silinir. Manuel müdahale gerekmez.

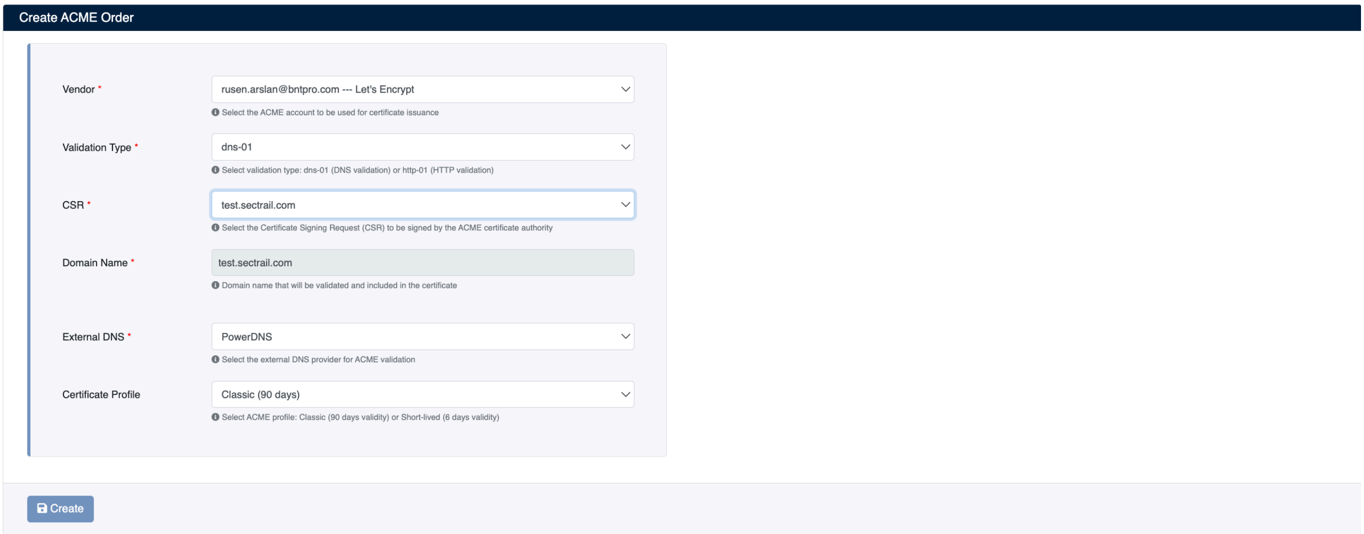
DNS Kayıt Durumları

- **Not Ready**: DNS kaydı oluşturuldu, propagation bekleniyor
- **Ready**: DNS kaydı propagate oldu, doğrulama başlatılabilir
- **Valid**: Doğrulama başarılı, sertifika düzenlendi

Sertifika Sipariş Oluşturma

ACME üzerinden yeni sertifika siparişi oluşturmak için:

Certificate Authorities (CA) > ACME > Orders bölümüne gidin ve **Create ACME Order** butonuna tıklayın:



Sipariş Bilgileri

Aşağıdaki bilgileri girin:

- **Vendor**: Kullanılacak ACME account seçimi (email --- vendor formatında)
- **Doğrulama Type**: Doğrulama yöntemi seçimi
- `dns-01`: DNS doğrulama (wildcard sertifikalar için zorunlu, tek domain için önerilen)
- `http-01`: HTTP challenge (sadece tek domain sertifikalar için)
- **CSR**: Certificate Signing Request seçimi
- Önceden oluşturulmuş CSR'lerden seçim yapın
- CSR'ler **Integration** bölümünden oluşturulabilir
- **Domain Name**: Sertifika için domain adları
- **External DNS**: DNS doğrulama için kullanılacak DNS provider seçimi (sadece dns-01 için)
- PowerDNS, Akamai, Cloudflare, Route53, vb.

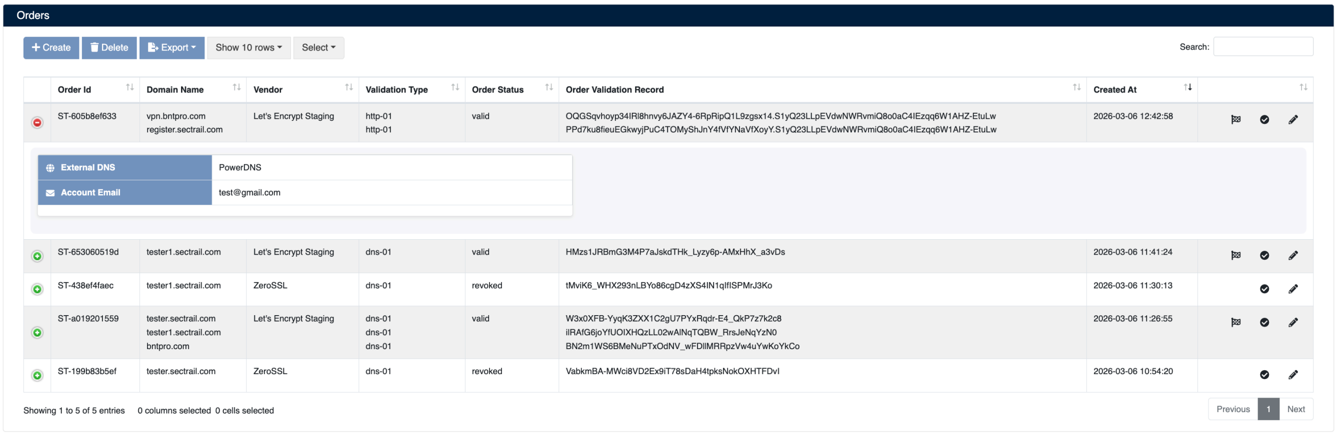
Submit butonuna tıklayarak sipariş oluşturun.

> **CSR (CERTİFİCATE SİGNİNG REQUEST)**
>
> Sipariş oluşturmadan önce **Certificates > CSR** bölümünden CSR oluşturmanız gerekir. CSR, sertifika için gerekli domain adlarını, organization bilgilerini ve public key'i içerir.

Sertifika Siparişlerini Görüntüleme

ACME sertifika siparişlerinizi görüntülemek için:

Certificate Authorities (CA) > ACME > Orders bölümüne gidin:



Sipariş Bilgileri

- **Order Id**: SecTrail sipariş ID'si
- **External DNS**: Kullanılan DNS provider
- **Domain Name**: Sertifika domain adları
- **Vendor**: ACME sağlayıcı
- **Account Email**: ACME account e-posta
- **Doğrulama Type**: Doğrulama yöntemi (dns-01 veya http-01)
- **Order Status**: Sipariş durumu (valid, processing, invalid)
- **Order Doğrulama Record**: ACME challenge token değerleri
- **Created At**: Sipariş oluşturulma tarihi

Sipariş İşlemleri

Her sipariş için aşağıdaki işlemler yapılabilir:

- **Refresh Order**: Sipariş durumunu güncelle
- **Finalize Order**: Doğrulama tamamlandığında sertifikayı al
- **Download Certificate**: Düzenlenmiş sertifikayı indir
- **Delete Order**: Siparişi sil

Sipariş Durumları

- **pending**: Sipariş oluşturuldu, doğrulama bekleniyor
- **ready**: Doğrulama başarılı, finalize edilmeye hazır
- **processing**: Sertifika düzenleniyor
- **valid**: Sertifika başarıyla düzenlendi
- **invalid**: Doğrulama başarısız

Sertifika Yaşam Döngüsü

1. Sipariş Oluşturma (Order Creation)

1. CSR oluşturun (**Certificates > CSR**)

2. ACME account seçin
3. Doğrulama type ve External DNS seçin
4. Sipariş oluşturun

2. DNS Challenge (Doğrulama)

Sipariş oluşturulduktan sonra otomatik olarak:

1. DNS doğrulama kayıtları oluşturulur (`_acme-challenge.example.com`)
2. DNS propagation beklenir (genellikle 30-60 saniye)
3. ACME server domain ownership'i doğrular
4. Doğrulama başarılı olduğunda sipariş durumu "ready" olur

3. Sertifika Alma (Finalization)

Doğrulama başarılı olduktan sonra:

1. **Finalize Order** butonuna tıklayın
2. Sertifika otomatik olarak düzenlenir
3. Sipariş durumu "valid" olur
4. DNS doğrulama kayıtları otomatik olarak silinir

4. Sertifika İndirme (Download)

1. **Download Certificate** butonuna tıklayın
2. Sertifika otomatik olarak sisteme eklenir
3. **Certificates** bölümünden görüntülenebilir

> **OTOMATİK İŞLEMLER**
>
> DNS doğrulama kayıtlarının oluşturulması, doğrulama ve sertifika alma işlemleri tamamen otomatiktir. Manuel müdahale gerektirmez.

Sertifika Yenileme

ACME sertifikaları otomatik olarak yenilenebilir:

1. **Certificates** bölümünden süresi dolacak sertifikayı seçin
2. **Renew** butonuna tıklayın
3. Yeni ACME siparişi otomatik olarak oluşturulur
4. Doğrulama ve finalization otomatik gerçekleşir

> **LET'S ENCRYPT SÜRELERİ**
>
> Let's Encrypt sertifikaları 90 gün geçerlidir.

HashiCorp Vault

SecTrail CM, HashiCorp Vault ile entegrasyon sağlayarak kurumsal SSL/TLS sertifikalarının otomatik olarak talep edilmesini ve yönetilmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	HTTPS	Vault API kullanılır
Port	Kullanılan Port	Standart Vault API portu
Kimlik Doğrulama	Token Authentication	Vault token ile kimlik doğrulama
Kullanıcı Yetkisi	PKI Secret Engine Read/Write	Sertifika talep ve kayıt yetkisi

Otomatik İşlemler

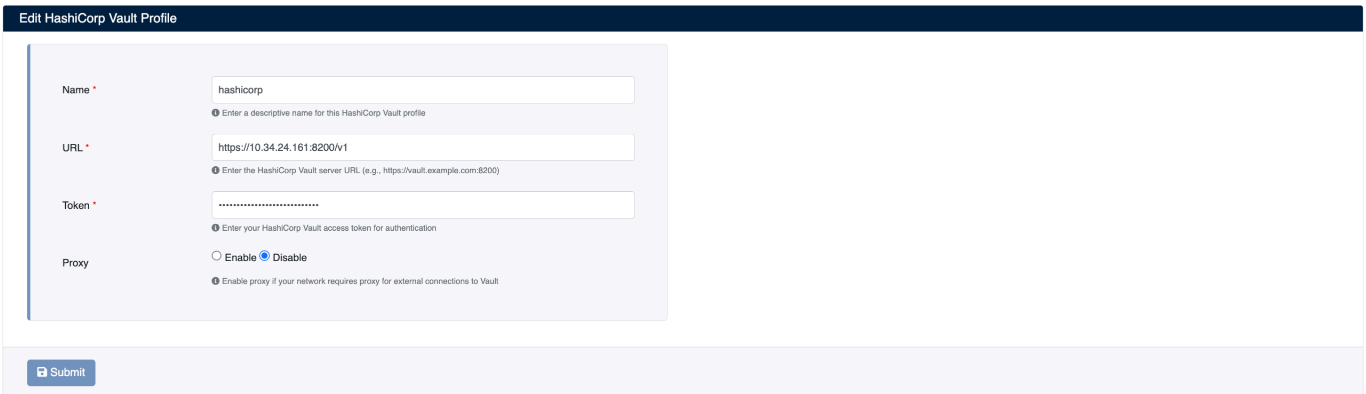
SecTrail CM, HashiCorp Vault üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika Talebi**: CSR (Certificate Signing Request) gönderimi
2. **Sertifika Kayıt**: Vault PKI Engine üzerinden sertifika düzenleme
3. **Role Yönetimi**: Farklı sertifika rollerini kullanma
4. **Otomatik Onay**: Yapılandırılmış roller için otomatik onay

Yapılandırma Adımları

1. HashiCorp Vault Profili Ekleme

Certificate Authorities (CA) > Hashicorp bölümüne gidin ve **Create** butonuna tıklayın:



Aşağıdaki bilgileri girin:

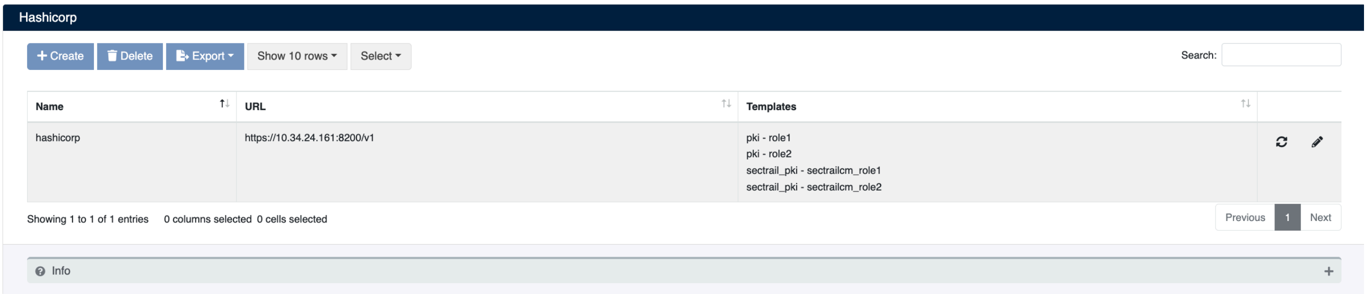
- **Name**: Profil adı
- **URL**: Vault sunucusunun URL'i
- **Token**: Vault API token'ı

- **Proxy**: Proxy kullanımı (Etkinleştir/Devre Dışı Bırak). Proxy'yi etkinleştirdikten sonra **Settings -> Proxy** ayarlarından proxy yapılandırmanızı tamamlayın.

Submit butonuna tıklayarak profili kaydedin.

2. HashiCorp Vault Profillerini Görüntüleme

Profil eklendikten sonra **Certificate Authorities (CA) > Hashicorp** listesinde görüntülenecektir:



Liste ekranında aşağıdaki bilgiler gösterilir:

- **Name**: Profil adı
- **URL**: Vault sunucu adresi
- **Templates**: Kullanılabilir sertifika rolleri (PKI rolleri)

Profil İşlemleri

Her profil için aşağıdaki işlemler yapılabilir:

- **Refresh**: Profil bilgilerini ve role listesini yenile
- **Edit**: Profil ayarlarını düzenle
- **Delete**: Profili sil

> **SERTİFİKA İMZALAMA**
>
> HashiCorp Vault entegrasyonu sayesinde, istediğiniz role ile sertifika imzalama işlemini gerçekleştirebilirsiniz. Role seçimi, sertifikanın geçerlilik süresi, kullanım amacı ve güvenlik seviyesini belirler.

F5 BIG-IP

SecTrail CM, F5 BIG-IP cihazlarına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	iControl REST API (HTTPS)	F5 BIG-IP'nin native REST API'si kullanılır
Port	`443`	Standart HTTPS portu
Kimlik Doğrulama	Basic Authentication	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	tmsh + Administrator	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, F5 BIG-IP üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in güvenli transferi
2. **Virtual Server Güncelleme**: İlgili virtual server'ların yeni sertifikayı kullanması için yapılandırma
3. **Configuration Sync**: HA ortamlarında peer cihazlara otomatik senkronizasyon

Yapılandırma Adımları

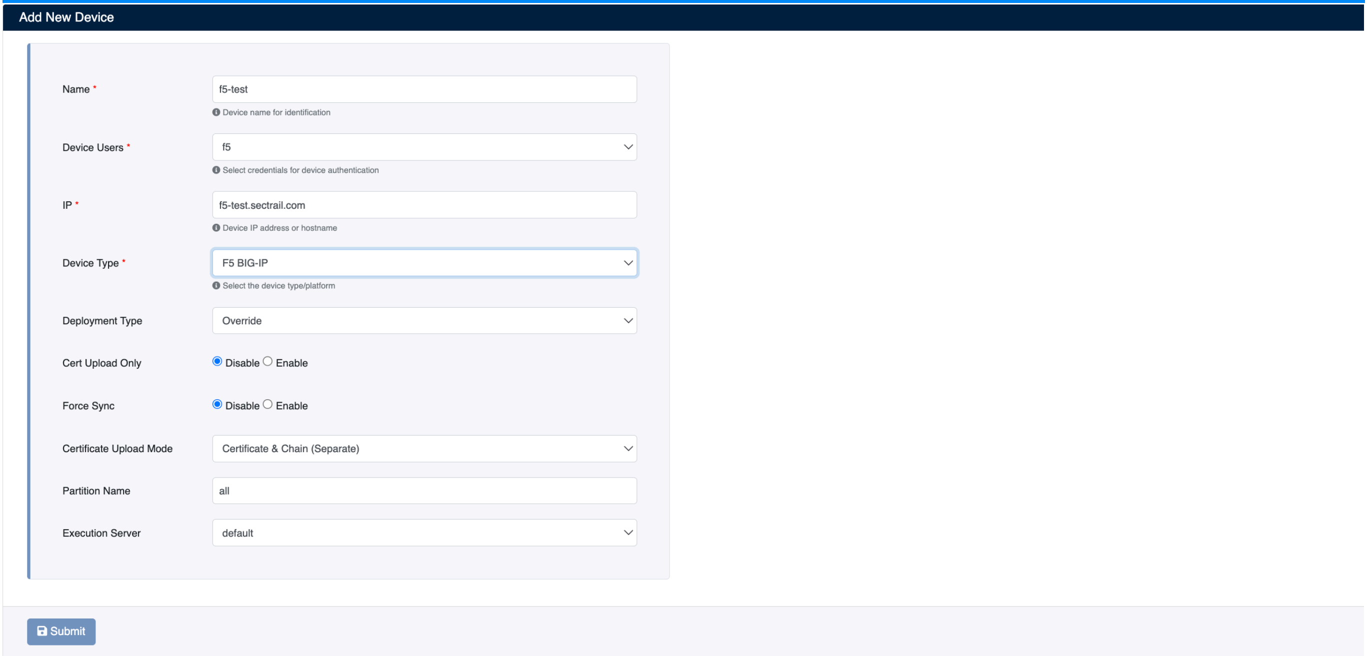
1. F5 BIG-IP Kullanıcısı Oluşturma

Automation > Device Users bölümüne gidin ve F5 için kullanıcı oluşturun.

> **KULLANICI YETKİLERİ**
>
> Kullanıcının tmsh (Traffic Management Shell) yetkisine sahip olduğundan emin olun.

2. F5 Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:



- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: F5 BIG-IP cihazının IP adresini girin
- **Device Type**: Açılır menüden `F5 BIG-IP` seçin
- **Deployment Type**: **Generative** veya **Override** modunu seçin
- **Cert Upload Only**: Yalnızca sertifika yüklensin mi? (Devre Dışı/Etkin)
- **Force Sync**: Standby cihaza otomatik senkronizasyon aktif olsun mu? (Devre Dışı/Etkin)
- **Partition Name**: Varsayılan olarak `all` bırakılabilir
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

Deployment Type Seçenekleri

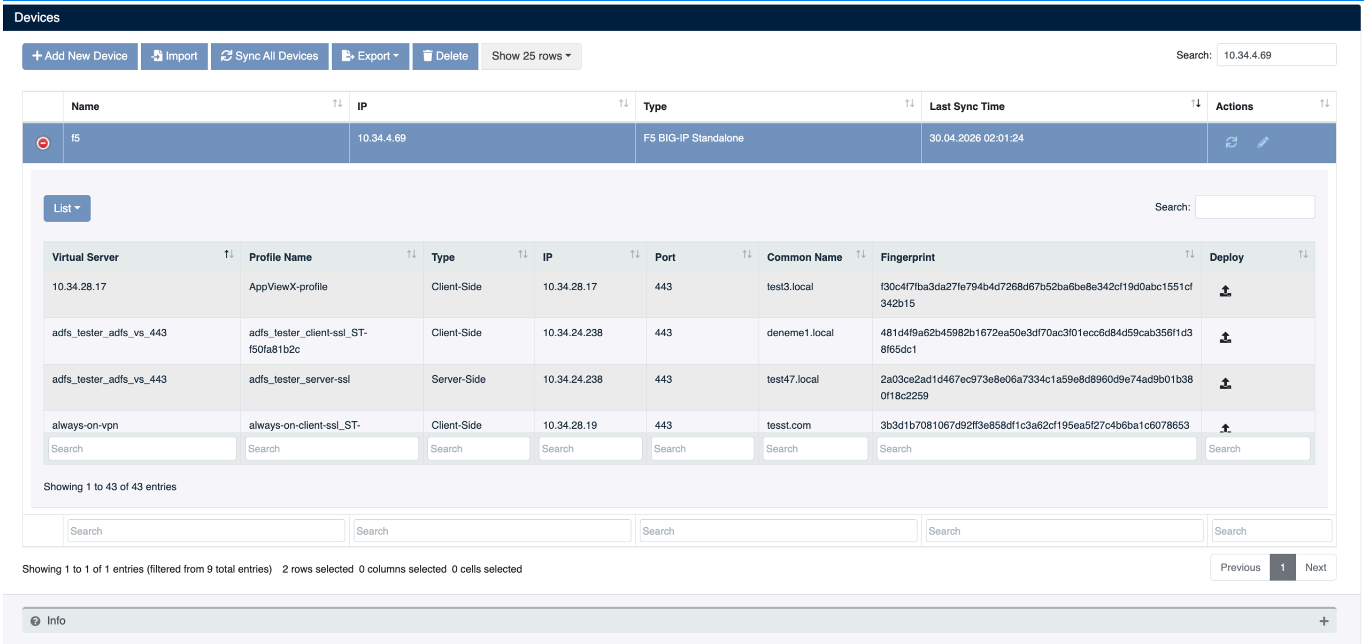
- **Generative**: SecTrail CM, yeni Client SSL Profile oluşturur ve Virtual Server'ı otomatik günceller
- **Override**: Mevcut SSL Profile'ı doğrudan değiştirir

> **FORCE SYNC**
>
> HA (High Availability) ortamlarında **Force Sync** seçeneğini etkinleştirerek standby cihaza otomatik senkronizasyon sağlayabilirsiniz.

> **OTOMATİK KEŞİF**
>
> F5 cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Virtual Server'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



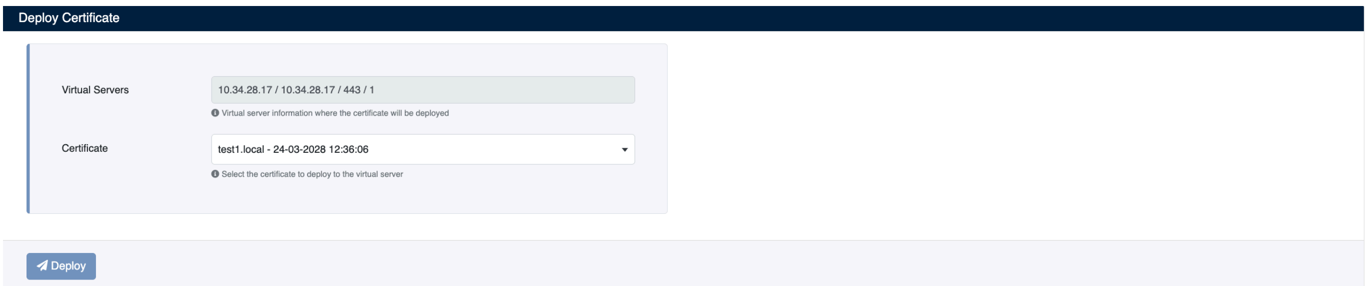
- **Virtual Server**: F5 cihazında tanımlı Virtual Server adları
- **Profile Name**: SSL profil isimleri
- **Type**: Client-Side veya Server-Side SSL profil tipi
- **Destination Address** ve **Port**: Virtual Server'ın dinlediği IP ve port
- **Common Name**: Mevcut sertifikanın Common Name değeri
- **Fingerprint**: Sertifikanın parmak izi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden F5 cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server**'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin



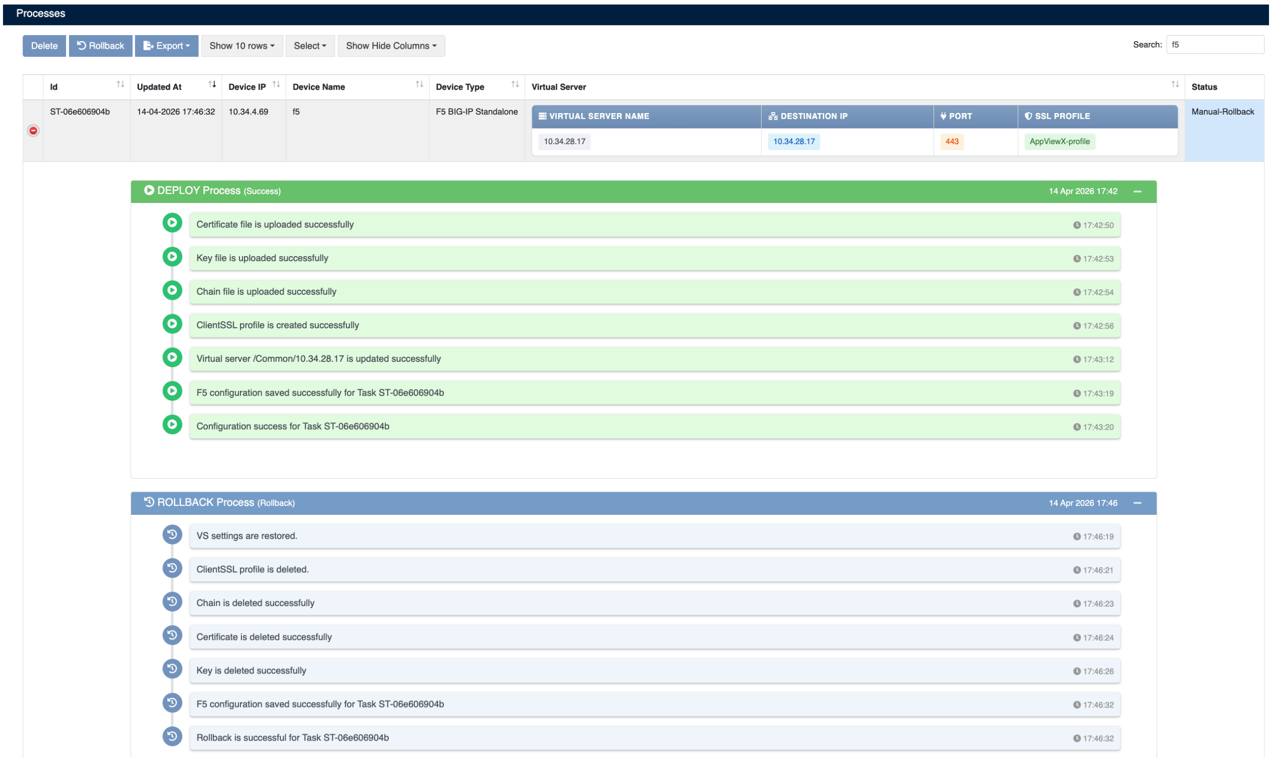
Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

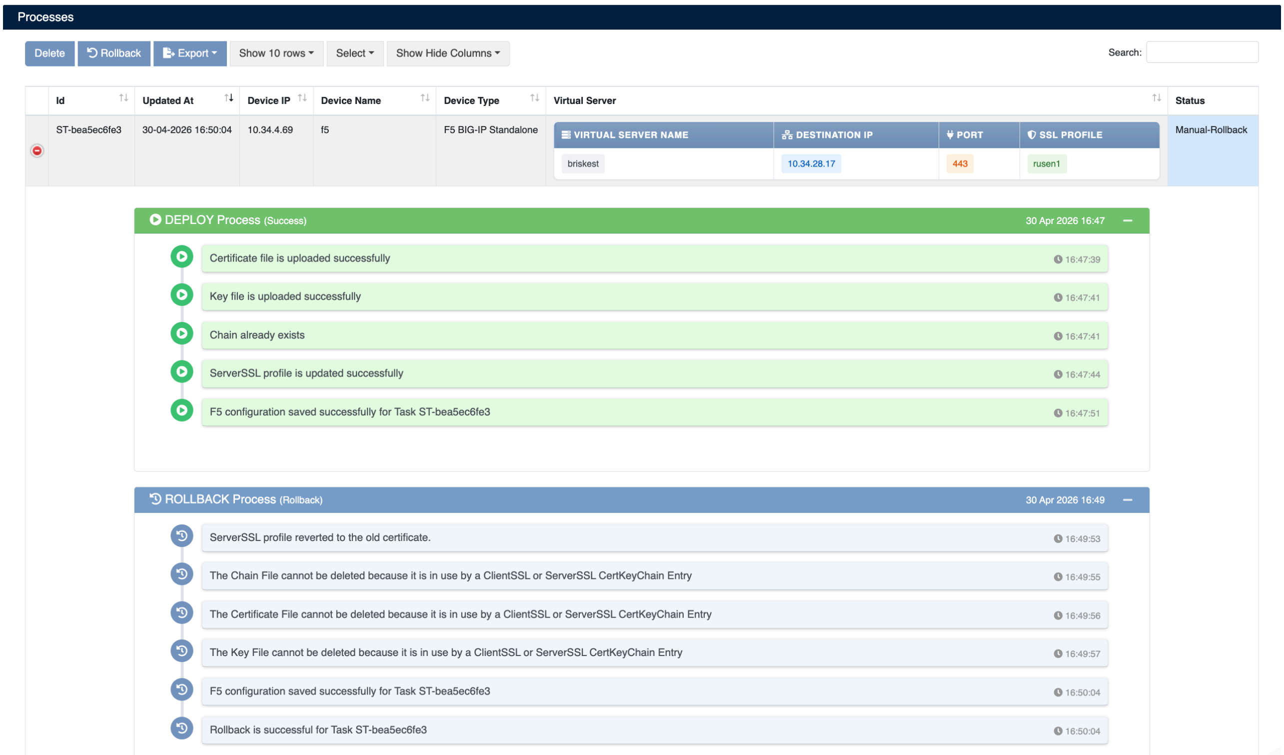
Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:

Generative Mode:



Override Mode:



İşlem Detayları

Adım	Generative Mode	Override Mode
1	Sertifika, key ve chain dosyaları F5 BIG-IP cihazına yüklenir	Sertifika, key ve chain dosyaları F5 BIG-IP cihazına yüklenir
2	Var olan Client SSL profili parent alınarak yeni bir Client SSL profil oluşturulur	Var olan Client SSL profili doğrudan güncellenir (yeni profil oluşturulmaz)
3	Oluşturulan yeni profil Virtual Server'a atanır	VS yapılandırması değiştirilmeden, profildeki sertifika güncellenir

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	Generative Mode Rollback	Override Mode Rollback
1	VS'nin önceki profil ayarları restore edilir	Profildeki sertifika referansları eski sertifikaya geri alınır
2	Deployment sırasında oluşturulan profil kaldırılır	Yeni yüklenen sertifika, key ve chain dosyaları silinir
3	F5 cihazından sertifika, key ve chain dosyaları silinir	-

Citrix NetScaler

SecTrail CM, Citrix NetScaler Application Delivery Controller (ADC) cihazlarına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	NITRO REST API (HTTPS)	NetScaler'ın native REST API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Basic Authentication	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	nsroot veya superuser role	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, Citrix NetScaler üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in güvenli transferi
2. **CertKey Oluşturma**: Certificate-key pair oluşturma ve yönetimi
3. **Virtual Server Binding**: SSL Virtual Server'lara sertifika bağlama
4. **Configuration Save**: Konfigürasyonun kalıcı hale getirilmesi

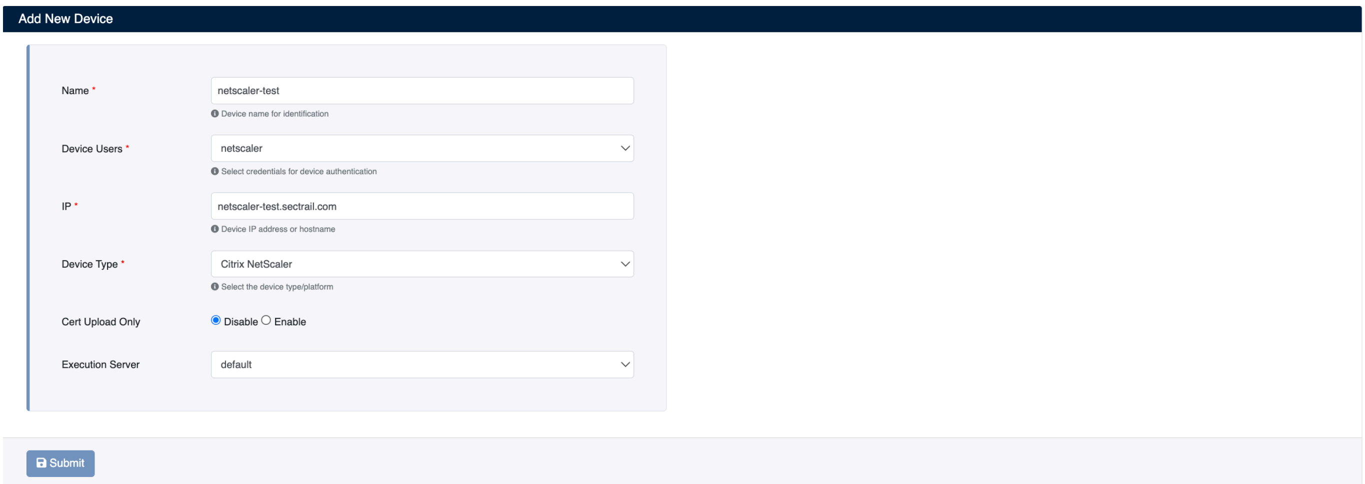
Yapılandırma Adımları

1. NetScaler Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve F5 için kullanıcı oluşturun.

2. NetScaler Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

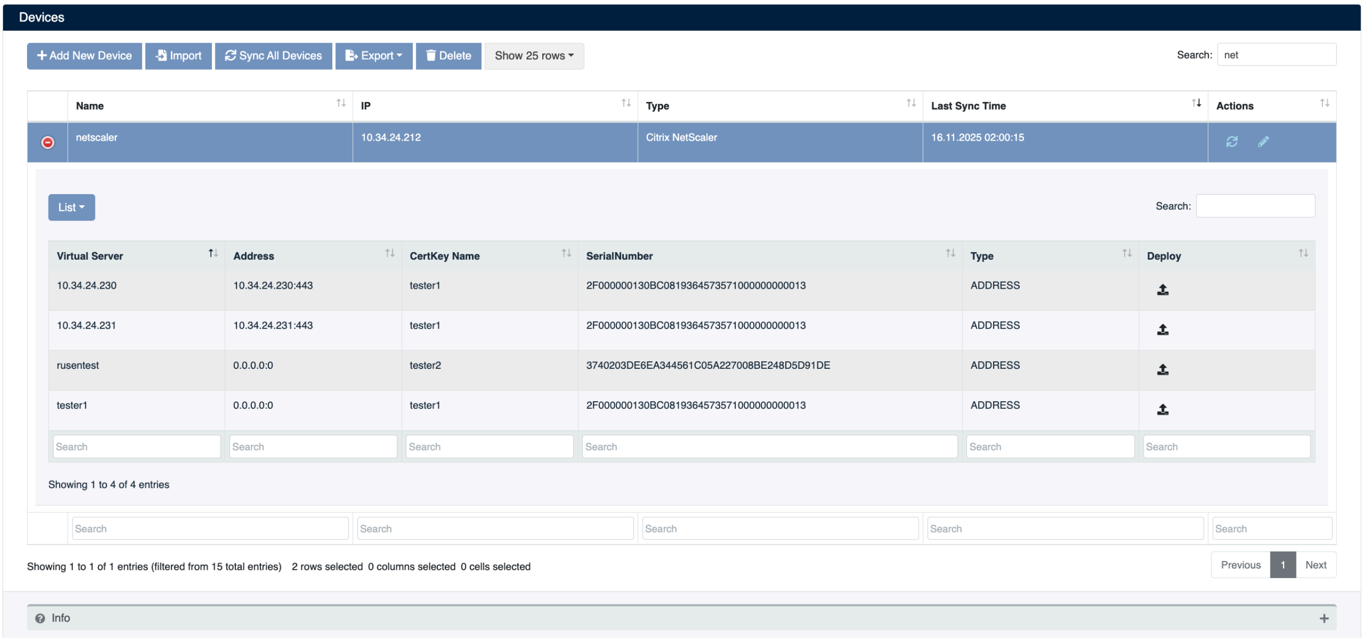


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: NetScaler cihazının NSIP adresini girin
- **Device Type**: Açılır menüden `Citrix NetScaler` seçin
- **Cert Upload Only**: Yalnızca sertifika yüklensin mi? (Devre Dışı/Etkin)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> NetScaler cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Virtual Server'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



- **Virtual Server**: NetScaler cihazında tanımlı Virtual Server adları
- **Address**: Virtual Server'ın IP adresi ve portu
- **CertKey Name**: Mevcut certificate-key pair isimleri
- **SerialNumber**: Sertifikanın seri numarası
- **Type**: Address tipini gösterir
- **Deploy**: Sertifika dağıtımı için

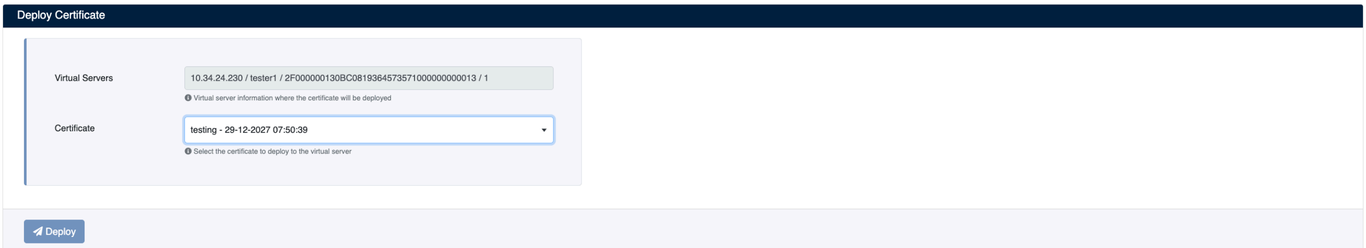
Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden NetScaler cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server**'ı bulun

3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir (IP, port, CertKey adı)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

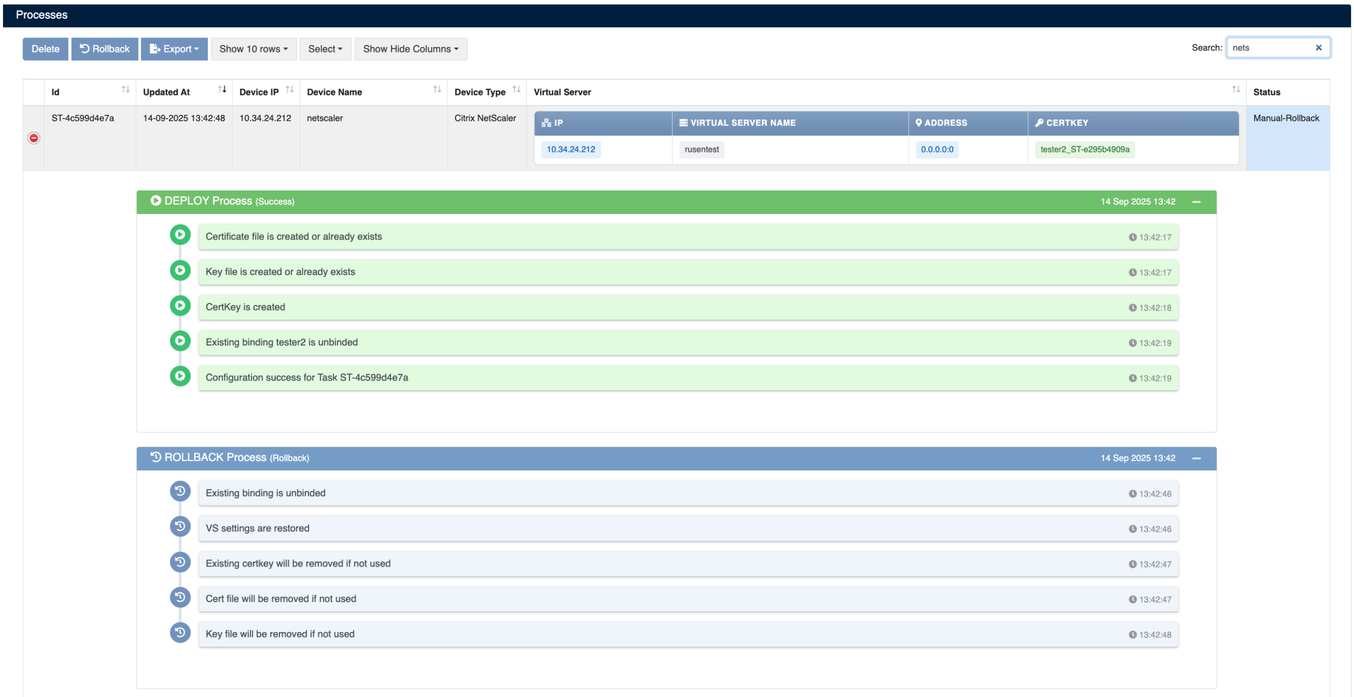


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika ve key dosyası sisteme yüklenir
2	Certificate-key pair oluşturulur
3	Mevcut sertifika bağlantısı kaldırılır
4	Yeni sertifika virtual server'a bağlanır

OTOMATİK TEMİZLİK

SecTrail CM, dağıtım sonrasında kullanılmayan eski sertifika ve key dosyalarını otomatik olarak temizler.

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

OTOMATİK GERİ ALMA

Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Eski sertifika-key pair korunur
2	Virtual Server'ın önceki binding ayarları restore edilir
3	Yeni yüklenen sertifika ve key dosyaları silinir
4	Deployment sırasında oluşturulan certkey kaldırılır

Palo Alto Networks

SecTrail CM, Palo Alto Networks firewall cihazlarına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	XML API (HTTPS)	Palo Alto'nun native XML API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Username ve Password	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	Admin veya Certificate Manager role	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, Palo Alto Networks firewall üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in güvenli transferi
2. **Certificate Import**: Sertifika ve key'in cihaza import edilmesi
3. **SSL Profile Update**: SSL decryption profile'larının güncellenmesi
4. **Configuration Commit**: Konfigürasyonun commit edilmesi ve kalıcı hale getirilmesi

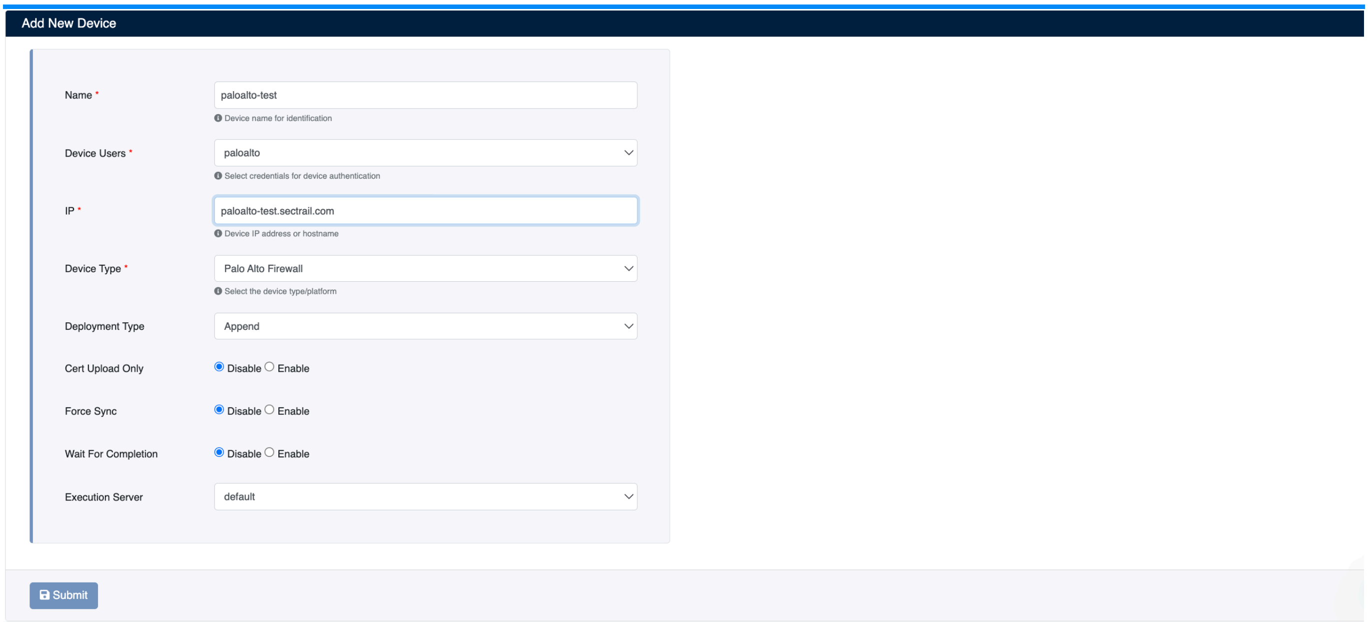
Yapılandırma Adımları

1. Palo Alto Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Palo Alto için kullanıcı oluşturun.

2. Palo Alto Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

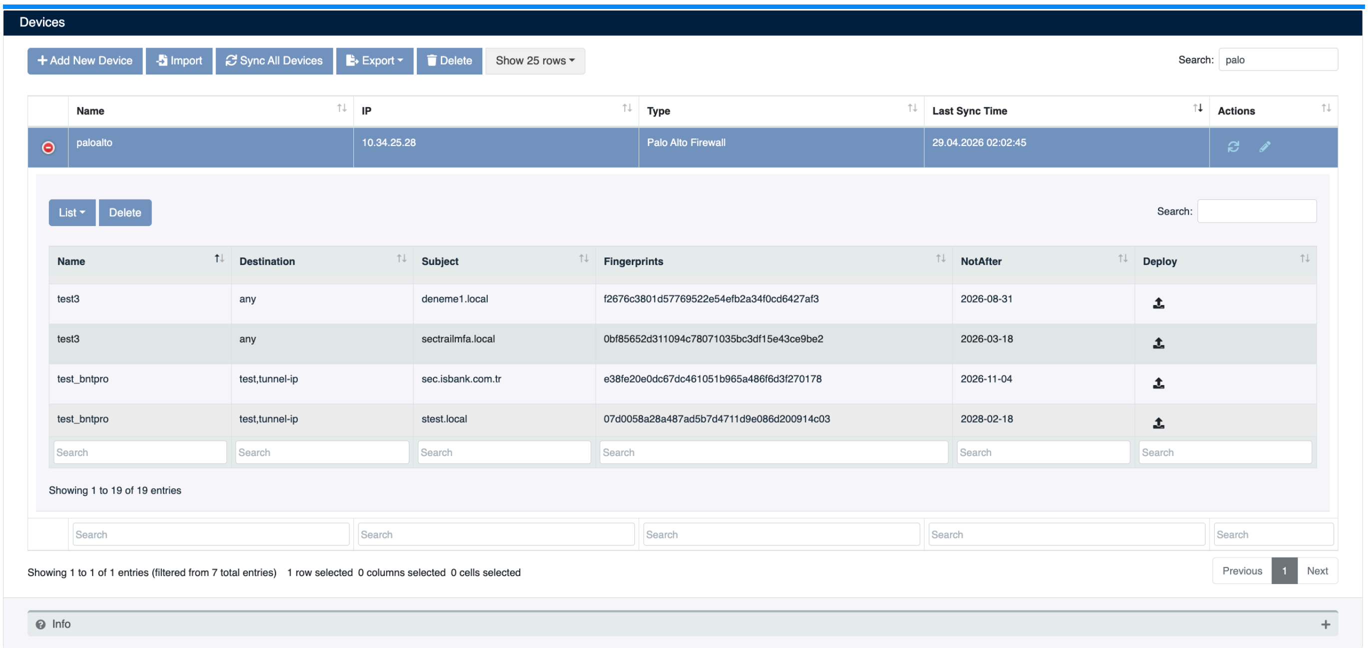


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: Palo Alto cihazının management IP adresini girin
- **Device Type**: Açılır menüden `Palo Alto Firewall` seçin
- **Deployment Type**: Dağıtım tipini seçin
- **Append**: Var olan decryption rule'a yeni sertifikayı ekler (mevcut sertifikalar korunur)
- **Override**: Mevcut sertifikayı yenisiyle değiştirir (eski sertifika silinir)
- **Cert Upload Only**: Yalnızca sertifika yüklensin mi? (Devre Dışı/Etkin)
- **Force Sync**: Değişiklikler otomatik commit edilsin mi? (Devre Dışı/Etkin)
- **Wait For Completion**: Commit işleminin tamamlanması beklensin mi? (Devre Dışı/Etkin)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF VE İZLEME**
>
> Palo Alto cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



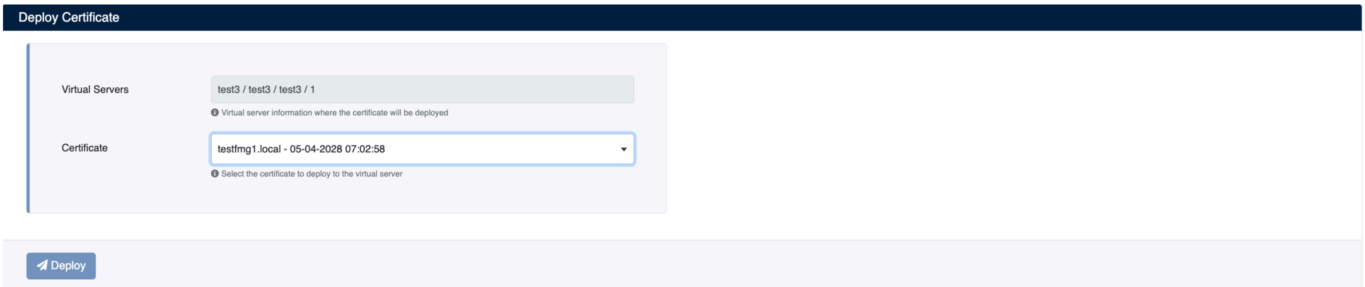
- **Name**: Cihazda tanımlı sertifika adları
- **Destination**: Sertifikanın kullanım alanı (any, tunnel-ip vb.)
- **Subject**: Sertifikanın subject bilgisi
- **Fingerprints**: Sertifikanın parmak izi
- **NotAfter**: Sertifikanın son geçerlilik tarihi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Palo Alto cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server**'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir (Name/Destination/Subject formatında)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

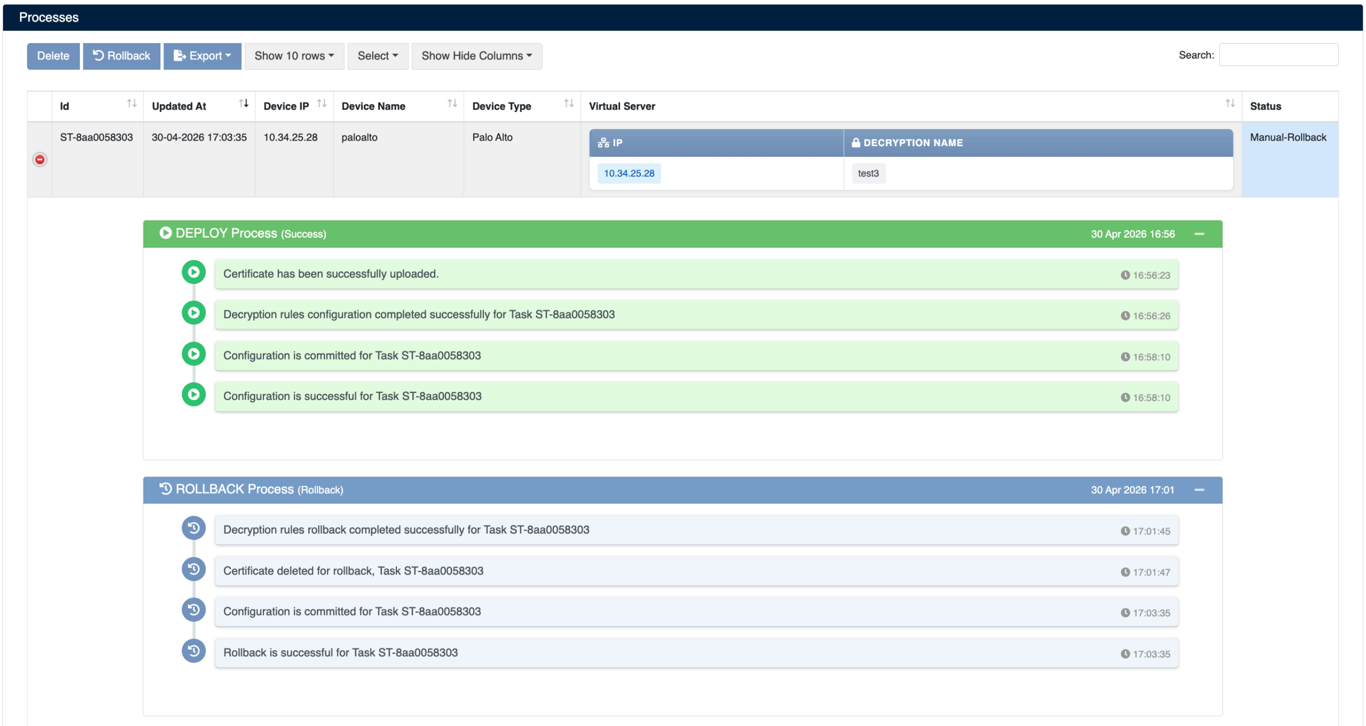


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika başarıyla güncellenir
2	Decryption kuralları yapılandırılır
3	Yapılandırma commit edilir
4	Yapılandırma başarıyla tamamlanır

> **COMMİT**
>
> **Force Sync** aktif olduğunda SecTrail CM, dağıtım sonrasında yapılandırma değişikliklerini otomatik olarak commit eder ve kalıcı hale getirir.

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Yeni yüklenen sertifika silinir
2	Önceki konfigürasyon geri yüklenir
3	Decryption kuralları eski haline getirilir
4	Geri alma işlemi başarıyla tamamlanır

PaloAlto Panorama

SecTrail CM, Palo Alto Panorama merkezi yönetim platformuna **ajansız** bağlantı kurarak yönetilen tüm firewall cihazlarına SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	XML API (HTTPS)	Panorama'nın native XML API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Username ve Password	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	Admin veya Certificate Manager role	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, Palo Alto Panorama üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in güvenli transferi
2. **Certificate Import**: Sertifika ve key'in Panorama üzerinden yönetilen cihazlara import edilmesi
3. **SSL Profile Update**: SSL decryption profile'larının güncellenmesi
4. **Configuration Commit**: Konfigürasyonun commit edilmesi ve kalıcı hale getirilmesi

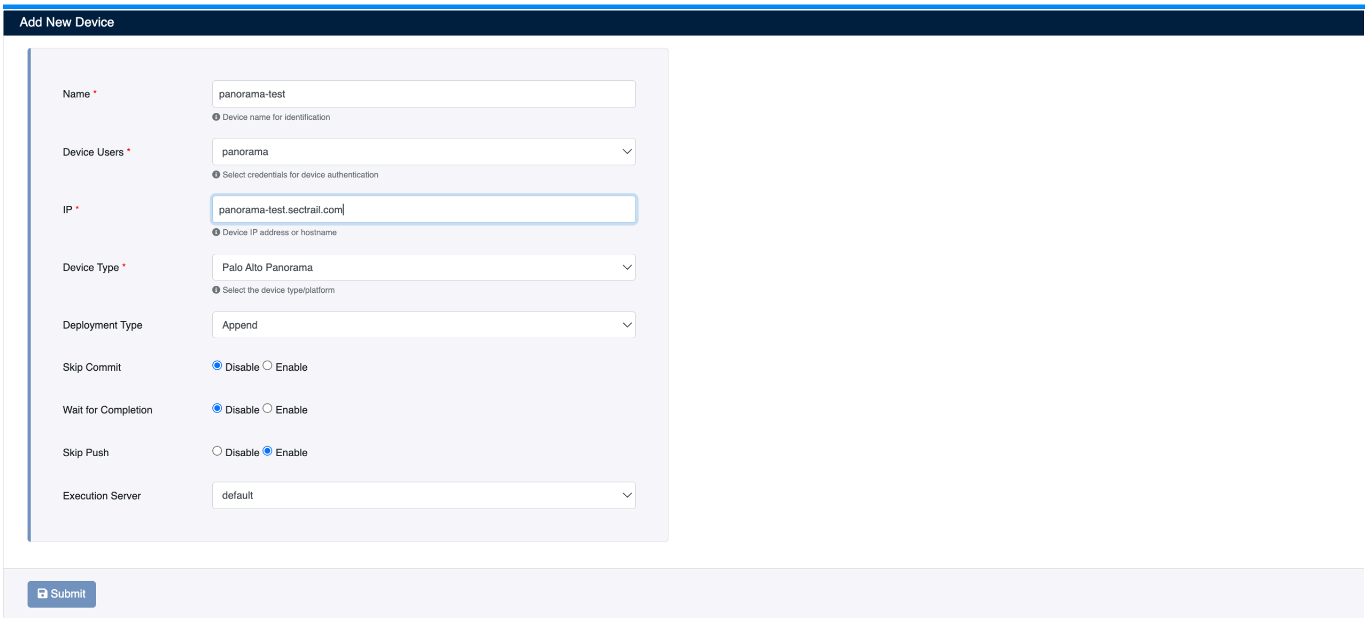
Yapılandırma Adımları

1. Panorama Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Panorama için kullanıcı oluşturun.

2. Panorama Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

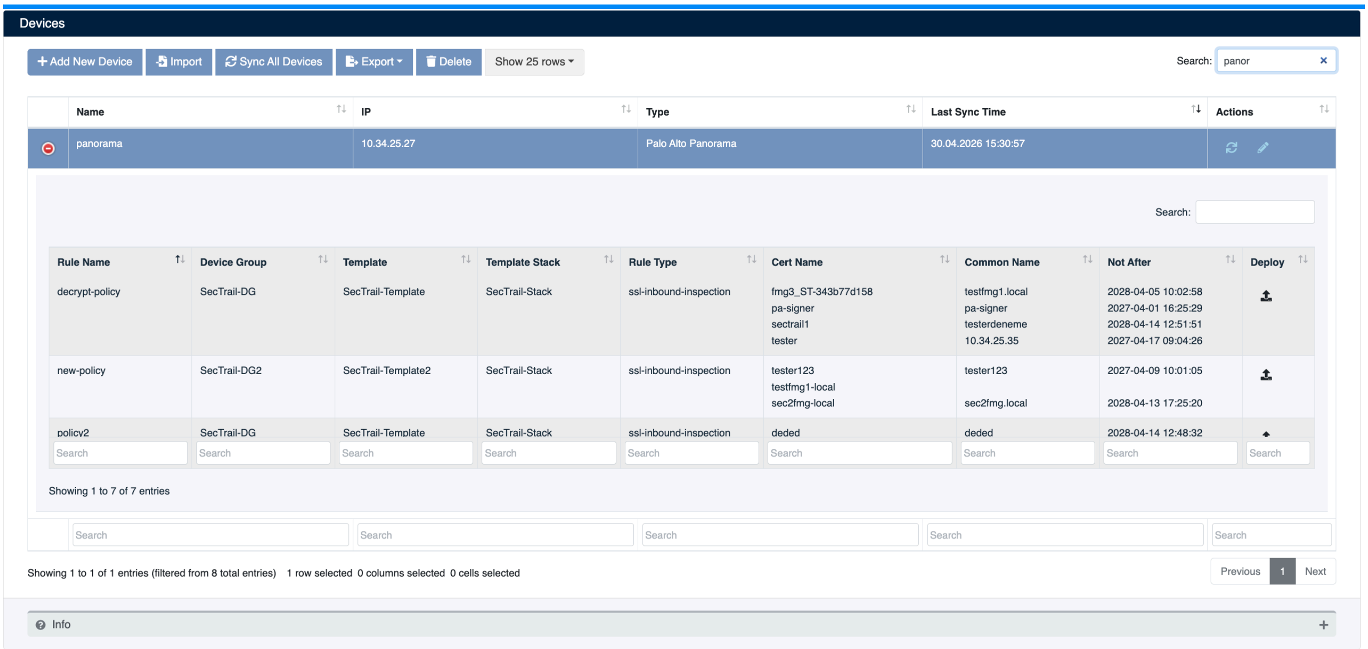


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: Panorama yönetim IP adresini girin
- **Device Type**: Açılır menüden `Panorama` seçin
- **Deployment Type**: Dağıtım tipini seçin
- **Append**: Var olan decryption rule'a yeni sertifikayı ekler (mevcut sertifikalar korunur)
- **Replace**: Mevcut sertifikayı yenisiyle değiştirir (eski sertifika silinir)
- **Skip Commit**: Değişiklikler commit edilsin mi? (Devre Dışı/Etkin)
- **Skip Push**: Sertifika karşı cihaza yüklensin mi? (Devre Dışı/Etkin)

> **OTOMATİK KEŞİF VE İZLEME**
>
> Panorama cihazı SecTrail CM'e eklendikten sonra, Panorama tarafından yönetilen tüm cihazlardaki sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



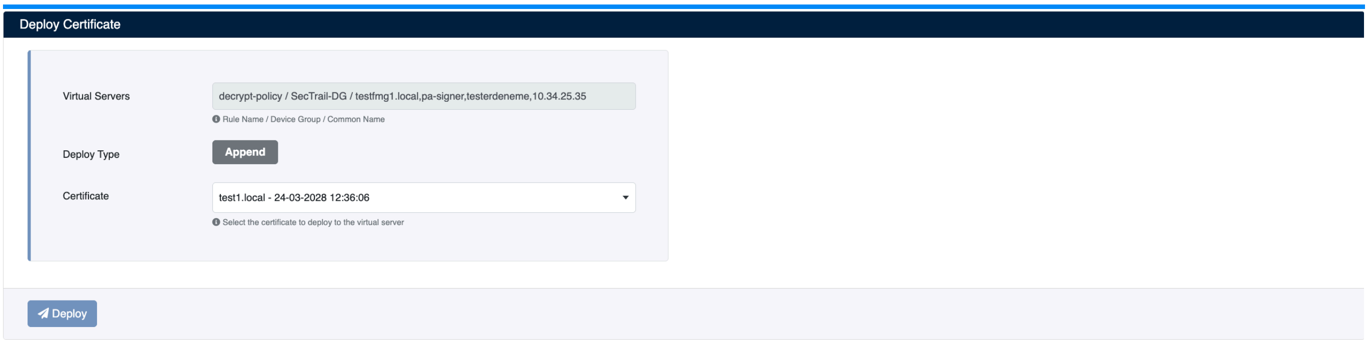
- **Rule Name**: Panorama üzerinde tanımlı kuralın adı
- **Device Group**: Sertifikanın ait olduğu cihaz grubu
- **Template**: Sertifikanın bağlı olduğu Panorama template adı
- **Template Stack**: Sertifikanın ait olduğu template stack adı
- **Rule Type**: Kuralın tipi (örn. decryption rule)
- **Cert Name**: Cihazda tanımlı sertifikanın adı
- **Common Name**: Sertifikanın Common Name (CN) bilgisi
- **Not After**: Sertifikanın son geçerlilik tarihi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Panorama cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server**'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir (Name/Destination/Subject formatında)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

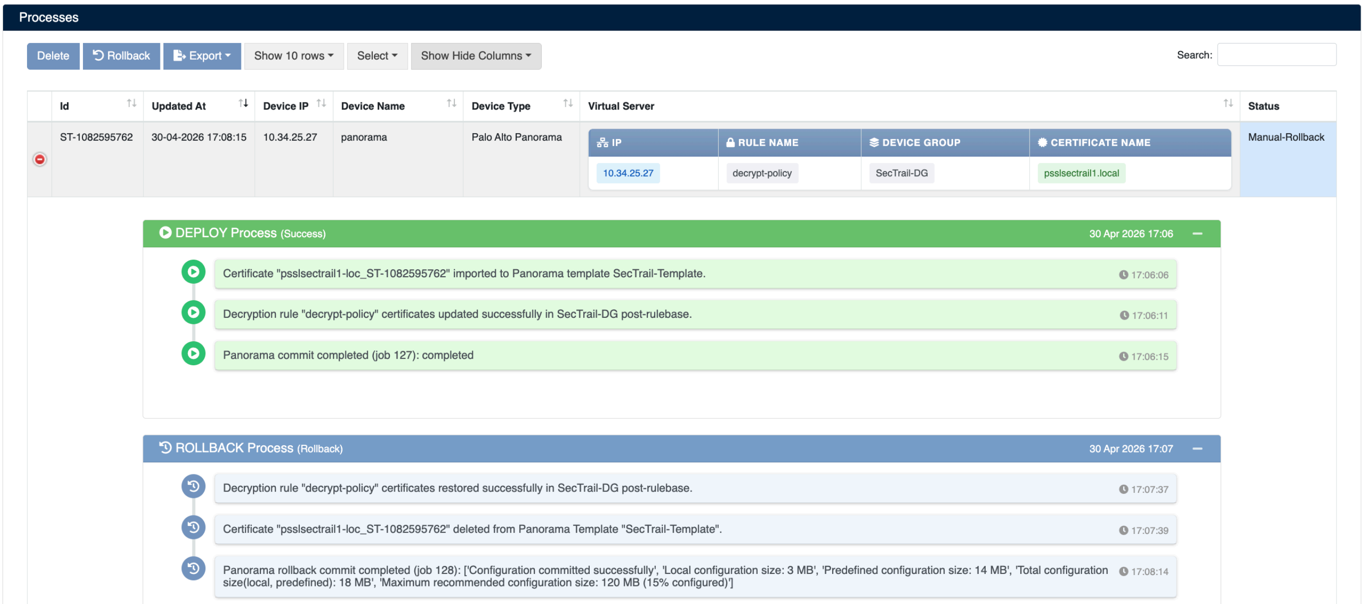


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika başarıyla güncellenir
2	Decryption kuralları yapılandırılır
3	Yapılandırma commit edilir
4	Yapılandırma başarıyla tamamlanır

> **COMMİT**
>
> **Skip Commit** devre dışı olduğunda SecTrail CM, dağıtım sonrasında yapılandırma değişikliklerini commit eder ve kalıcı hale getirir.

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Yeni yüklenen sertifika silinir
2	Önceki konfigürasyon geri yüklenir
3	Decryption kuralları eski haline getirilir
4	Geri alma işlemi başarıyla tamamlanır

FortiWeb

SecTrail CM, Fortinet FortiWeb Web Application Firewall (WAF) cihazlarına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	REST API (HTTPS)	FortiWeb'in native REST API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Basic Authentication	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	Administrator veya Certificate Manager	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, FortiWeb üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in güvenli transferi
2. **Certificate Chain Oluşturma**: Intermediate CA sertifikalarının zincir oluşturması
3. **Server Policy Güncelleme**: Server policy'deki sertifika referanslarının güncellenmesi
4. **SNI Members Güncelleme**: SNI bazlı sertifika atamaları
5. **Configuration Apply**: Yapılandırmanın aktif hale getirilmesi

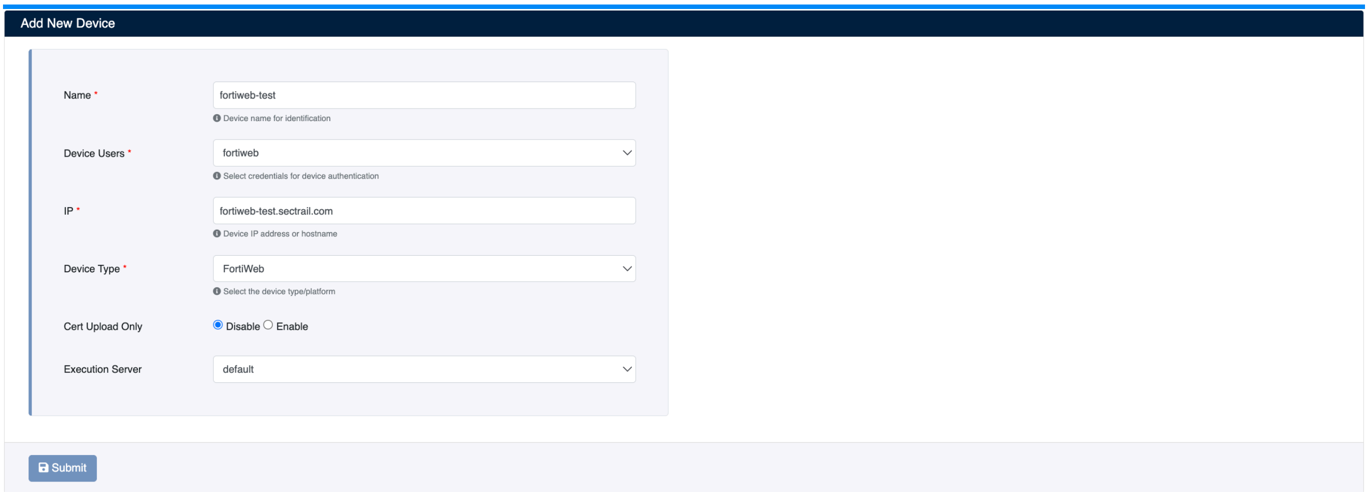
Yapılandırma Adımları

1. FortiWeb Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve FortiWeb için kullanıcı oluşturun.

2. FortiWeb Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

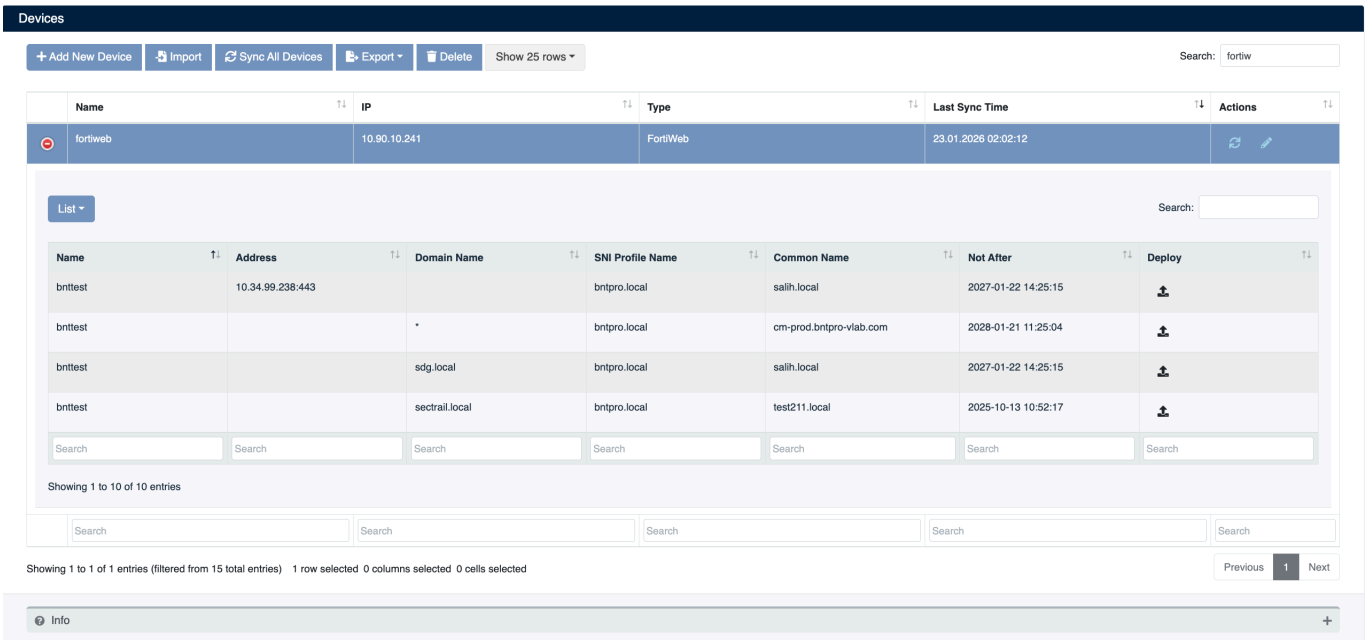


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: FortiWeb cihazının yönetim IP adresini girin
- **Device Type**: Açılır menüden `FortiWeb` seçin
- **Cert Upload Only**: Yalnızca sertifika yüklensin mi? (Devre Dışı/Etkin)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> FortiWeb cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Server Policy ve SNI'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



- **Server Policy**: FortiWeb cihazında tanımlı Server Policy adları

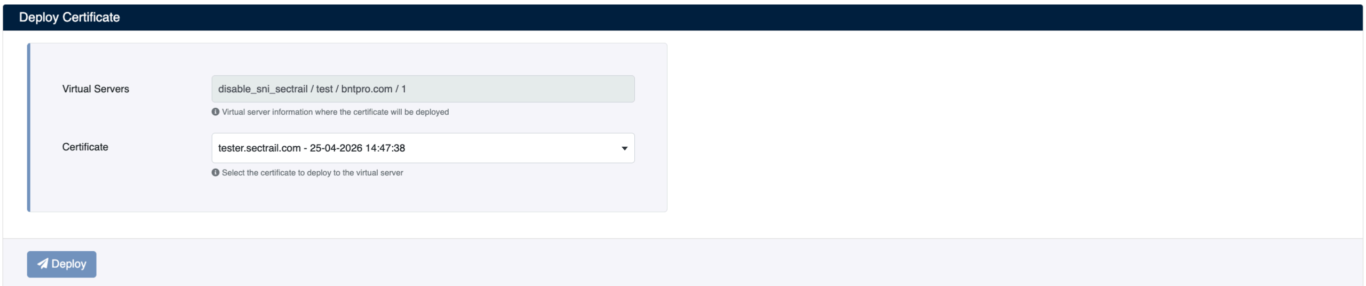
- **Type**: Policy tipini gösterir (Server-Policy veya SNI)
- **SNI**: Server Name Indication adı (SNI tipleri için)
- **Domain Name**: SNI profilinin İlişkili domain adı
- **Address**: Virtual server'ın IP adresi ve portu
- **Common Name**: Sertifikanın Common Name değeri
- **Not After**: Sertifika son geçerlilik tarihi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Server Policy ve Sertifika Seçimi

1. **Automation > Devices** bölümünden FortiWeb cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Server Policy** veya **SNI**'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Server Policy/SNI**: Hedef policy bilgisi görüntülenir
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

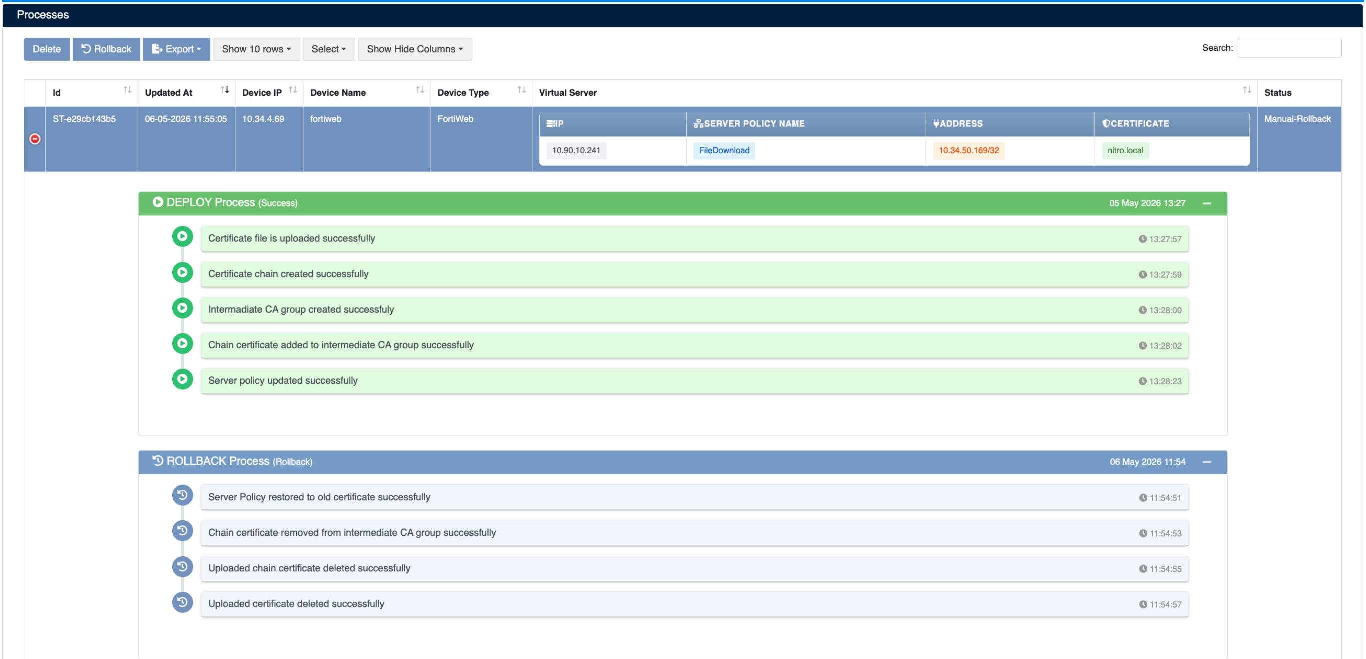


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

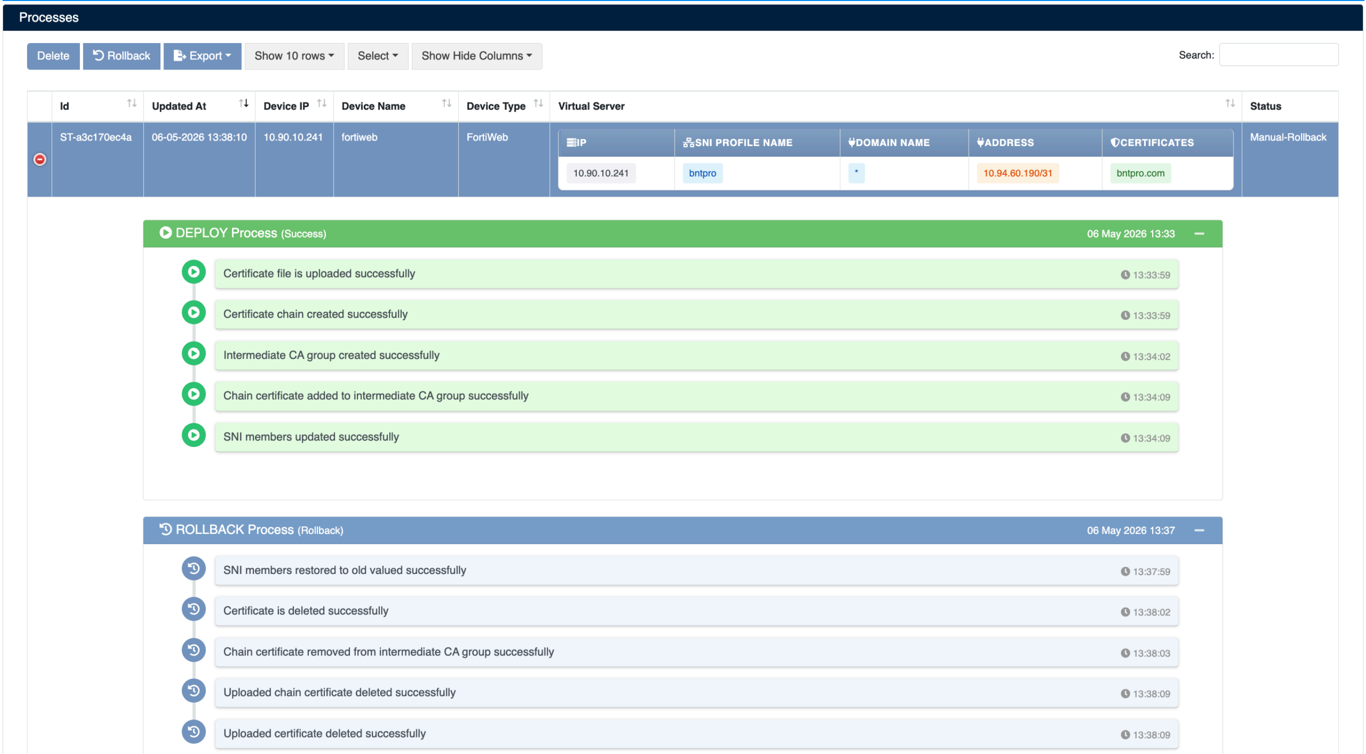
Adım	İşlem Açıklaması
1	Sertifika dosyası cihaza yüklenir
2	Sertifika zinciri oluşturulur
3	Intermediate CA grubu oluşturulur
4	Zincir sertifikası CA grubuna eklenir
5	Server policy yeni sertifika ile güncellenir

SERVER POLİCY İŞLEMLERİ

FortiWeb entegrasyonu, **Server Policy** bazlı sertifika güncellemelerini destekler. Dağıtım sırasında ilgili server policy'deki sertifika referansı otomatik olarak güncellenir.

SNI (Server Name Indication) Yönetimi

FortiWeb, SNI bazlı sertifika yönetimini destekler. SNI dağıtım işlemleri:



SNI İşlem Detayları

Adım	İşlem Açıklaması
1	Sertifika dosyası cihaza yüklenir
2	Sertifika zinciri oluşturulur
3	Intermediate CA grubu oluşturulur
4	Zincir sertifikası CA grubuna eklenir
5	SNI member sertifikası güncellenir

> **SNI OVERRİDE İŞLEMLERİ**
>
> SNI member güncellemelerinde, mevcut sertifika referansları yeni sertifika ile override edilir. Bu sayede domain bazlı sertifika yönetimi kolaylaşır.

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin

2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	Server Policy Rollback	SNI Rollback
1	Server policy eski sertifikaya geri alınır	SNI member eski sertifikaya geri alınır
2	Zincir sertifikası CA grubundan kaldırılır	Zincir sertifikası CA grubundan kaldırılır
3	Yüklenen zincir sertifikası silinir	Yüklenen zincir sertifikası silinir
4	Yüklenen sertifika silinir	Yüklenen sertifika silinir

FortiGate

SecTrail CM, FortiGate firewall cihazlarına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	REST API (HTTPS)	FortiGate'in native REST API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Username ve Password	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	Admin veya Certificate Manager role	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, FortiGate üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in cihaza güvenli transferi
2. **SSL Profile Update**: SSL inspection profile'larının güncellenmesi
3. **Policy Update**: Firewall policy'lerinin yeni profili kullanacak şekilde güncellenmesi
4. **Configuration Commit**: Konfigürasyonun kalıcı hale getirilmesi

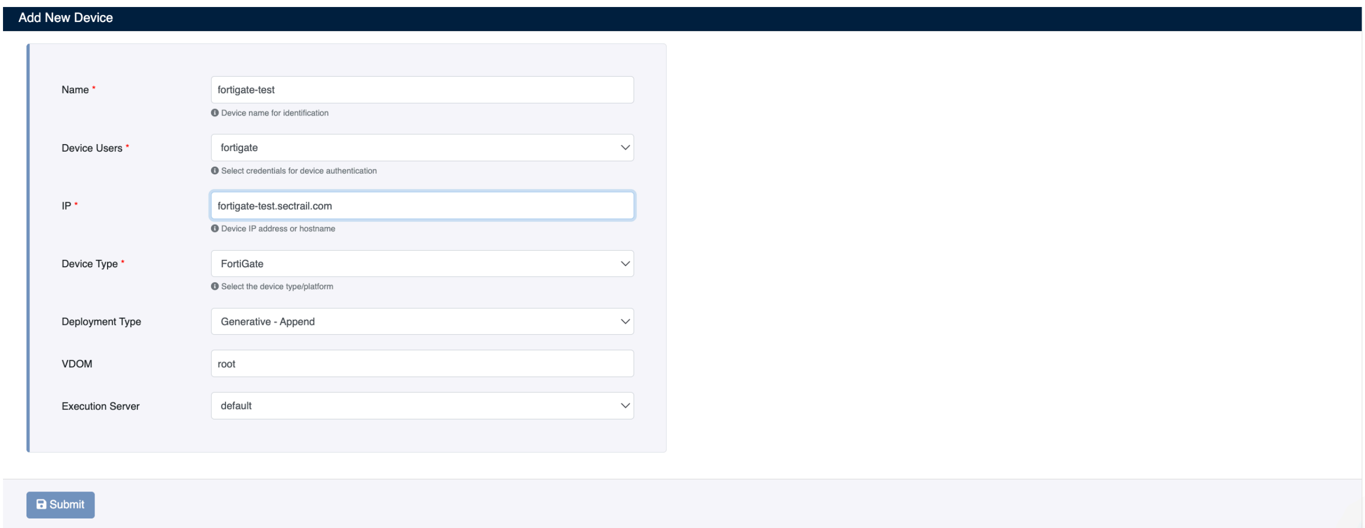
Yapılandırma Adımları

1. FortiGate Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve FortiGate için kullanıcı oluşturun.

2. FortiGate Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

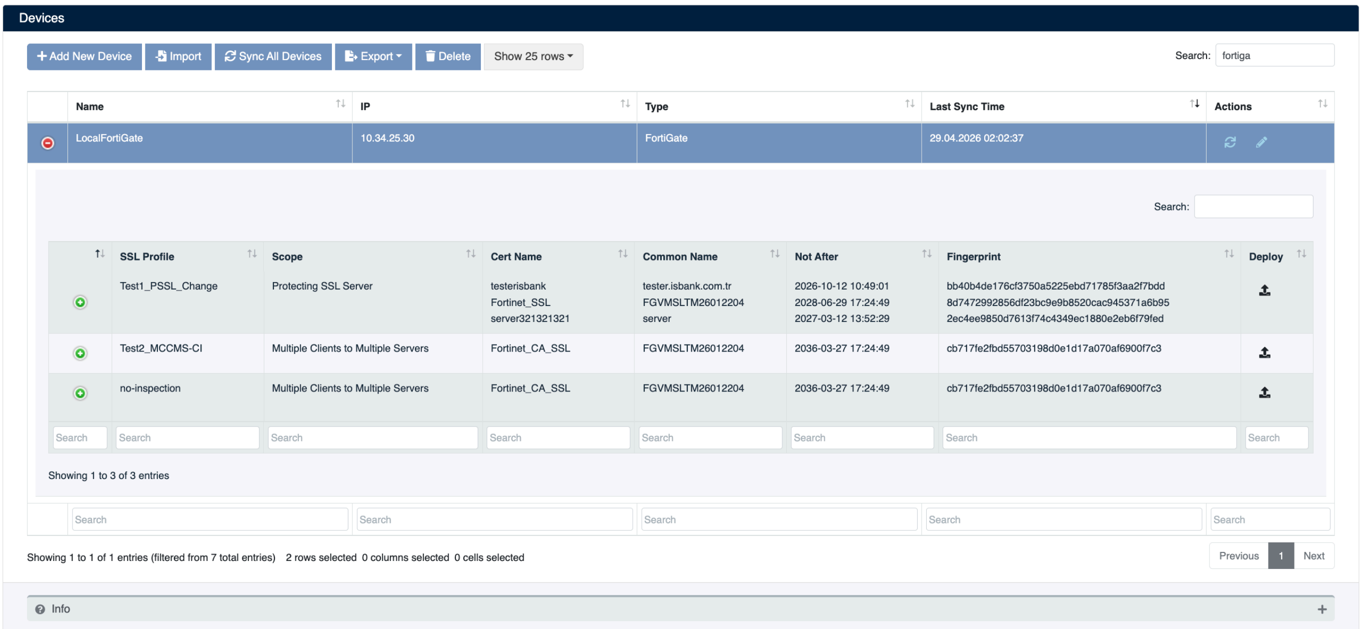


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: FortiGate cihazının IP adresi veya hostname'ini girin
- **Device Type**: Açılır menüden `FortiGate` seçin
- **Deployment Type**: Dağıtım tipini seçin
- **Generative - Append**: Yeni bir SSL profili oluşturur, bu profile yeni sertifikayı ekler ve eşleşen policy'lere bağlar
- **Generative - Replace**: Yeni bir SSL profili oluşturur, sertifikayı değiştirerek bu profile ekler ve eşleşen policy'lere bağlar
- **Override - Append**: Var olan SSL profile'a yeni sertifikayı ekler
- **Override - Replace**: Var olan SSL profile'daki sertifikayı kaldırır ve yerine yeni sertifikayı ekler
- **VDOM**: FortiGate VDOM adı (örn. `root`)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF VE İZLEME**
>
> FortiGate cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



- **SSL Profile**: Sertifika ile ilişkili SSL inspection profili adı
- **Scope**: SSL profilinin kapsamı (örn. Protecting SSL Server, Multiple Clients to Multiple Servers)
- **Cert Name**: Cihazda tanımlı sertifikanın adı
- **Common Name**: Sertifikanın Common Name (CN) bilgisi
- **Not After**: Sertifikanın son geçerlilik tarihi

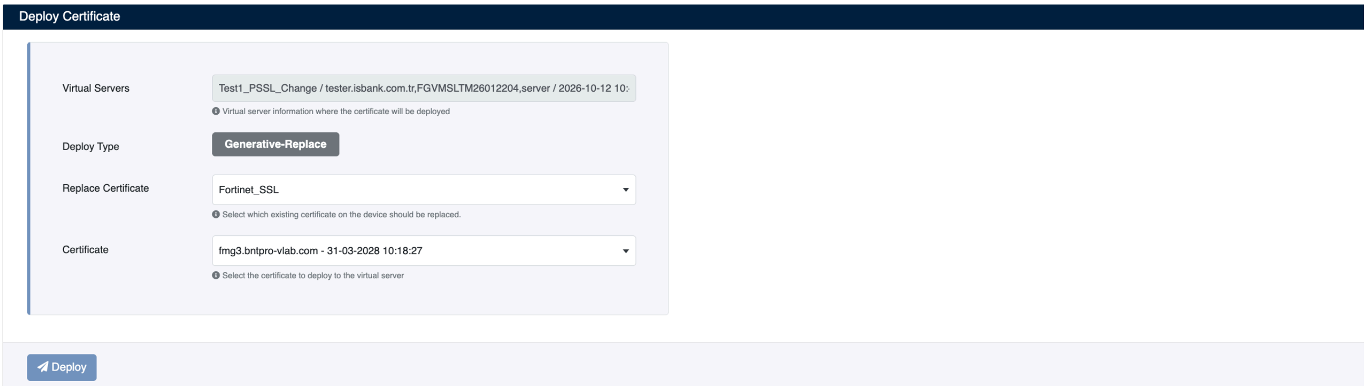
- **Fingerprint**: Sertifikanın parmak izi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: SSL Profile ve Sertifika Seçimi

1. **Automation > Devices** bölümünden FortiGate cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz SSL profile'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef virtual server bilgisi görüntülenir (SSL Profile / Common Name / Installation Target / Not After formatında)
- **Deploy Type**: Yapılandırılan dağıtım tipi görüntülenir (örn. Generative-Replace)
- **Replace Certificate**: Cihazda değiştirilecek mevcut sertifikayı seçin
- **Certificate**: Açılır menüden dağıtmak istediğiniz yeni sertifikayı seçin

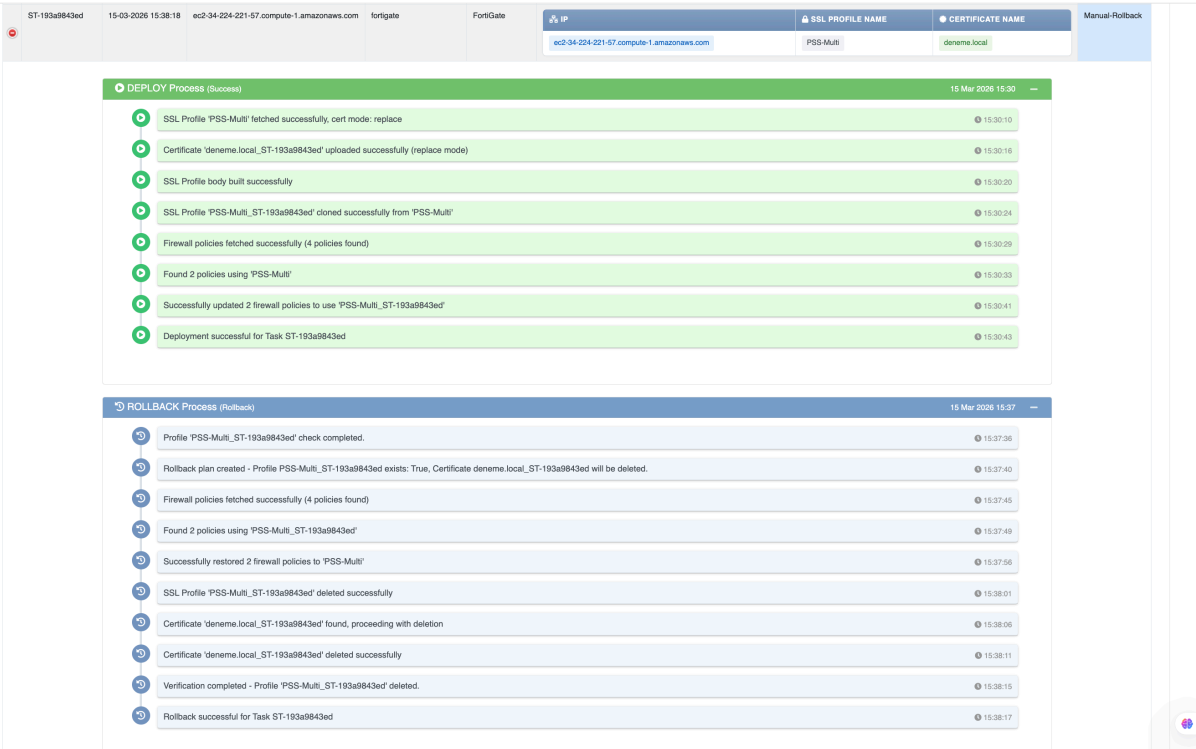


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	SSL profili alınır ve cert mode belirlenir
2	Sertifika cihaza yüklenir
3	SSL profil gövdesi oluşturulur
4	SSL profili kaydedilir
5	Firewall policy'leri alınır
6	Eşleşen policy'ler yeni profili kullanacak şekilde güncellenir
7	Dağıtım başarıyla tamamlanır

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun

3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Rollback planı oluşturulur ve silinecek sertifika belirlenir
2	Firewall policy'leri alınır
3	Eşleşen policy'ler eski profile geri döndürülür
4	Yeni SSL profili silinir
5	Sertifika cihazdan silinir
6	Geri alma başarıyla tamamlanır

FortiManager

SecTrail CM, FortiManager merkezi yönetim platformuna **ajansız** bağlantı kurarak yönetilen tüm FortiGate cihazlarına SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	REST API (HTTPS)	FortiManager'ın native REST API'si kullanılır
Port	`443`	Standart HTTPS portu veya custom management port
Kimlik Doğrulama	Username ve Password	Username ve Password ile kimlik doğrulama
Kullanıcı Yetkisi	Admin veya Certificate Manager role	Sertifika yükleme ve yapılandırma yetkisi

Otomatik İşlemler

SecTrail CM, FortiManager üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası ve private key'in ADOM local store'a güvenli transferi
2. **Certificate Import**: Sertifika ve key'in FortiManager üzerinden yönetilen cihazlara dağıtılması
3. **SSL Profile Update**: SSL inspection profile'larının güncellenmesi
4. **Policy Install**: Güncellenen policy'lerin hedef cihazlara yüklenmesi
5. **Configuration Commit**: Workspace'in commit edilmesi ve yapılandırmanın kalıcı hale getirilmesi

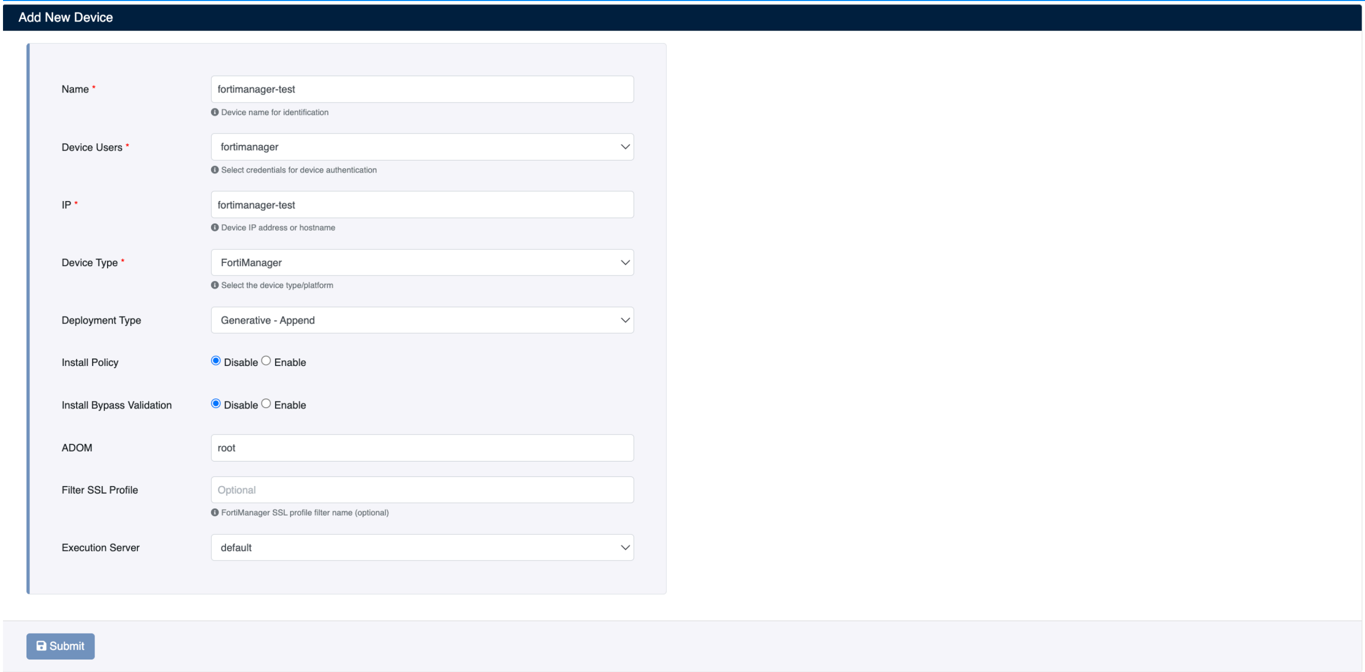
Yapılandırma Adımları

1. FortiManager Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve FortiManager için kullanıcı oluşturun.

2. FortiManager Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

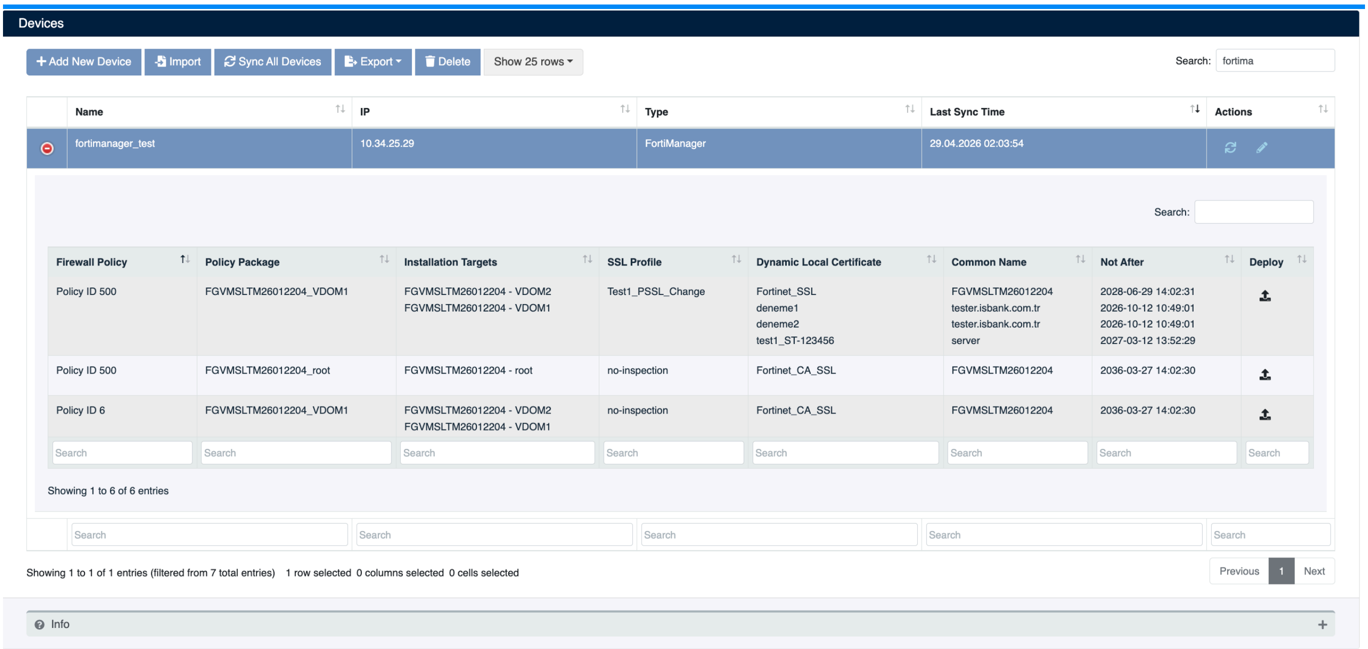


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: FortiManager yönetim IP adresi veya hostname'i girin
- **Device Type**: Açılır menüden `FortiManager` seçin
- **Deployment Type**: Dağıtım tipini seçin
- **Generative - Append**: Yeni bir SSL profili oluşturur, bu profile yeni sertifikayı ekler ve eşleşen policy'lere bağlar
- **Generative - Replace**: Yeni bir SSL profili oluşturur, sertifikayı değiştirerek bu profile ekler ve eşleşen policy'lere bağlar
- **Override - Append**: Var olan SSL profile'a yeni sertifikayı ekler
- **Override - Replace**: Var olan SSL profile'daki sertifikayı kaldırır ve yerine yeni sertifikayı ekler
- **Install Policy**: Güncellenen policy'ler cihazlara yüklensin mi? (Devre Dışı/Etkin)
- **Install Bypass Validation**: Policy yüklemesi sırasında doğrulama atlanabilsin mi? (Devre Dışı/Etkin)
- **ADOM**: FortiManager ADOM adı (örn. `root`)
- **Filter SSL Profile**: FortiManager SSL profil filtre adı (opsiyonel)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF VE İZLEME**
>
> FortiManager cihazı SecTrail CM'e eklendikten sonra, FortiManager tarafından yönetilen tüm cihazlardaki sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



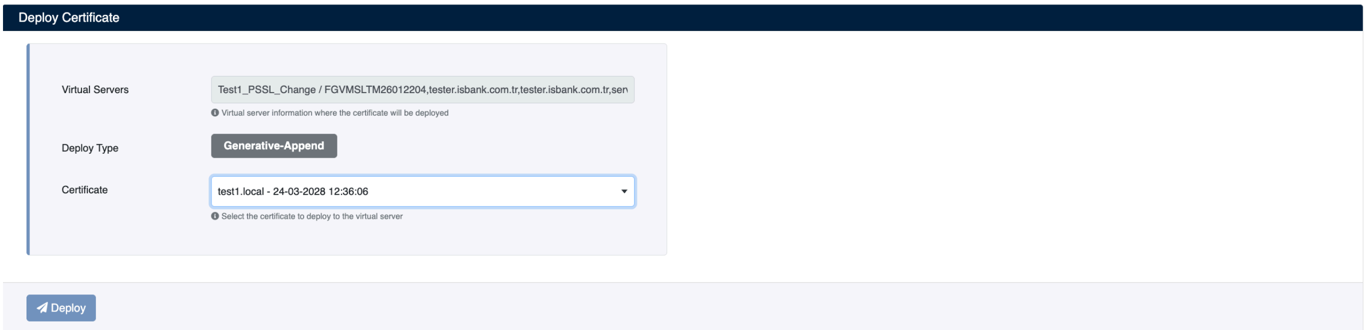
- **Firewall Policy**: Sertifika ile ilişkili firewall policy'sinin adı
- **Policy Package**: Kuralın ait olduğu policy paketi
- **Installation Targets**: Policy'nin yükleneceği hedef FortiGate cihazları
- **SSL Profile**: Sertifika ile ilişkili SSL inspection profili adı
- **Dynamic Local Certificate**: Yönetilen cihazlardaki dynamic local certificate eşleşmeleri
- **Common Name**: Sertifikanın Common Name (CN) bilgisi
- **Not After**: Sertifikanın son geçerlilik tarihi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden FortiManager cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz policy'yi bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef virtual server bilgisi görüntülenir (SSL Profile / Installation Targets / Common Name formatında)
- **Deploy Type**: Yapılandırılan dağıtım tipi görüntülenir (örn. Generative-Append)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

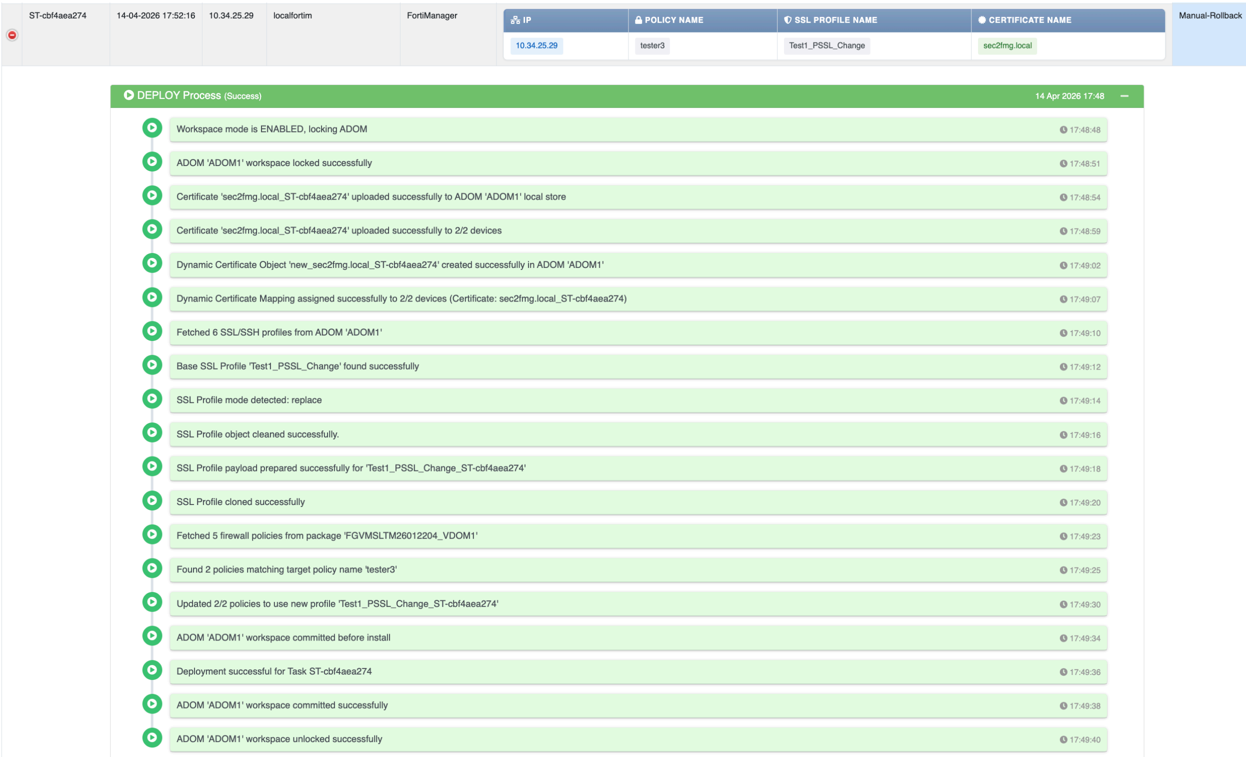


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Workspace modu etkinleştirilir, ADOM kilitleniir
2	Sertifika ADOM local store'a yüklenir
3	Sertifika yönetilen cihazlara dağıtılır
4	ADOM'da Dynamic Certificate Object oluşturulur
5	Dynamic Certificate Mapping cihazlara atanır
6	SSL profili alınır ve klonlanır
7	SSL profil payload'ı hazırlanır ve uygulanır
8	Firewall policy'leri yeni profili kullanacak şekilde güncellenir
9	ADOM workspace commit edilir ve policy yüklenir
10	ADOM workspace başarıyla kilidi açılır

> **COMMİT**
>
> SecTrail CM, dağıtım öncesinde ADOM workspace'i kilitler, işlem tamamlandıktan sonra tüm değişiklikleri commit eder ve workspace kilidini açar. **Install Policy** etkinse güncellenen policy hedef FortiGate cihazlarına da iletilir.

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Workspace modu etkinleştirilir, ADOM kilitleniir
2	ADOM'dan SSL profilleri alınır
3	Firewall policy'leri base profile'a geri döndürülür
4	SSL profili başarıyla silinir
5	Dynamic mapping'ler yönetilen cihazlardan silinir
6	Dynamic Certificate Object silinir
7	Sertifika ADOM ve cihaz veritabanlarından silinir
8	ADOM workspace başarıyla commit edilir
9	ADOM workspace başarıyla kilidi açılır

IIS (Internet Information Services)

SecTrail CM, Windows IIS (Internet Information Services) web sunucularına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	WinRM (Windows Remote Management)	Windows Remote Management protokolü kullanılır
Port	`5986` / `5985`	Güvenli bağlantı için HTTPS portu önerilir
Transport	NTLM / Kerberos / CredSSP	Windows kimlik doğrulama mekanizmaları
Kimlik Doğrulama	Domain hesabı / Local Administrator	Windows kullanıcı kimlik bilgileri

Otomatik İşlemler

SecTrail CM, Windows IIS üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Certificate Store Import**: Sertifika ve private key'in Windows Certificate Store'a güvenli transferi
2. **IIS Binding Update**: Virtual Server (Web Site) SSL binding'lerinin güncellenmesi
3. **Configuration Backup**: Değişiklik öncesi yapılandırmanın yedeklenmesi
4. **SSL Validation**: HTTPS bağlantı testi ve doğrulama

Yapılandırma Adımları

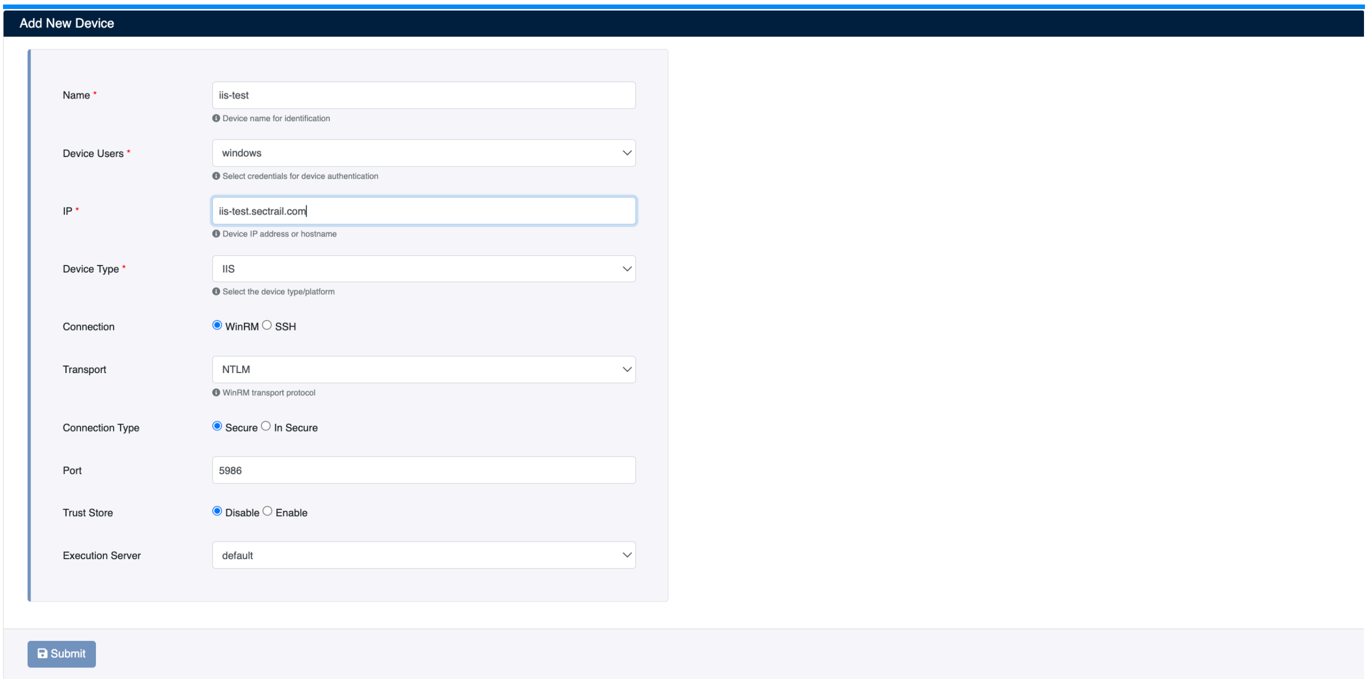
1. IIS Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve IIS için kullanıcı oluşturun:

- Windows domain kullanıcısı
- Veya local administrator

2. IIS Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

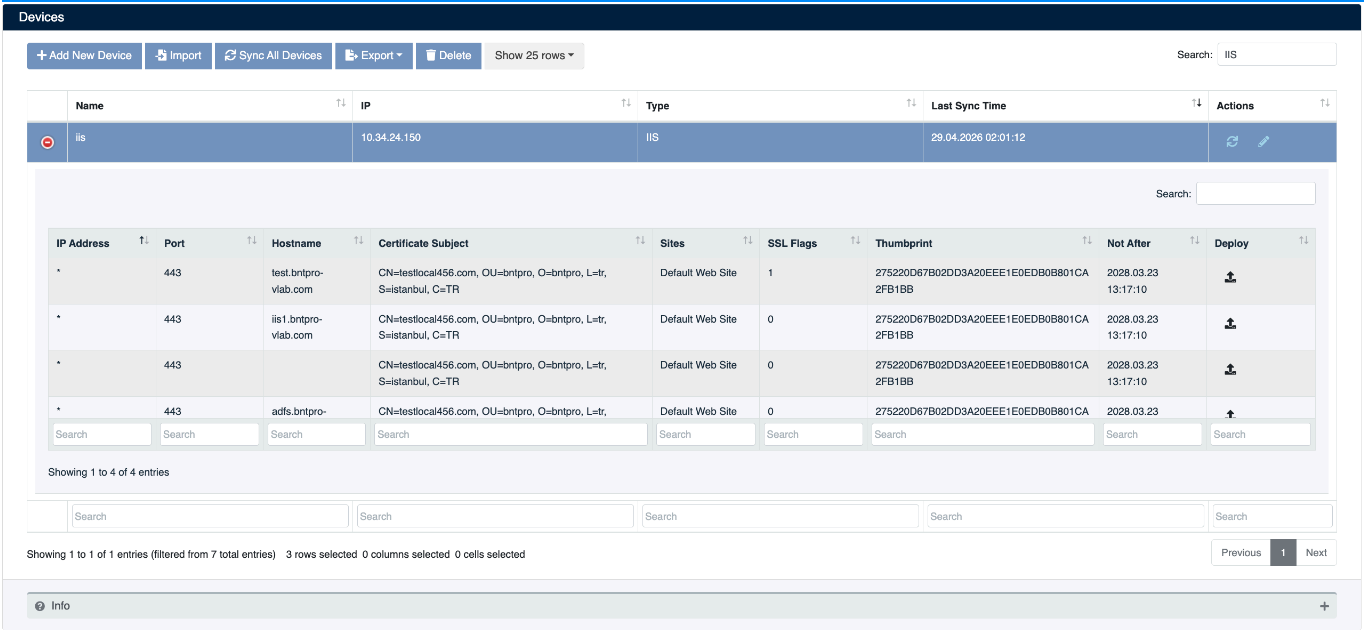


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz Windows kullanıcısını seçin
- **IP**: Windows IIS sunucusunun IP adresini girin
- **Device Type**: Açılır menüden `IIS` seçin
- **Connection**: `WinRM` veya `SSH` seçeneklerinden birini seçin
- **Transport**: NTLM veya Kerberos seçeneklerinden birini seçin
- **Connection Type**: Güvenli bağlantı için `Secure` seçin
- **Port**: WinRM portu (varsayılan: `5986` HTTPS veya `5985` HTTP)
- **Trust Store**: Trust Store dahil edilsin mi? `Devre Dışı` veya `Etkin`
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> IIS cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Web Site'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



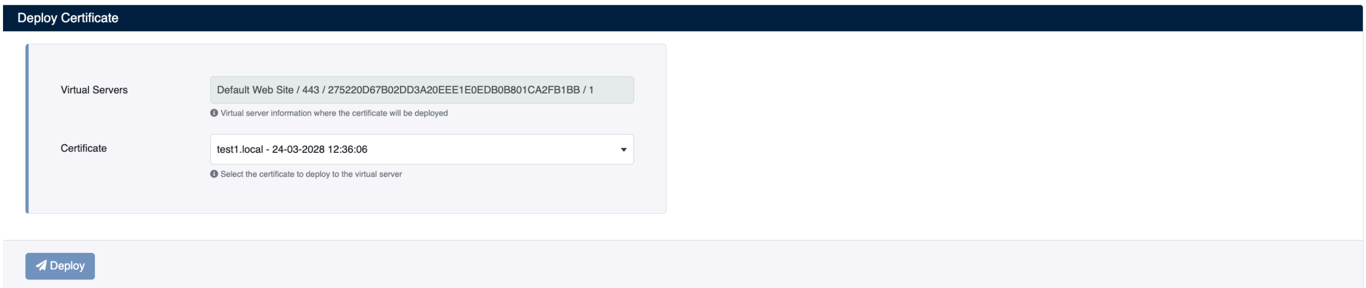
- **IP Address**: IIS sunucusunun IP adresi
- **Port**: HTTPS portu (443)
- **Hostname**: IIS web sitesinin hostname bilgisi
- **Certificate Subject**: Mevcut sertifikanın subject (CN) bilgisi
- **Sites**: IIS site adı (Default Web Site veya özel site adı)
- **SSL Flags**: SSL flag değeri (0: SNI yok, 1: SNI var)
- **Thumbprint**: Mevcut sertifikanın thumbprint değeri
- **Not After**: Sertifikanın son geçerlilik tarihi
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden IIS cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server** (Web Site binding)'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir (Hostname, IP, Port)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

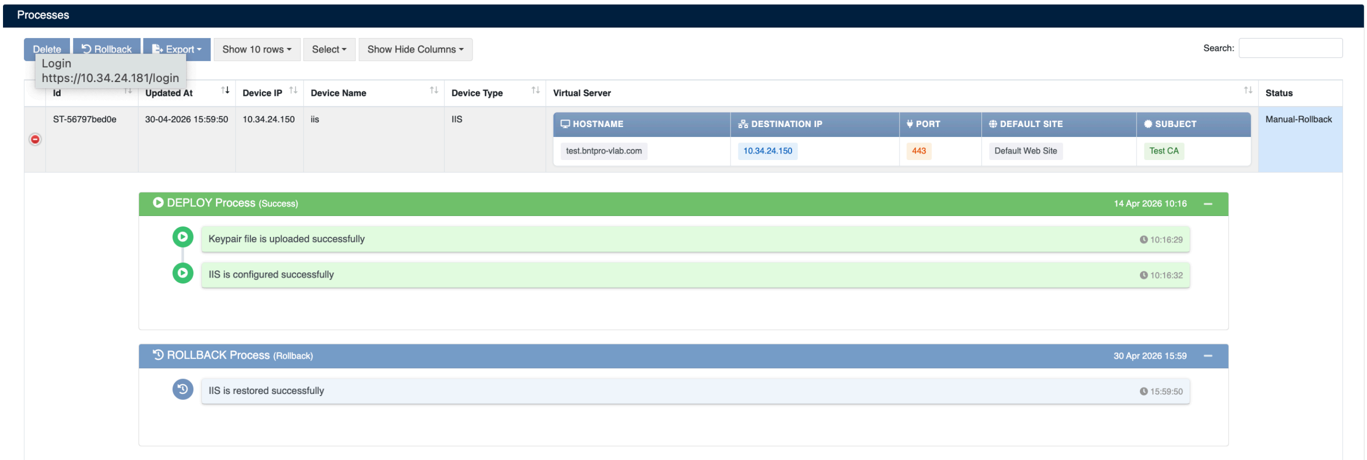


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika PFX formatında Windows Certificate Store'a import edilir
2	IIS web sitesi SSL binding yapılandırması güncellenir

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	IIS web sitesi SSL binding'i önceki durumuna geri alınır
2	Eski sertifika bağlantısı restore edilir

Apache HTTP Server

SecTrail CM, Apache HTTP Server'lara **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	SSH (Secure Shell)	Güvenli uzak bağlantı protokolü
Port	`22`	Standart SSH portu veya custom port
Kimlik Doğrulama	SSH Key veya Password	SSH anahtarı veya şifre ile kimlik doğrulama
Kullanıcı Yetkisi	Konfigürasyon okuma/yazma yetkisi	Apache config dosyalarına erişim ve düzenleme yetkisi

Otomatik İşlemler

SecTrail CM, Apache HTTP Server üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası, private key ve chain dosyasının güvenli transferi
2. **Konfigürasyon Güncelleme**: Apache VirtualHost SSL direktiflerinin güncellenmesi
3. **Konfigürasyon Testi**: Sözdizimi kontrolü ve doğrulama
4. **Servis Yenileme**: Apache servisinin kesintisiz yeniden yüklenmesi

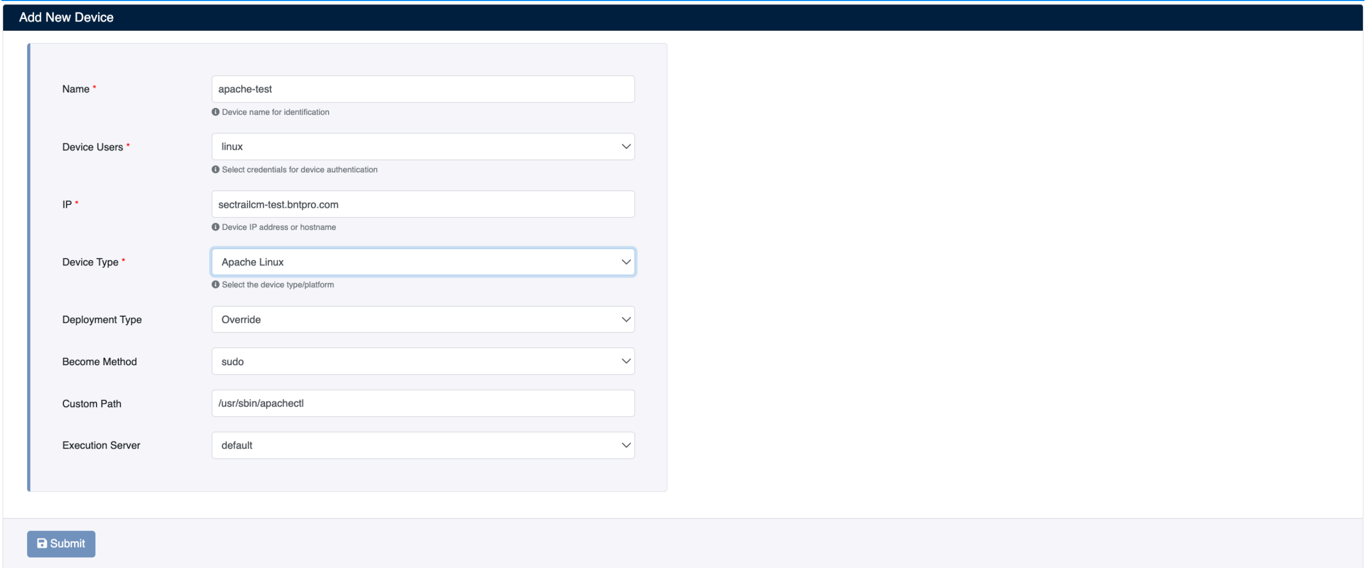
Yapılandırma Adımları

1. Apache Linux Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Apache için kullanıcı oluşturun.

2. Apache Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

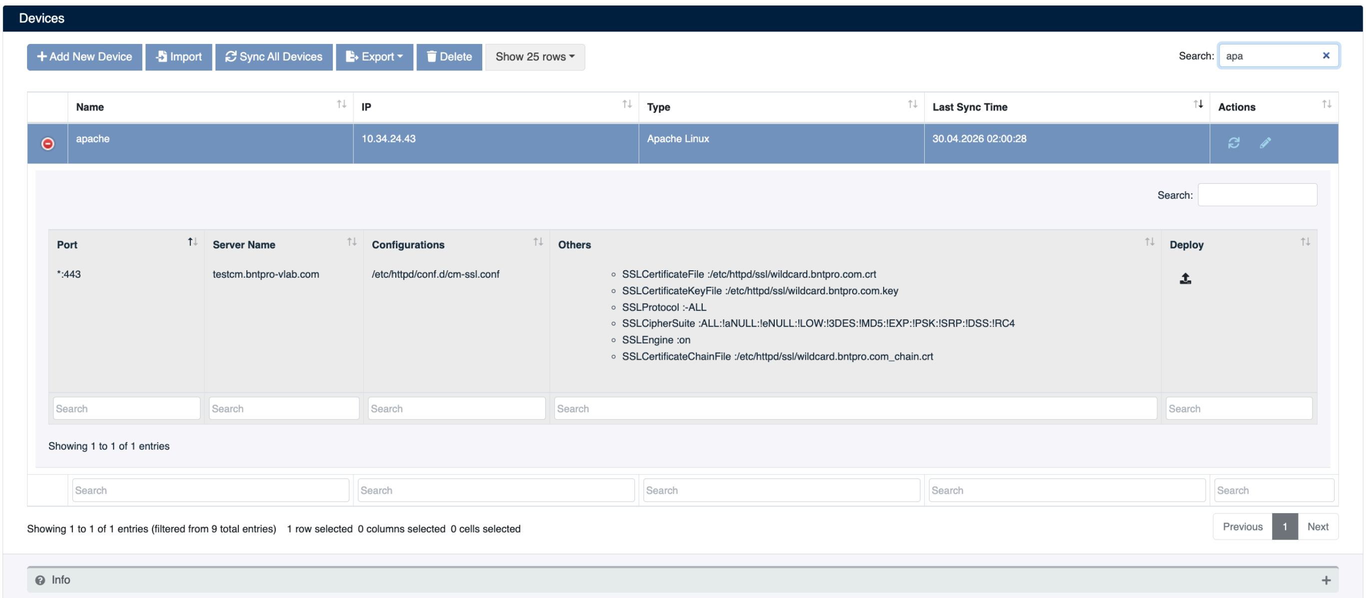


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: Apache sunucusunun IP adresini girin
- **Device Type**: Açılır menüden `Apache Linux` seçin
- **Become Method**: Yetki yükseltme yöntemini seçin
- **Custom Path**: Apache binary dosyasının yolunu girin (örn: `/usr/sbin/apachectl`)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> Apache cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Virtual Host'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



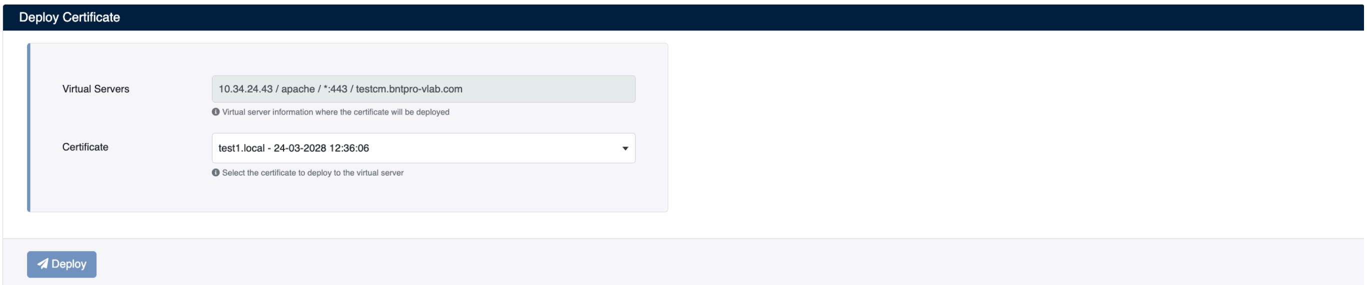
- **Port**: Apache'nin dinlediği portlar (örn: `*:443`, `*:444`)
- **Server Name**: VirtualHost server name veya `*` (tüm hostlar)
- **Configurations**: Apache konfigürasyon dosyası yolu (örn: `/etc/httpd/conf.d/cm-ssl.conf`)
- **Others**: Mevcut SSL konfigürasyon detayları
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Virtual Host ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Apache cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Host**'u bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Host bilgisi görüntülenir (IP, port, server name)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

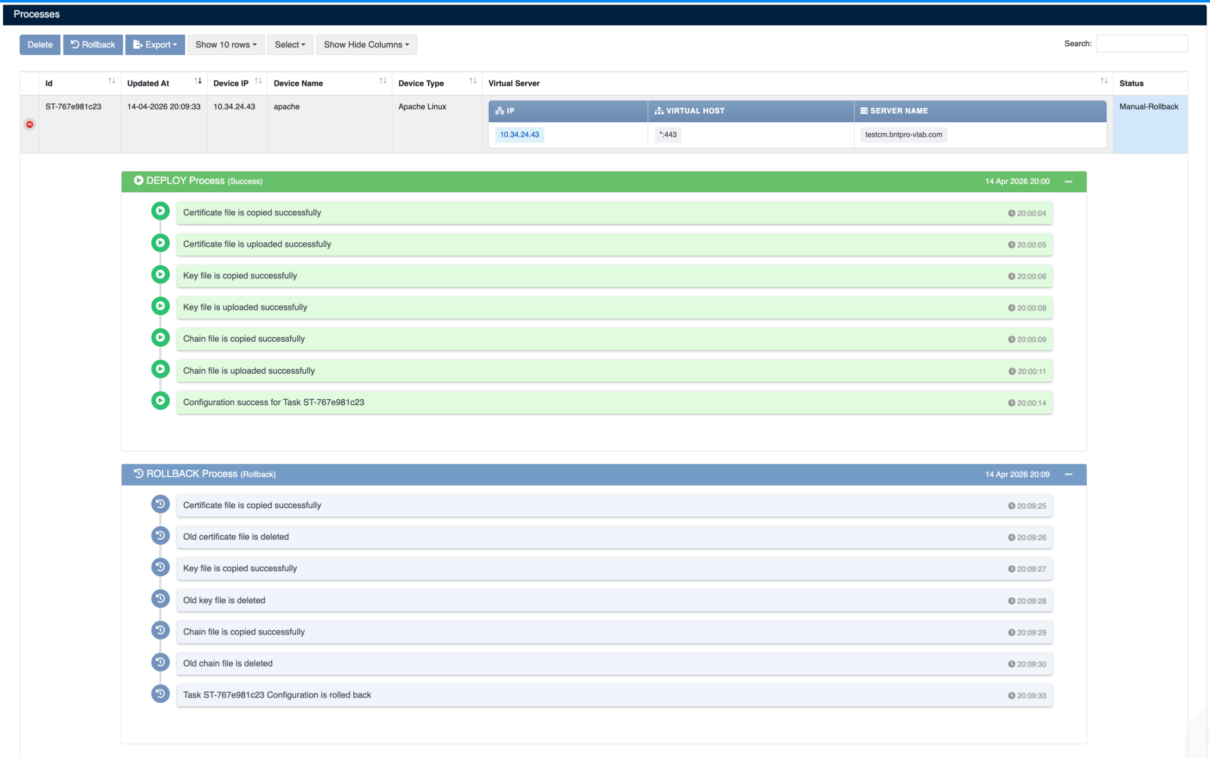


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika, key ve chain dosyaları sunucuya yüklenir
2	Mevcut sertifika dosyaları yedeklenir
3	Yeni sertifika konfigürasyonu uygulanır
4	Apache servisi yeniden yüklenir (reload)

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Yeni konfigürasyon kaldırılır
2	Yedeklenen sertifika dosyaları geri yüklenir
3	Yeni yüklenen sertifika, key ve chain dosyaları silinir
4	Apache servisi yeniden yüklenir (reload)

NGINX

SecTrail CM, NGINX web sunucularına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	SSH (Secure Shell)	Güvenli uzak bağlantı protokolü
Port	`22`	Standart SSH portu veya custom port
Kimlik Doğrulama	SSH Key veya Password	SSH anahtarı veya şifre ile kimlik doğrulama
Kullanıcı Yetkisi	Konfigürasyon okuma/yazma yetkisi	NGINX config dosyalarına erişim ve düzenleme yetkisi

Otomatik İşlemler

SecTrail CM, NGINX üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Sertifika ve Key Yükleme**: SSL sertifikası, private key ve chain dosyasının güvenli transferi
2. **Konfigürasyon Güncelleme**: NGINX Server Block SSL direktiflerinin güncellenmesi
3. **Konfigürasyon Testi**: Sözdizimi kontrolü ve doğrulama
4. **Servis Yenileme**: NGINX servisinin kesintisiz yeniden yüklenmesi

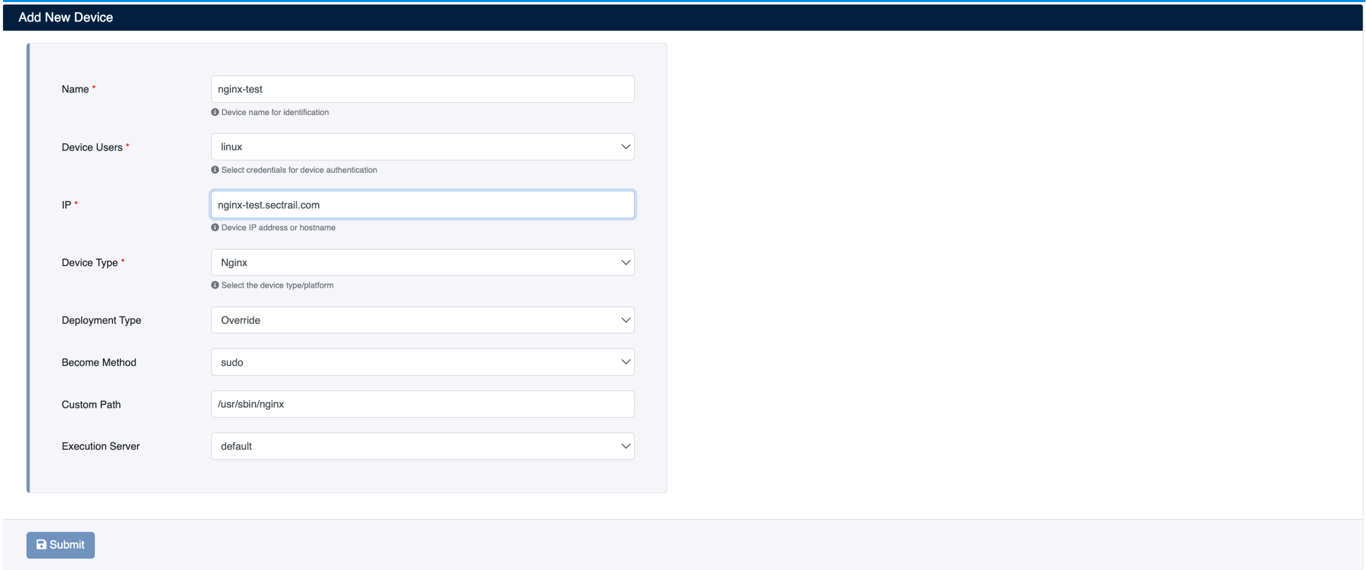
Yapılandırma Adımları

1. NGINX Linux Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve NGINX için kullanıcı oluşturun.

2. NGINX Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

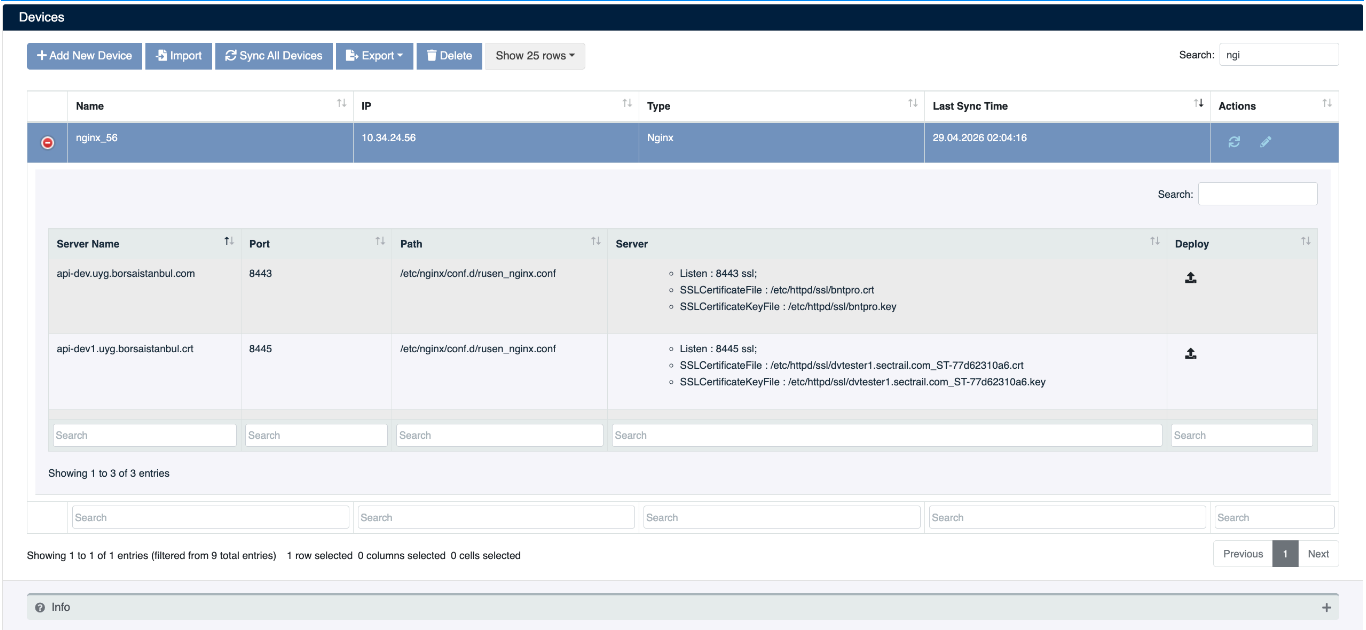


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: NGINX sunucusunun IP adresini girin
- **Device Type**: Açılır menüden `Nginx` seçin
- **Become Method**: Yetki yükseltme yöntemini seçin (örn: `sudo`)
- **Custom Path**: NGINX binary dosyasının yolunu girin (örn: `/usr/sbin/nginx`)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> NGINX cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Server Block'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



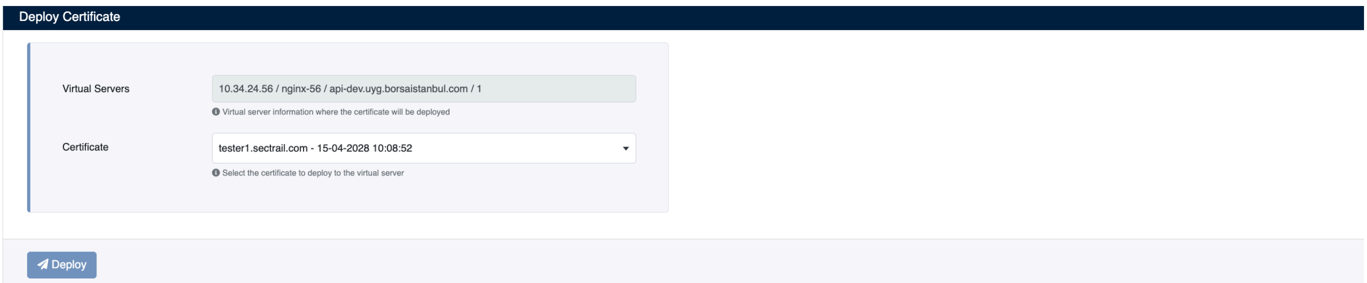
- **Server Name**: Server block server name (örn: `sectrailcm-test.borsaistanbul.com`)
- **Port**: NGINX'in dinlediği portlar (örn: `8443`)
- **Path**: NGINX konfigürasyon dosyası yolu (örn: `/etc/nginx/conf.d/domain_nginx.conf`)
- **Server**: SSL konfigürasyon detayları
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: Server Block ve Sertifika Seçimi

1. **Automation > Devices** bölümünden NGINX cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Server Block**'u bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Server Block bilgisi görüntülenir (IP, port, server name)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

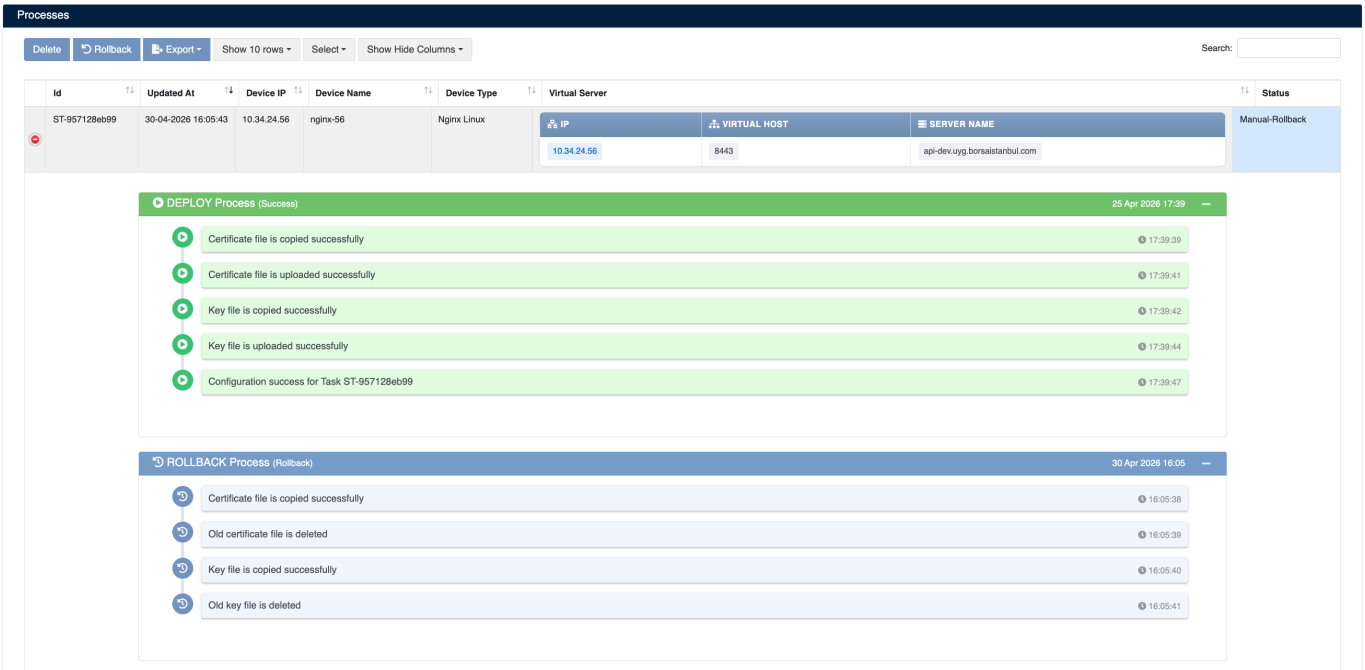


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika, key ve chain dosyaları sunucuya yüklenir
2	Mevcut sertifika dosyaları yedeklenir
3	Yeni sertifika konfigürasyonu uygulanır
4	NGINX servisi yeniden yüklenir (reload)

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

> **OTOMATİK GERİ ALMA**
>
> Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Yeni konfigürasyon kaldırılır
2	Yedeklenen sertifika dosyaları geri yüklenir
3	Yeni yüklenen sertifika, key ve chain dosyaları silinir
4	NGINX servisi yeniden yüklenir (reload)

Apache Tomcat

SecTrail CM, Apache Tomcat application server'larına **ajansız** bağlantı kurarak SSL sertifikalarının otomatik dağıtımını ve yenilenmesini sağlar.

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	SSH (Secure Shell)	Güvenli uzak bağlantı protokolü
Port	`22` (varsayılan)	Standart SSH portu veya custom port
Kimlik Doğrulama	SSH Key veya Password	SSH anahtarı veya şifre ile kimlik doğrulama
Kullanıcı Yetkisi	Keystore ve restart yetkisi	Java keystore oluşturma ve Tomcat yeniden başlatma yetkisi

Otomatik İşlemler

SecTrail CM, Apache Tomcat üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Keystore Yönetimi**: Java KeyStore (JKS/PKCS12) oluşturma ve güncelleme
2. **Sertifika Import**: SSL sertifikası ve private key'in keystore'a eklenmesi
3. **Konfigürasyon Güncelleme**: Tomcat server.xml SSL connector ayarlarının güncellenmesi
4. **Servis Yenileme**: Tomcat servisinin yeniden başlatılması

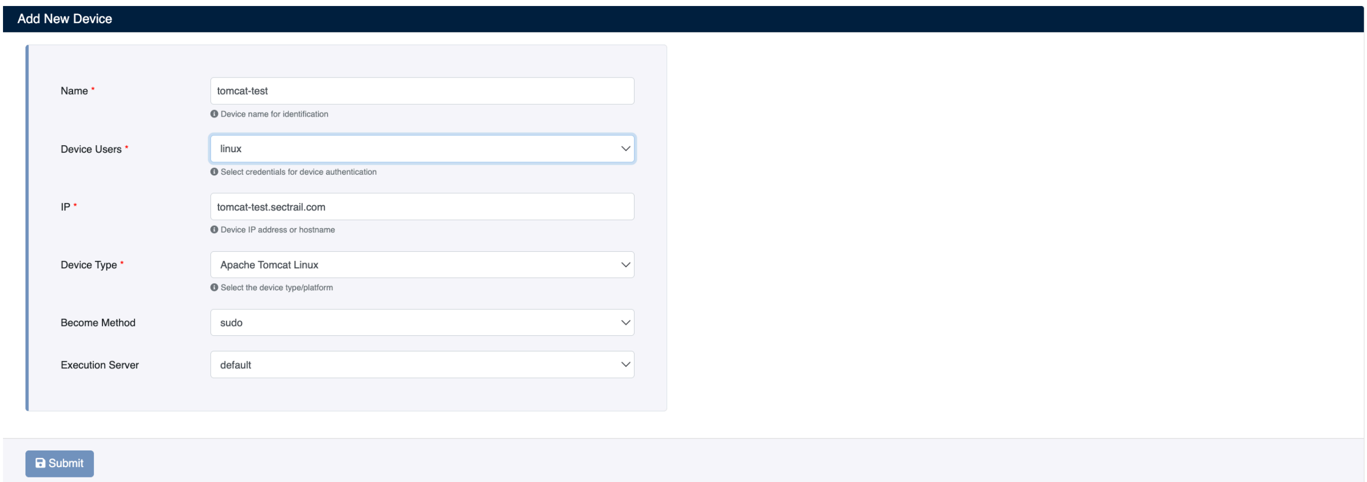
Yapılandırma Adımları

1. Tomcat Linux Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Tomcat için kullanıcı oluşturun.

2. Tomcat Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

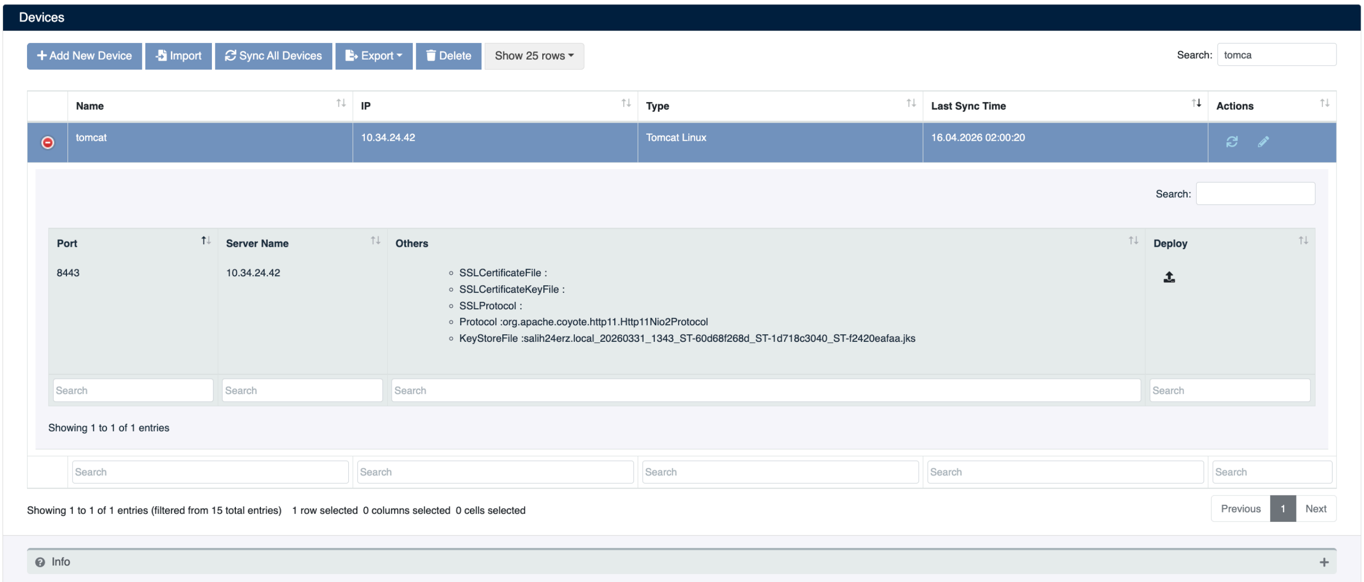


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: Tomcat sunucusunun IP adresini girin
- **Device Type**: Açılır menüden `Apache Tomcat Linux` seçin
- **Become Method**: Yetki yükseltme yöntemini seçin (örn: `sudo`)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF**
>
> Tomcat cihazı SecTrail CM'e eklendikten sonra, cihazda tanımlı tüm Virtual Server'ların IP adresleri ve portları otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



- **Port**: Tomcat'in dinlediği SSL portları (örn: `8446` , `8448`)
- **Server Name**: Virtual server IP adresi (örn: `10.34.24.42`)
- **Others**: Mevcut SSL konfigürasyon detayları:
- **Deploy**: Sertifika dağıtımı için

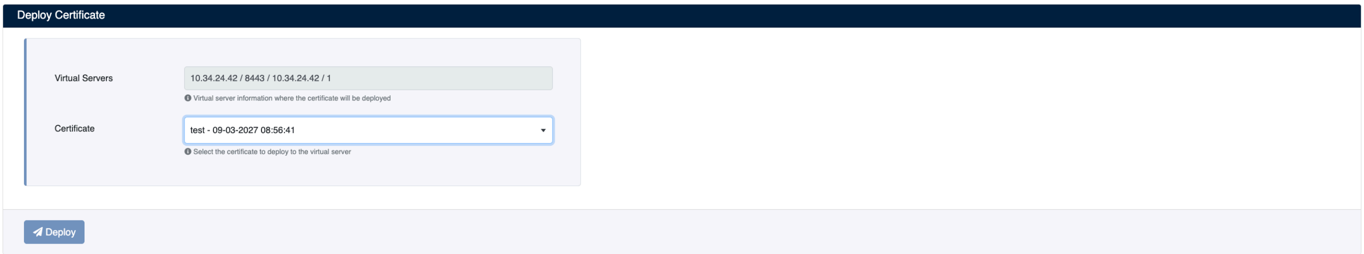
Sertifika Dağıtımı

Adım 1: Virtual Server ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Tomcat cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **Virtual Server**'ı bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef Virtual Server bilgisi görüntülenir (IP ve port)

- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

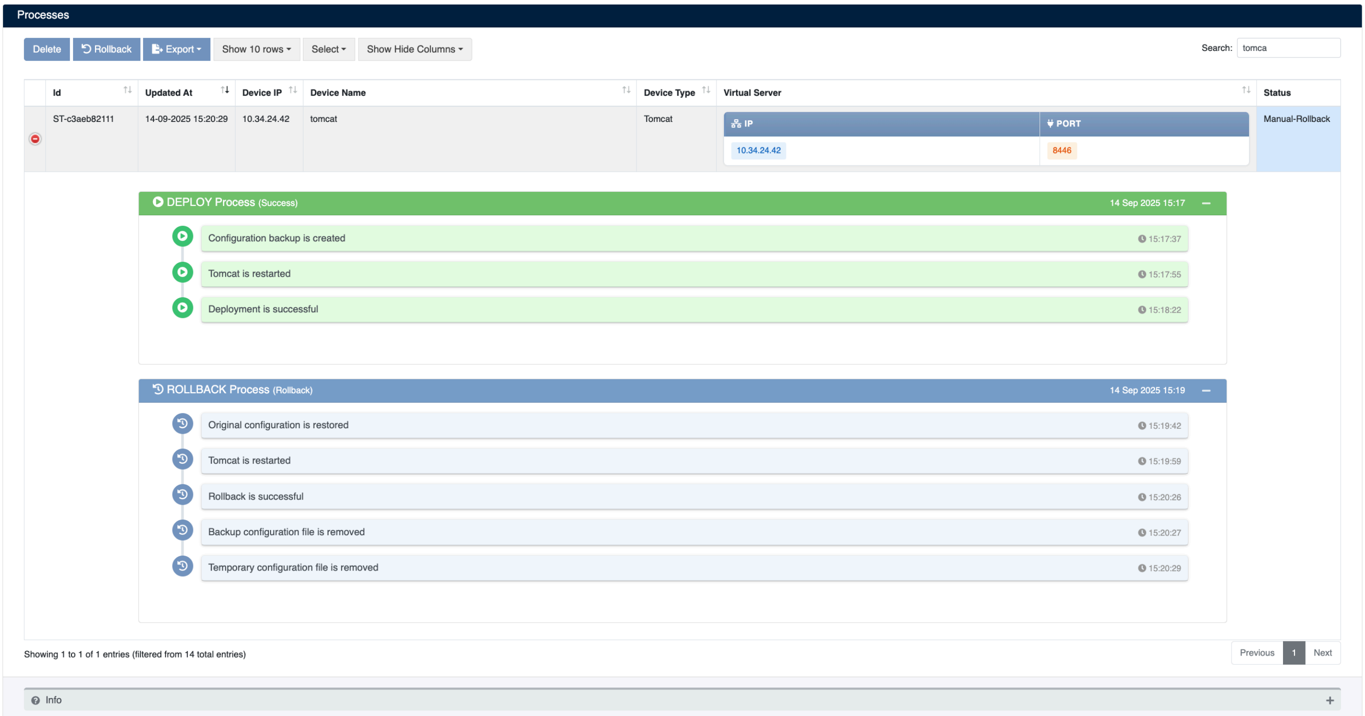


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Konfigürasyon yedekleme dosyası oluşturulur
2	JKS (Java KeyStore) dosyası oluşturulur ve sertifika yüklenir
3	Konfigürasyon dosyası içerisinde değişiklik yapılır
4	Tomcat servisi yeniden başlatılır

Geri Alma İşlemi

Sertifika dağıtımı sonrasında sorun yaşanması durumunda **Manual Rollback** özelliği kullanılabilir.

OTOMATİK GERİ ALMA

Dağıtım işlemi sırasında herhangi bir adımda hata oluşması durumunda, sistem otomatik olarak geri alma işlemini gerçekleştirir ve tüm değişiklikler geri alınır.

Geri Alma Adımları

1. **Automation > Processes** bölümüne gidin
2. Geri almak istediğiniz işlemi bulun
3. **Status** sütununda **Manual-Rollback** seçeneğini kullanın
4. Onay verin

Geri Alma Sırasında Gerçekleşen İşlemler

Adım	İşlem
1	Orijinal konfigürasyon geri yüklenir
2	Tomcat servisi yeniden başlatılır
3	Yeni oluşturulan keystore dosyası kaldırılır
4	Yedek ve geçici dosyalar temizlenir

Java Keystore (JKS)

SecTrail CM, Java Keystore (JKS/PKCS12) kullanan uygulamalara **ajansız** bağlantı kurarak SSL sertifikalarının otomatik yönetimini sağlar.

> **PLATFORM DESTEĞİ**
>
> SecTrail CM, hem **Linux** hem de **Windows** sistemlerinde çalışan Java KeyStore'ları destekler. Her iki platform için de otomatik sertifika dağıtımı ve yönetimi yapabilirsiniz.

Kullanım Alanları

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

Bağlantı Gereksinimleri

Linux Sistemler

Gereksinim	Detay	Açıklama
Protokol	SSH (Secure Shell)	Güvenli uzak bağlantı protokolü
Port	`22`	Standart SSH portu veya custom port
Kimlik Doğrulama	SSH Key veya Password	SSH anahtarı veya şifre ile kimlik doğrulama
Kullanıcı Yetkisi	Keystore okuma/yazma yetkisi	Keystore dosyalarına erişim ve düzenleme yetkisi

Windows Sistemler

Gereksinim	Detay	Açıklama
Protokol	WinRM (Windows Remote Management)	Windows uzak yönetim protokolü
Port	`5985` (HTTP) / `5986` (HTTPS)	Standart WinRM portları
Kimlik Doğrulama	Username ve Password	Windows kullanıcı kimlik doğrulama
Kullanıcı Yetkisi	Keystore okuma/yazma yetkisi	Keystore dosyalarına erişim ve düzenleme yetkisi

Otomatik İşlemler

SecTrail CM, Java KeyStore üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Keystore Backup**: Mevcut keystore'un yedeğini alma
2. **Certificate Import**: `keytool` ile yeni sertifika ve private key import

3. **Truststore Update**: Root/Intermediate CA sertifikalarını truststore'a ekleme
4. **Validation**: SSL/TLS bağlantı testi ve doğrulama

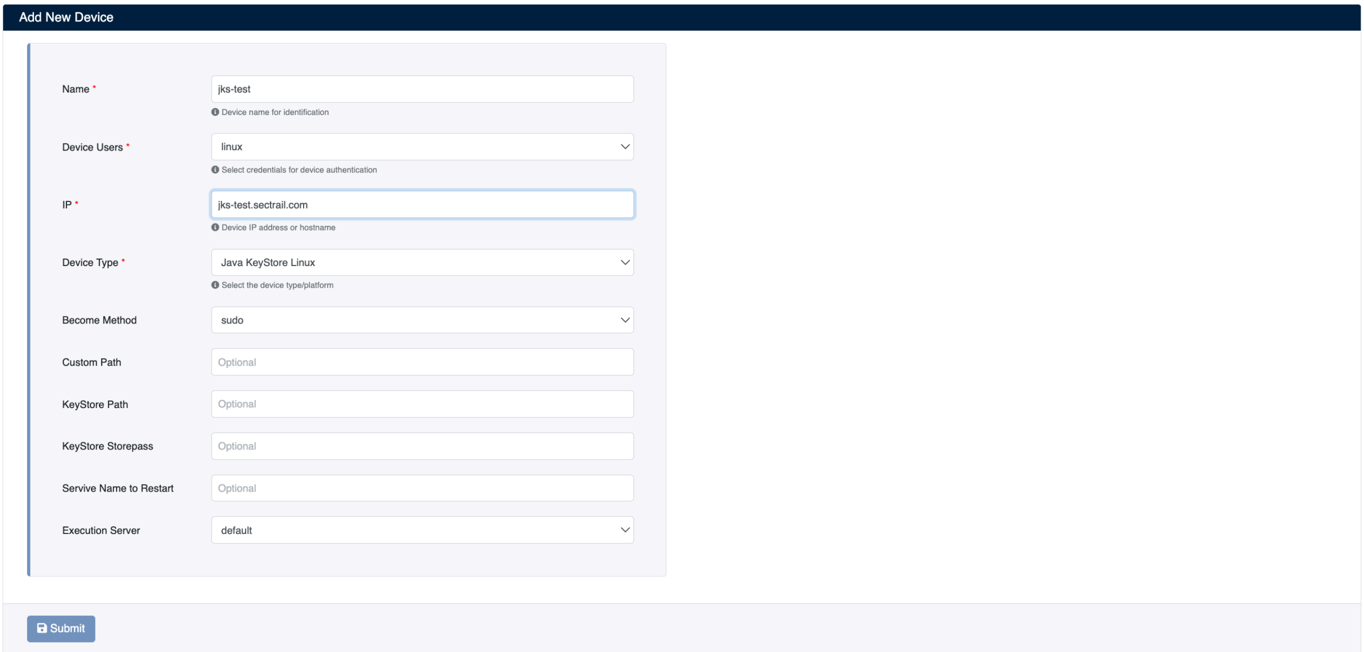
Yapılandırma Adımları

1. Java KeyStore Linux Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Java KeyStore için kullanıcı oluşturun.

2. Java KeyStore Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:

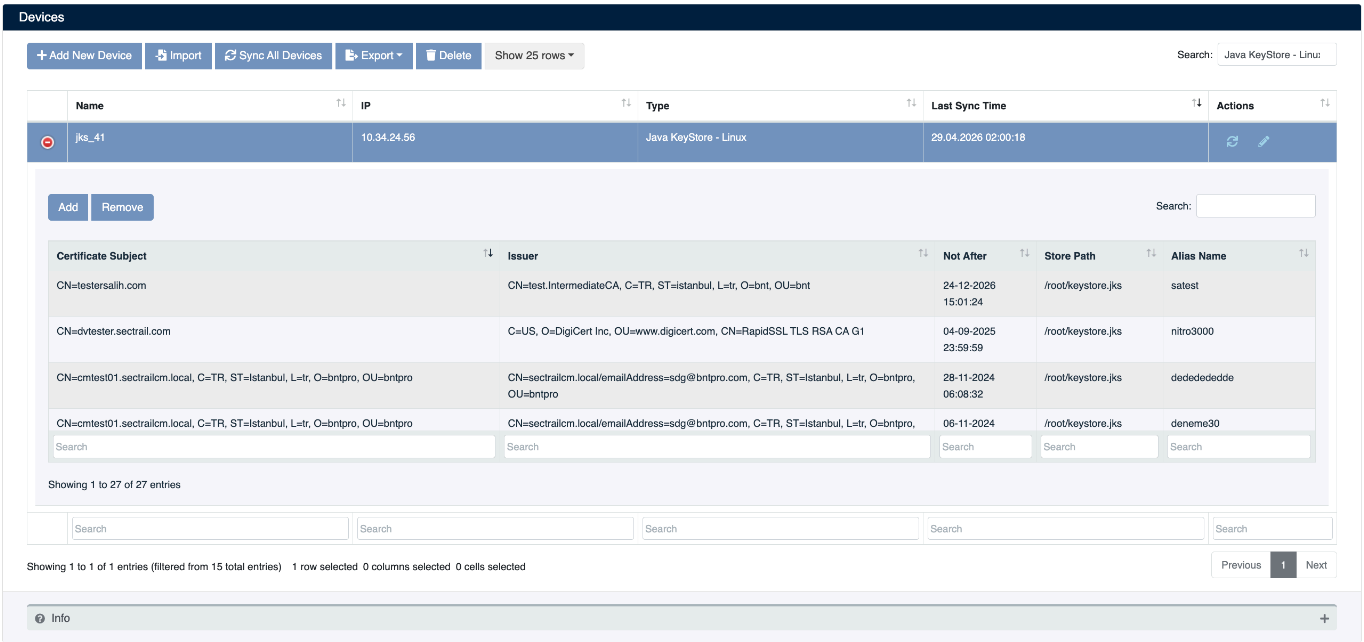


- **Name**: Cihaz için tanımlayıcı isim verin
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin
- **IP**: Java KeyStore sunucusunun IP adresini girin
- **Device Type**: Açılır menüden `Java KeyStore Linux` seçin
- **Become Method**: Yetki yükseltme yöntemini seçin (örn: `sudo`)
- **Custom Path**: (Opsiyonel) Custom path belirtebilirsiniz
- **KeyStore Path**: KeyStore dosyasının yolunu girin
- **KeyStore Storepass**: KeyStore şifresini girin
- **Servive Name to Restart**: (Opsiyonel) Yeniden başlatılacak servis adını girin
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF VE İZLEME**
>
> Java KeyStore cihazı SecTrail CM'e eklendikten sonra, KeyStore içindeki sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



Cihaz detaylarında aşağıdaki bilgiler görüntülenir:

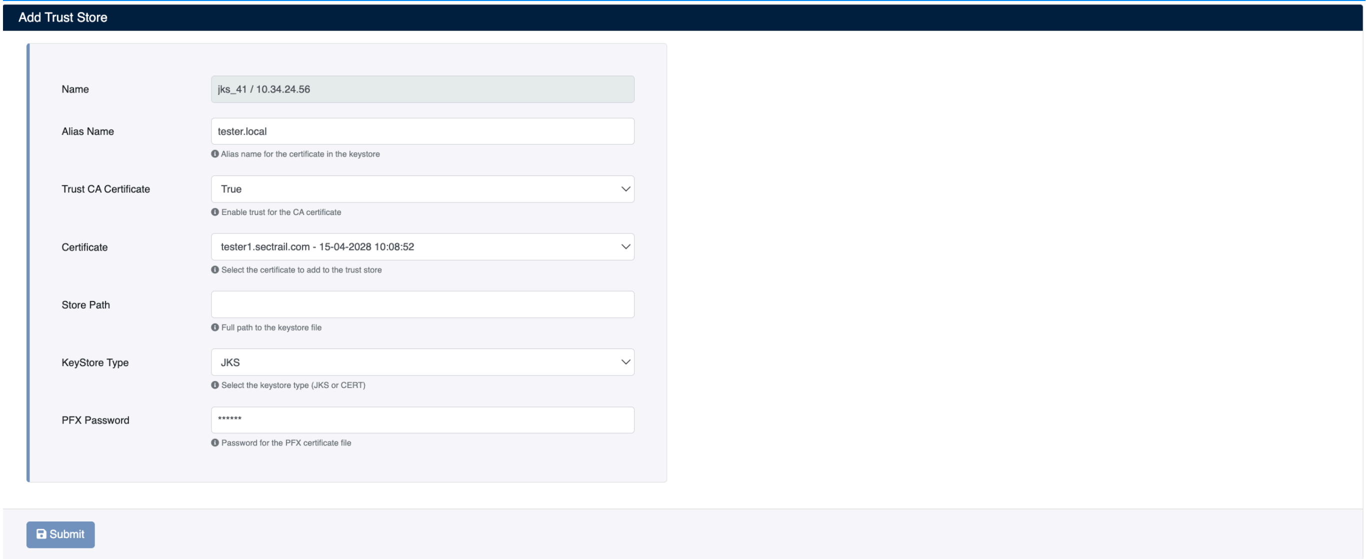
- **Certificate Subject**: Sertifika özne bilgileri (CN, ST, L, O, OU)
- **Issuer**: Sertifikayı veren CA bilgileri
- **Not After**: Sertifika geçerlilik son tarihi
- **Store Path**: KeyStore dosya yolu
- **Alias Name**: Sertifika alias adı
- **Deploy**: Sertifika dağıtımı için

Sertifika Dağıtımı

Adım 1: KeyStore ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Java KeyStore cihazınızı seçin
2. Cihaz detaylarında, sertifika dağıtmak istediğiniz **KeyStore**'u bulun
3. İlgili satırdaki **Deploy** butonuna tıklayın
4. Açılan **Deploy Certificate** penceresinde:

- **Virtual Servers**: Hedef KeyStore bilgisi görüntülenir (IP, Subject, Alias Name)
- **Certificate**: Açılır menüden dağıtmak istediğiniz sertifikayı seçin

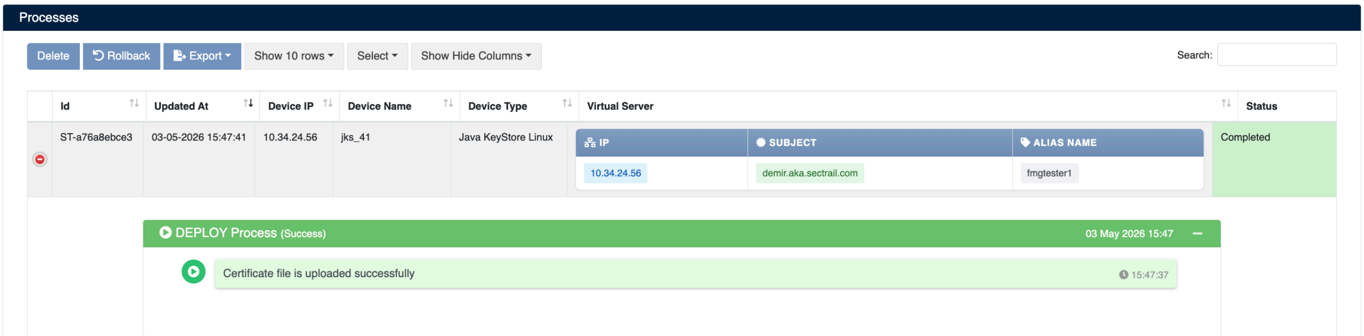


Adım 2: Dağıtım İşlemini Başlatma

Deploy butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



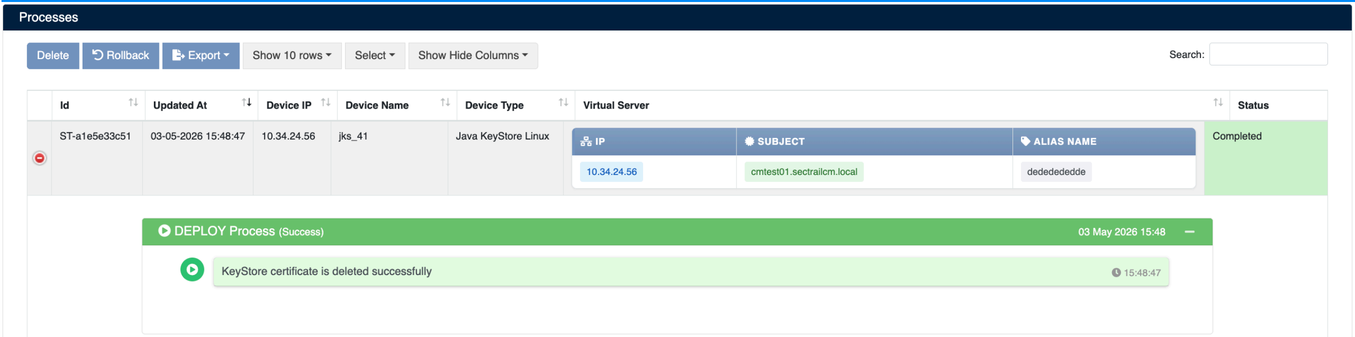
İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika dosyası sunucuya yüklenir
2	Yeni sertifika mevcut keystore dosyasına eklenir

Sertifika Silme (Remove)

SecTrail CM, Java KeyStore'dan sertifika silme işlemini destekler.



Silme İşlemi Adımları

1. **Automation > Devices** bölümünden Java KeyStore cihazınızı seçin
2. Silmek istediğiniz sertifikanın satırında ilgili işlemi seçin
3. Onay vererek silme işlemini başlatın

Silme İşlemi Task Detayları

Silme işlemi **Automation > Processes** bölümünden takip edilebilir. İşlem sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Mevcut keystore dosyası yedeklenir
2	Belirtilen alias ile sertifika keystore'dan silinir

Windows TrustStore

SecTrail CM, Windows TrustStore'a **ajansız** bağlantı kurarak güvenilir sertifikaların (Trusted Root ve Intermediate CA) otomatik yönetimini sağlar.

> **PLATFORM DESTEĞİ**
>
> SecTrail CM, Windows sistemlerinde çalışan TrustStore'ları destekler. WinRM protokolü üzerinden otomatik sertifika dağıtımı ve yönetimi yapabilirsiniz.

Kullanım Alanları

- **Trusted Root CA Management**: Root CA sertifikalarının merkezi yönetimi
- **Intermediate CA Certificates**: Ara CA sertifikalarının dağıtımı
- **Corporate PKI**: Kurumsal PKI altyapısı yönetimi
- **Certificate Chain Management**: Sertifika zinciri güven ilişkilerinin kurulması

Bağlantı Gereksinimleri

Gereksinim	Detay	Açıklama
Protokol	WinRM (Windows Remote Management)	Windows uzak yönetim protokolü
Port	`5986` veya `5985`	Güvenli WinRM portu (önerilen)
Kimlik Doğrulama	Username ve Password	Windows kullanıcı kimlik doğrulama
Transport	NTLM veya Kerberos	Windows kimlik doğrulama protokolü
Kullanıcı Yetkisi	Certificate Store yönetim yetkisi	TrustStore'a sertifika ekleme/silme yetkisi

Otomatik İşlemler

SecTrail CM, Windows TrustStore üzerinde aşağıdaki işlemleri otomatik gerçekleştirir:

1. **Certificate Discovery**: Mevcut TrustStore sertifikalarını listeleme
2. **Certificate Import**: Güvenilir sertifikaları TrustStore'a ekleme
3. **Certificate Remove**: Mevcut sertifikaları TrustStore'dan silme
4. **Validation**: Sertifika geçerliliği ve zincir testi

Desteklenen Certificate Store'lar

Store Location	Açıklama
LocalMachine	Makine bazlı sertifika deposu
My	Kişisel sertifikalar
Root	Güvenilen root CA sertifikaları
CA	Intermediate CA sertifikaları

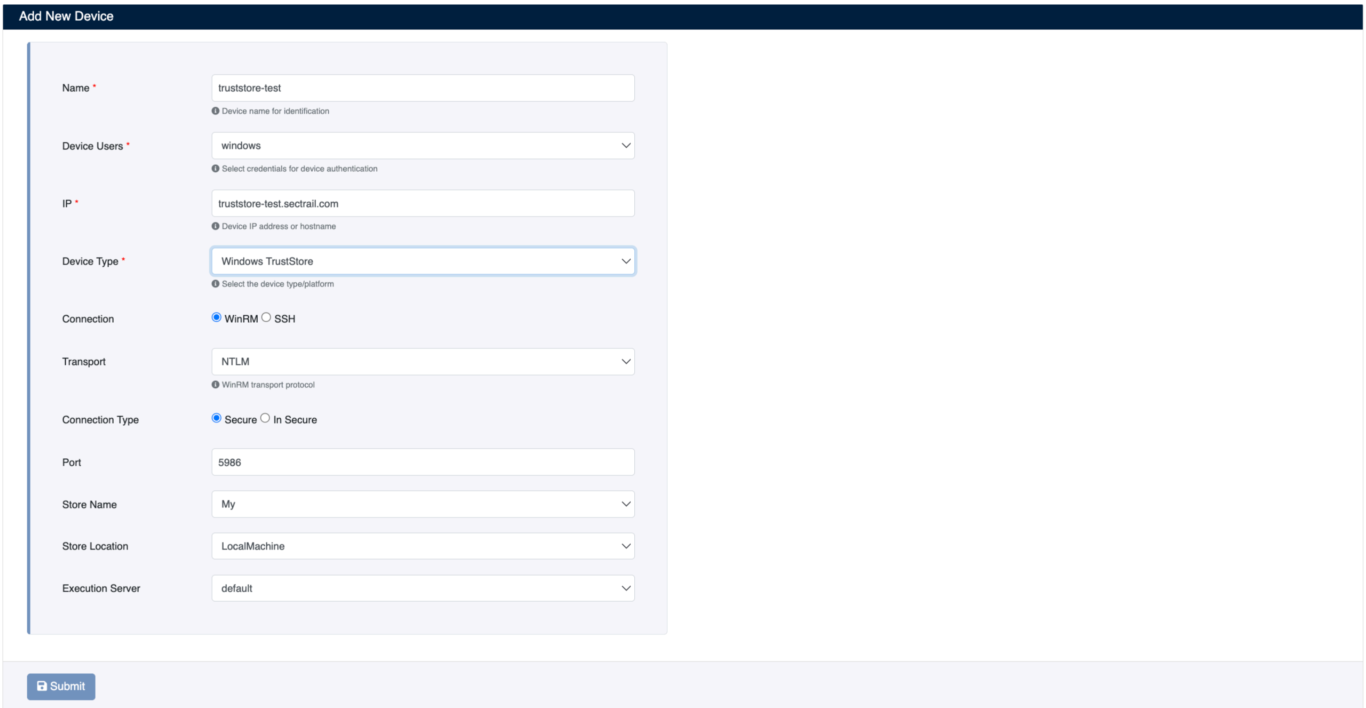
Yapılandırma Adımları

1. Windows TrustStore Kullanıcı Oluşturma

Automation > Device Users bölümüne gidin ve Windows TrustStore için kullanıcı oluşturun.

2. Windows TrustStore Cihazını SecTrail CM'e Ekleme

Automation > Devices > Add New Device butonuna tıklayın ve aşağıdaki bilgileri girin:



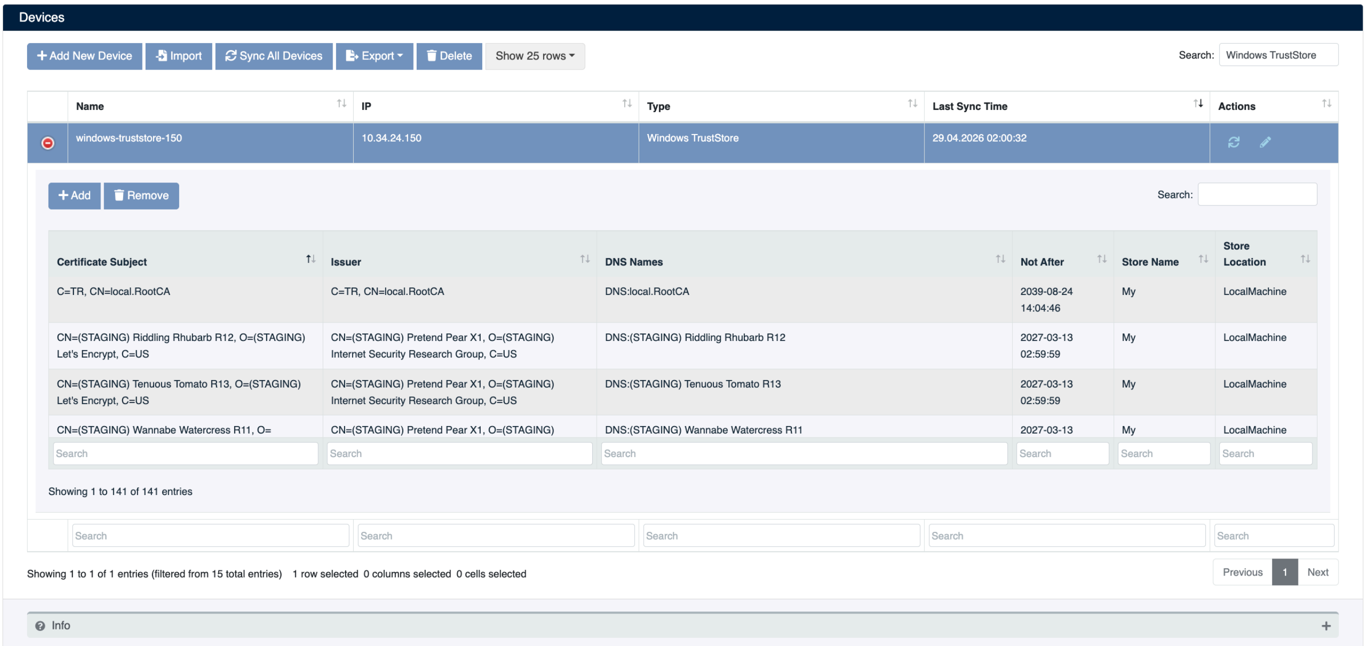
- **Name**: Cihaz için tanımlayıcı isim verin (örn: `wintrust`)
- **Device Users**: Adım 1'de oluşturduğunuz kullanıcıyı seçin (örn: `windows`)
- **IP**: Windows TrustStore sunucusunun IP adresini girin (örn: `10.34.24.150`)
- **Device Type**: Açılır menüden `Windows TrustStore` seçin
- **Connection**: `WinRM` veya `SSH` seçin (Windows için WinRM önerilir)
- **Transport**: `NTLM` seçin (veya Kerberos)
- **Connection Type**: `Secure` seçin (HTTPS için)
- **Port**: WinRM portu girin (örn: `5986`)

- **Store Name**: Store adını seçin (örn: `My`)
- **Store Location**: Store konumunu seçin (örn: `LocalMachine`)
- **Execution Server**: Dağıtım işlemlerini yürütmek için kullanılacak sunucu

> **OTOMATİK KEŞİF VE İZLEME**
>
> Windows TrustStore cihazı SecTrail CM'e eklendikten sonra, TrustStore içindeki sertifikalar otomatik olarak keşif periyoduna dahil edilir ve düzenli olarak taranır. Süresi dolmak üzere olan veya sorunlu sertifikalar için otomatik alarm oluşturulur.

3. Cihaz Bilgilerini Görüntüleme

Cihaz eklendikten sonra **Automation > Devices** listesinde görüntülenecektir. Cihaz detaylarını görmek için satıra tıklayın:



Cihaz detaylarında aşağıdaki bilgiler görüntülenir:

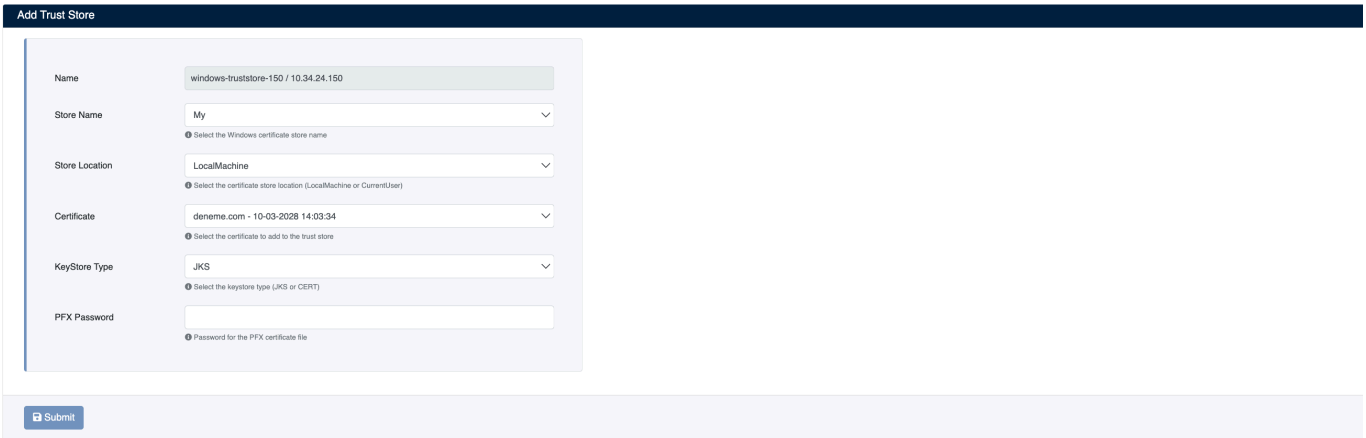
- **Certificate Subject**: Sertifika özne bilgileri (CN, ST, L, O, OU)
- **Issuer**: Sertifikayı veren CA bilgileri
- **DNS Names**: Sertifikada tanımlı DNS isimleri
- **Not After**: Sertifika geçerlilik son tarihi
- **Store Name**: Certificate Store adı
- **Store Location**: Certificate Store konumu

Sertifika Dağıtımı

Adım 1: TrustStore ve Sertifika Seçimi

1. **Automation > Devices** bölümünden Windows TrustStore cihazınızı seçin
2. Cihaz detaylarında **Add** butonuna tıklayın
3. Açılan **Add Trust Store** penceresinde:

- **Name**: Sertifika için tanımlayıcı isim verin (örn: `wintrusttest / 10.34.24.150`)
- **Store Name**: Store adını seçin (örn: `My`)
- **Store Location**: Store konumunu seçin (örn: `LocalMachine`)
- **Certificate**: Açılır menüden eklemek istediğiniz sertifikayı seçin (örn: `dvtester.sectrail.com - 09-11-2025 23:59:59`)
- **KeyStore Type**: `JKS` seçin (veya PKCS12)
- **Pfx Password**: Sertifika şifresini girin

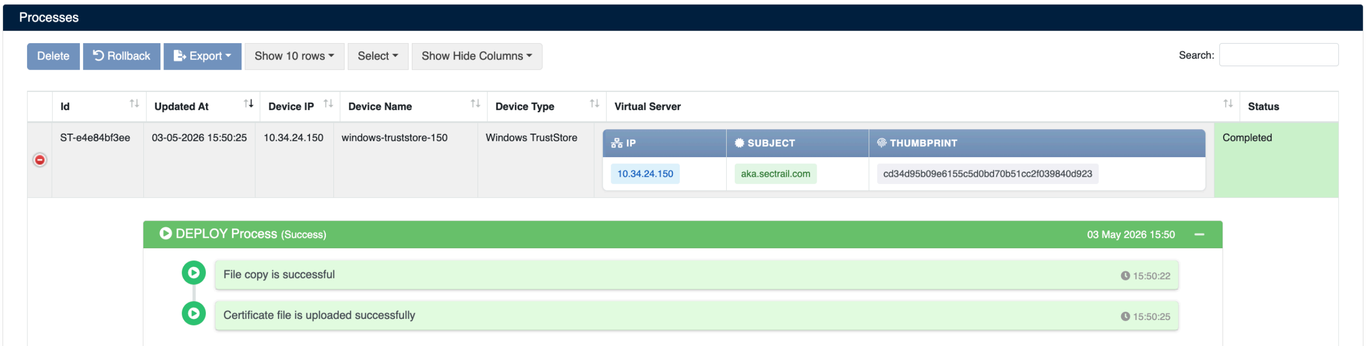


Adım 2: Dağıtım İşlemini Başlatma

Submit butonuna tıklayarak sertifika dağıtım işlemini başlatın.

Adım 3: İşlem Takibi

Dağıtım işlemi **Automation > Processes** bölümünden takip edilebilir:



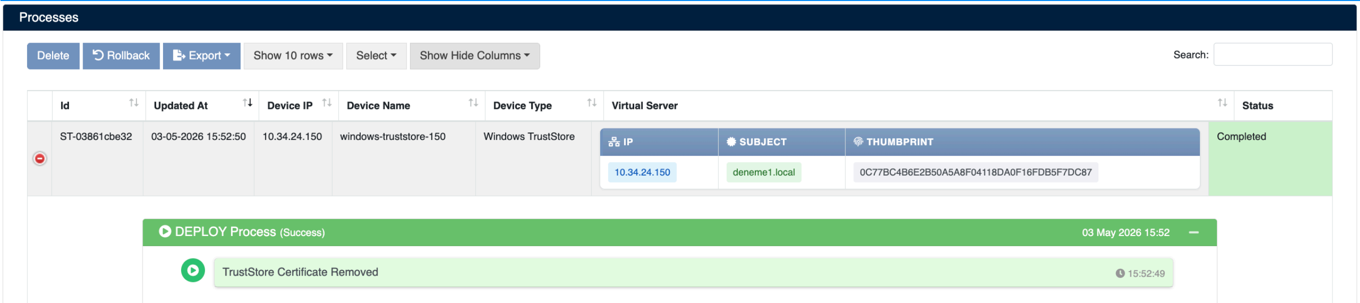
İşlem Detayları

Dağıtım sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Sertifika dosyası sunucuya kopyalanır (`File copy is successful`)
2	Sertifika Windows TrustStore'a başarıyla yüklenir (`Certificate file is uploaded successfully`)

Sertifika Silme (Remove)

SecTrail CM, Windows TrustStore'dan sertifika silme işlemini destekler.



Silme İşlemi Adımları

1. **Automation > Devices** bölümünden Windows TrustStore cihazınızı seçin
2. Silmek istediğiniz sertifikanın satırında **Remove** butonuna tıklayın
3. Onay vererek silme işlemini başlatın

Silme İşlemi Task Detayları

Silme işlemi **Automation > Processes** bölümünden takip edilebilir. İşlem sırasında aşağıdaki adımlar gerçekleştirilir:

Adım	İşlem Açıklaması
1	Belirtilen sertifika Windows TrustStore'dan silinir (`TrustStore Certificate Removed`)

Dashboard

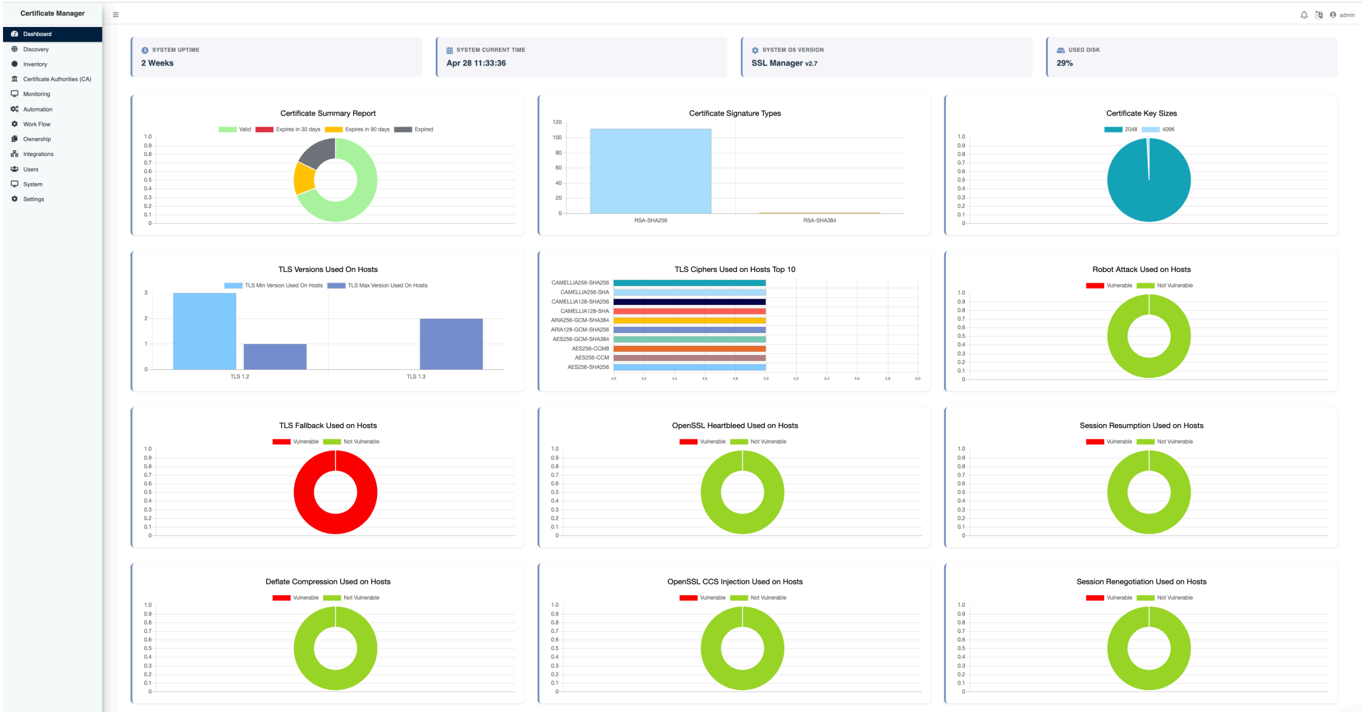
Dashboard, SecTrail CM'de sistem durumunuzun ve sertifika envanterinizin kapsamlı görünümünü sunan ana ekrandır.

Genel Bakış

Giriş yaptıktan sonra karşılaşacağınız dashboard, altyapınızdaki tüm sertifikaların durumunu, güvenlik metriklerini ve sistem bilgilerini tek bir ekranda toplar. Dashboard'da:

- **Gerçek zamanlı sertifika metrikleri** ve durum raporları
- **Güvenlik açığı analizi** ve TLS/SSL yapılandırma durumu
- [!] **Alarm sistemi** ile süresi yaklaşan sertifika uyarıları
- **Görselleştirilmiş raporlar** ile kolay takip imkanı

bulunur.



SecTrail CM Ana Dashboard - Sistem Genel Bakış

Sistem Metrikleri

Dashboard'un üst kısmında sistemin genel durumunu gösteren metrikler bulunur:

Metrik	Açıklama
System Uptime	Sistemin kesintisiz çalışma süresi
System Current Time	Sistemin şu anki zamanı
System OS Version	İşletim sistemi versiyonu (SSL Manager v2.6.9)
Used Disk	Kullanılan disk alanı yüzdesi

> **SİSTEM SAĞLIĞI**
>
> Bu metrikler sayesinde sistem performansını ve kaynak kullanımını anlık olarak izleyebilirsiniz.

Dashboard Grafikleri ve Raporlar

Dashboard, altyapınızdaki sertifikaların durumunu görselleştiren çeşitli grafikler sunar:

Sertifika Durum Grafikleri

Certificate Summary Report

Sertifikaların genel durumunu kategorilere göre gösterir:

- [OK] **Geçerli** - Geçerli sertifikalar
- **60 gün içinde sona erecek** - 60 gün içinde sona erecek
- **30 gün içinde sona erecek** - 30 gün içinde sona erecek
- **Süresi dolmuş** - Süresi dolmuş sertifikalar

Certificate Signature Types

Kullanılan sertifika imza türlerinin dağılımını gösterir. Modern ve güvenli algoritmalar (RSA-SHA256, ECDSA-SHA256) tercih edilmelidir. Eski algoritmalar (RSA-SHA1, MD5) güvenlik riski oluşturur.

Certificate Key Sizes

Sertifika anahtar boyutlarının dağılımını gösterir. Minimum 2048-bit RSA veya 256-bit ECC anahtarları önerilir. 1024-bit ve daha küçük anahtarlar güvenli değildir.

Güvenlik ve Protokol Grafikleri

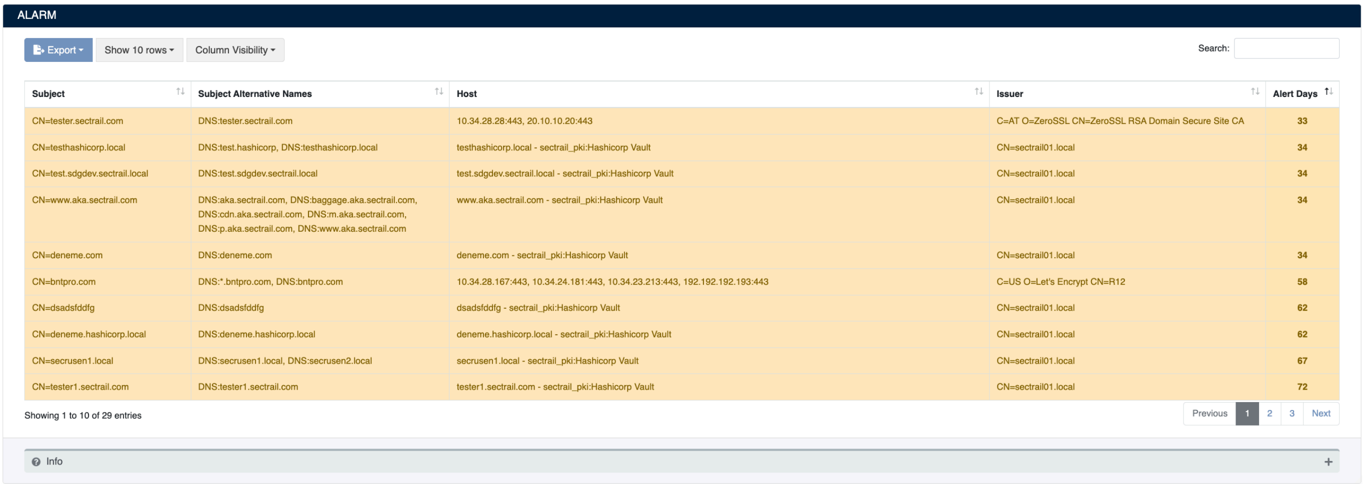
Grafik	Açıklama
TLS Versions Used On Hosts	Host'larda kullanılan TLS versiyonlarının dağılımı (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)
TLS Ciphers Used on Hosts Top 10	En çok kullanılan TLS cipher suite'leri
TLS Fallback Used on Hosts	TLS Fallback SCSV kullanım durumu (Vulnerable/Not Vulnerable)
OpenSSL Heartbleed	Heartbleed (CVE-2014-0160) güvenlik açığı tespiti
OpenSSL CCS Injection	CCS Injection (CVE-2014-0224) güvenlik açığı tespiti

[!] Güvenlik Açıkları Grafikleri

Grafik	Açıklama
Robot Attack Used on Hosts	ROBOT saldırısına karşı güvenlik durumu tespiti
Deflate Compression Used on Hosts	TLS compression (CRIME saldırısı) güvenlik açığı durumu
Session Resumption Used on Hosts	TLS session resumption mekanizması kullanım durumu
Session Renegotiation Used on Hosts	TLS session renegotiation güvenlik yapılandırması

Alarm Tablosu

Dashboard'un alt kısmında, altyapınızdaki sertifikaların alarm durumlarını gösteren detaylı bir tablo bulunur:



Subject	Subject Alternative Names	Host	Issuer	Alert Days
CN=tester.sectrail.com	DNS:tester.sectrail.com	10.34.28.28:443, 20.10.10.20:443	C=AT O=ZeroSSL CN=ZeroSSL RSA Domain Secure Site CA	33
CN=testhashicorp.local	DNS:test.hashicorp, DNS:testhashicorp.local	testhashicorp.local - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	34
CN=test.sdgdev.sectrail.local	DNS:test.sdgdev.sectrail.local	test.sdgdev.sectrail.local - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	34
CN=www.aka.sectrail.com	DNS:aka.sectrail.com, DNS:baggage.aka.sectrail.com, DNS:cdn.aka.sectrail.com, DNS:m.aka.sectrail.com, DNS:p.aka.sectrail.com, DNS:www.aka.sectrail.com	www.aka.sectrail.com - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	34
CN=deneme.com	DNS:deneme.com	deneme.com - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	34
CN=bntpro.com	DNS:*.bntpro.com, DNS:bntpro.com	10.34.28.167:443, 10.34.24.181:443, 10.34.23.213:443, 192.192.192.193:443	C=US O=Let's Encrypt CN=R12	58
CN=dsadsfddfg	DNS:dsadsfddfg	dsadsfddfg - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	62
CN=deneme.hashicorp.local	DNS:deneme.hashicorp.local	deneme.hashicorp.local - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	62
CN=secrusen1.local	DNS:secrusen1.local, DNS:secrusen2.local	secrusen1.local - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	67
CN=tester1.sectrail.com	DNS:tester1.sectrail.com	tester1.sectrail.com - sectrail_pki:Hashicorp Vault	CN=sectrail01.local	72

Dashboard Alarm Tablosu - Sertifika Uyarıları ve Durum Bilgileri

- **Subject** - Sertifikanın konusu *(CN, O, OU bilgileri)*
- **Subject Alternative Names -** Alternatif domain isimleri (SAN). Sertifikanın geçerli olduğu tüm domainleri gösterir.
- **Host -** Sertifikanın kullanıldığı sunucu/host adresi *(IP adresi veya hostname)*
- **Issuer** - Sertifikayı veren CA (Certificate Authority) bilgisi *(Örn: Let's Encrypt, DigiCert, Sectigo)*
- **Progress** - Sertifikanın yaşam döngüsündeki ilerleme durumu. Görsel progress bar ile gösterilir.
- **Alert Days** - Sertifikanın sona ermesine kalan gün sayısı ⏰ Kritik uyarı zamanı

Alarm Renk Kodları

Alarm tablosu, sertifikaların durumunu görsel olarak renklerle gösterir:

Renk	Durum	Aksiyon
Kırmızı	Süresi dolmuş veya çok yakında dolacak sertifikalar	**KRİTİK** - Acil müdahale gerekli
Turuncu/Sarı	30-60 gün içinde süresi dolacak sertifikalar	**UYARI** - Yenileme planı yapın
Yeşil	Geçerli ve süresi uzun olan sertifikalar	**NORMAL** - İyi durumda

ALARM BİLDİRİMLERİ

Dashboard'daki alarm tablosunu **düzenli olarak kontrol edin**. Kırmızı veya turuncu renkteki sertifikalar için acil aksiyonlar planlayın ve yenileme süreçlerini başlatın.

Grafikleri Anlamak ve Yorumlama

Dashboard'daki grafikler, sertifika güvenliğiniz ve altyapınızın durumu hakkında değerli bilgiler sağlar.

Sertifika Durumu İzleme

Sertifika durumlarını anlamak için öncelik seviyelerine dikkat edin:

- [OK] **Geçerli** - Normal izleme periyodunda, endişe edilecek bir durum yok
- [!] **60 gün içinde sona erecek** - Yenileme planlaması başlatın, tedarikçi ile iletişime geçin
- **30 gün içinde sona erecek** - Yüksek öncelik, acil yenileme işlemi başlatılmalı
- **Süresi Dolmuş** - **KRİTİK DURUM** - Hizmet kesintisi riski var, acil müdahale gerekli

:::

OTOMATİK BİLDİRİMLER

SecTrail CM, kritik durumlar için otomatik bildirim sistemi sağlar. E-posta ve entegrasyon ayarlarınızı yaparak anlık uyarılar alabilirsiniz.

Keşif Yapılandırması

Bu kılavuz, SecTrail CM'de sertifikaların nasıl keşfedileceğini, yönetileceğini ve izleneceğini adım adım anlatır.

> **ÖZELLİK HAKKINDA**
>
> Sertifika Keşfi özelliğinin ne olduğunu, nasıl çalıştığını ve avantajlarını öğrenmek için önce Özellikler: Sertifika Keşfi sayfasını inceleyin.

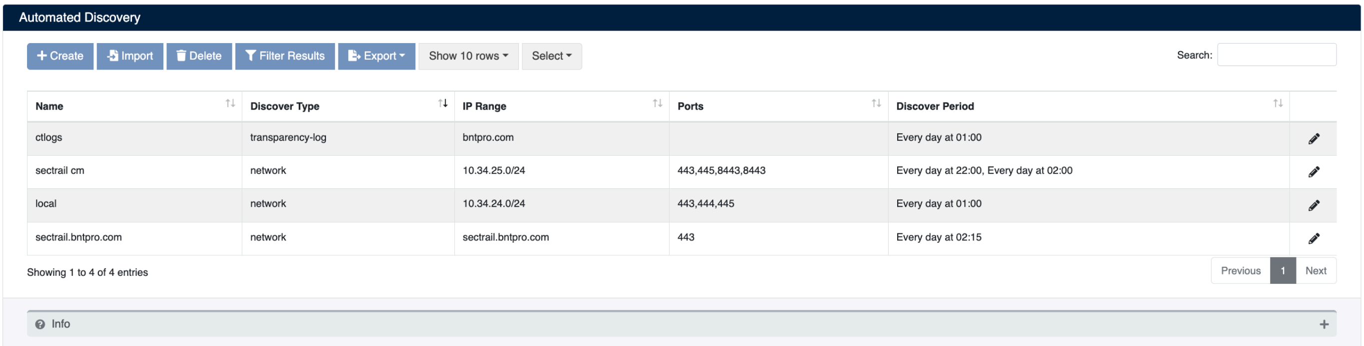
Sertifika Keşfi

Keşif Yapılandırmalarına Erişim

> **ERİŞİM YOLU**
>
> Keşif işlemlerini yönetmek için uygulama panelinde: **Discovery -> Automated Discovery** menüsüne gidin.

Keşif Yapılandırmaları Listesi

SecTrail CM'de tanımlı tüm keşif periyotlarını ve yapılandırmalarını merkezi bir listede görüntüleyebilirsiniz.



Keşif Yapılandırmaları Listesi - Tüm Tanımlı Keşif Görevleri

Liste Bilgileri

Keşif yapılandırmaları listesinde her satır için aşağıdaki bilgiler görüntülenir:

- **Name** - Keşif görevi için verdiğiniz açıklayıcı isim
- **Discover Type** - Hangi keşif yönteminin kullanıldığı (`Network Scan` veya `CT Logs`)
- **IP Range** - Taranacak IP aralığı veya domain adı
- **Ports** - Hangi portların tarandığı (örn: `443, 444, 8443`)
- **Discover Period** - Keşfin ne sıklıkla çalıştığı

Yapılabilecek İşlemler

Liste üzerinden şu işlemleri gerçekleştirebilirsiniz:

- **Görüntüleme ve Filtreleme** - Keşif yapılandırmalarını inceleyin
- **Düzenleme** - Mevcut yapılandırmaları güncelleyin
- **Silme** - Gereksiz yapılandırmaları kaldırın

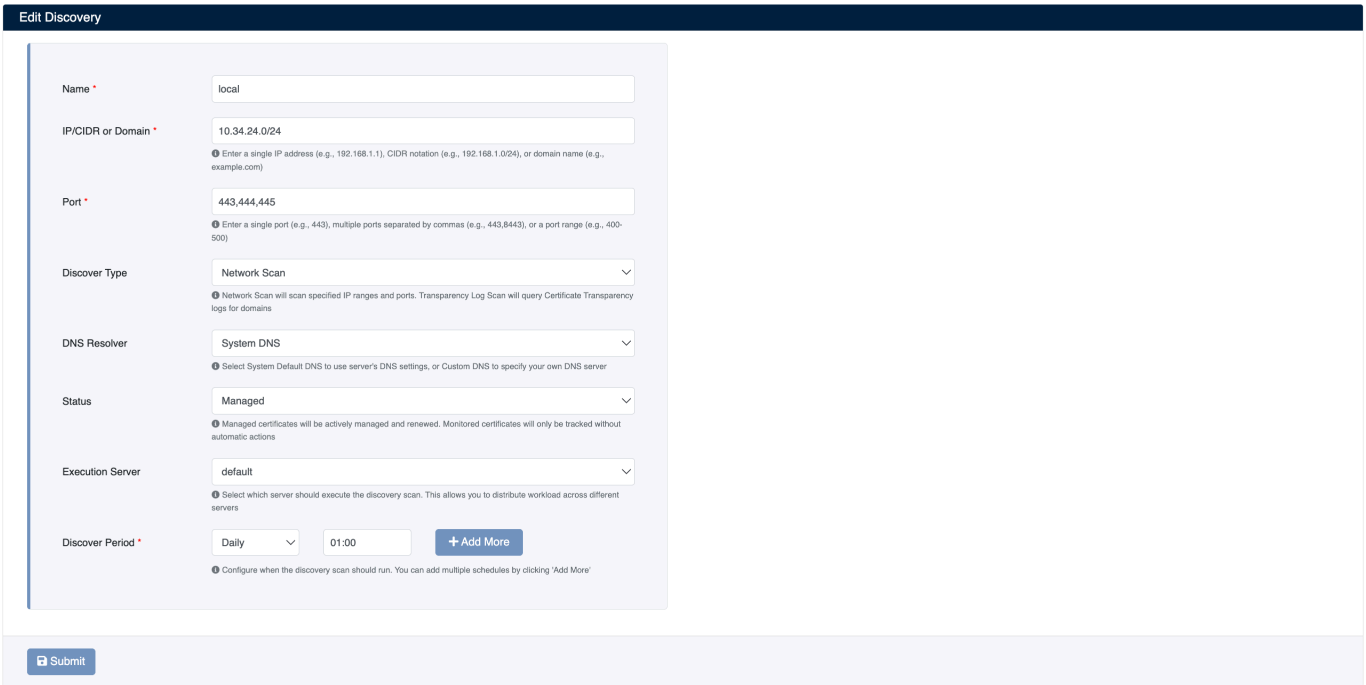
- **Yeni Oluşturma -** Yeni keşif yapılandırması ekleyin

Network Scan Yapılandırması

Network Scan ile iç ağınızdaki (internal) SSL/TLS sertifikalarını keşfedebilirsiniz.

Yeni Network Scan Oluşturma

Aşağıdaki görselde gösterildiği gibi, Network Scan yapılandırması oluşturabilirsiniz:



Network Scan Yapılandırma Formu

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
Name	Keşif görevi için açıklayıcı bir isim verin	IP aralığını veya hedef sistemin adını kullanın
IP or CIDR	Taramak istediğiniz IP adresini, CIDR notasyonunu veya domain adını girin	- Tek IP: `192.168.1.100` - IP aralığı: `10.34.24.0/24` - Alt ağ: `172.16.0.0/16` - Domain: `example.com`
Port	Taranacak portları virgülle ayırarak yazın	- Tek port: `443` - Birden fazla: `443,444,8443`
Discover Type	Keşif yöntemini seçin	`Network Scan` seçin
Status	Bulunan sertifikaların durumunu belirleyin	- **Managed:** Yönetilen sertifikalar - **Monitored:** Sadece izlenen sertifikalar
Discover Period	Taramanın ne sıklıkla çalışacağını ayarlayın	- **Periyot tipi:** Günlük veya Haftalık - **Saat:** SS:DD formatında - **Add More** ile birden fazla zaman eklenebilir

İPUÇLARI

- İş saatleri dışında tarama yapmak ağ trafiğini azaltır
- **Add More** butonu ile her gün farklı saatlerde tarama yapabilirsiniz

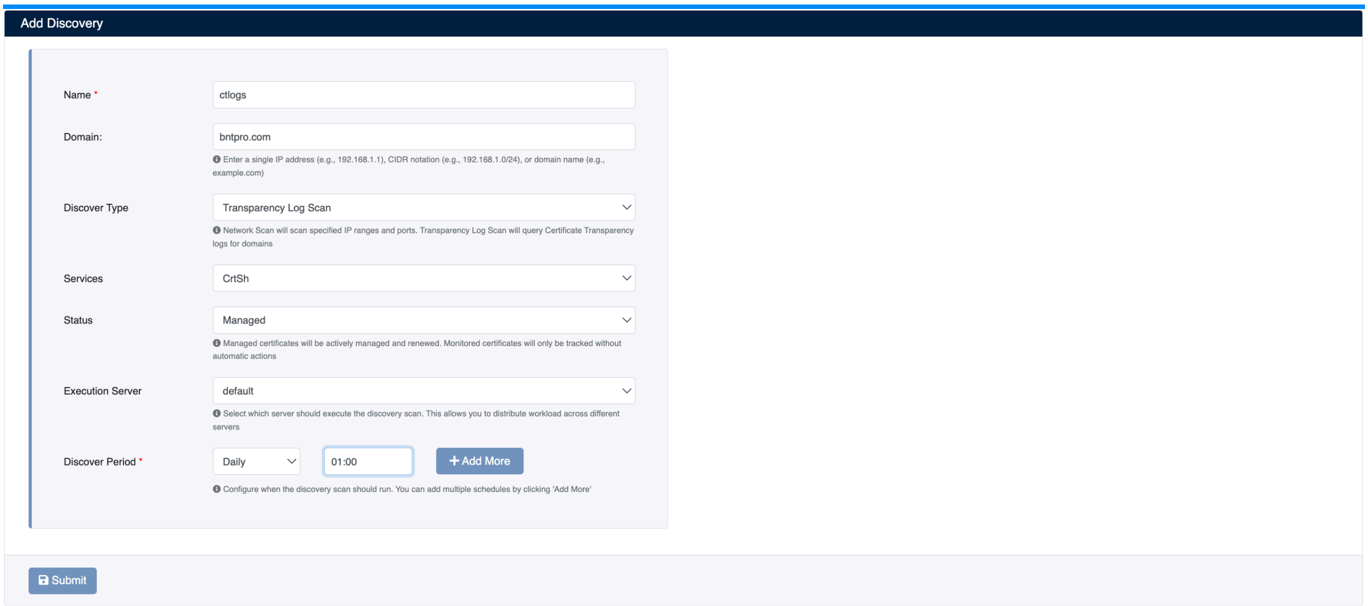
Form bilgilerini girdikten sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

CT Logs Yapılandırması

CT Logs ile public olarak yayınlanmış domain sertifikalarınızı keşfedebilirsiniz.

Yeni CT Log Taraması Oluşturma

Aşağıdaki görselde gösterildiği gibi, CT Logs yapılandırması oluşturabilirsiniz:



CT Logs Yapılandırma Formu

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
Name	Keşif görevi için açıklayıcı bir isim verin	Örnek: `Example.com CT Taraması`, `Şirket Domain'leri`
Domain	Taramak istediğiniz domain adını girin	- Örnek: `example.com` - Subdomain'ler otomatik dahil edilir - Wildcard (`*.example.com`) kullanmaya gerek yok
Discover Type	Keşif yöntemini seçin	`CT Logs` seçin
Status	Bulunan sertifikaların durumunu belirleyin	- **Managed:** Yönetilen sertifikalar - **Monitored:** Sadece izlenen sertifikalar
Discover Period	Taramanın ne sıklıkla çalışacağını ayarlayın	- **Periyot tipi:** Günlük veya Haftalık - **Saat:** SS:DD formatında

SUBDOMAİN KEŞFİ

`example.com` girdiğinizde, bu domain'e ait tüm subdomain sertifikaları da otomatik olarak bulunur: `www.example.com` , `api.example.com` , `mail.example.com` ve diğerleri.

CT LOGS İÇİN ÖNERİLER

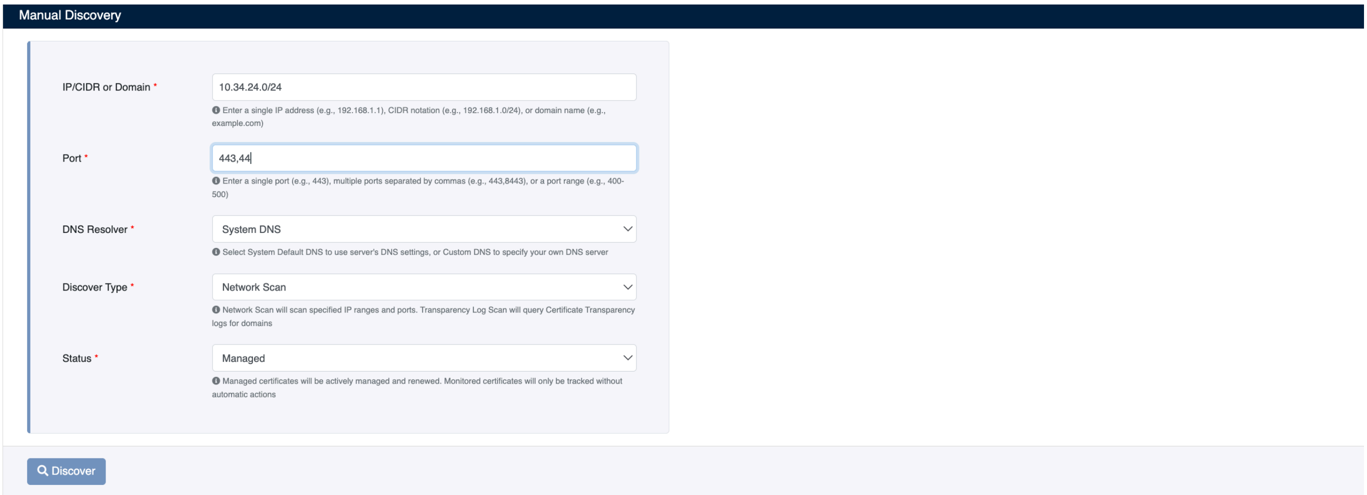
- CT Logs için **günlük tarama** önerilir (yeni sertifikaları yakalamak için)
- Shadow IT tespiti için mutlaka günlük tarama yapın
- Yeni sertifikaların CT log'lara kaydedilmesi birkaç saat sürebilir

Form bilgilerini girdikten sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

Manuel Keşif

Discovery > Manuel Keşif bölümünden zamanlanmış keşif görevleri oluşturmadan hızlı ve anlık taramalar yapabilirsiniz.

> **MANUEL KEŞİF NE ZAMAN KULLANILIR?**
>
> - Yeni bir sunucu eklediğinizde hızlı kontrol
> - Acil durum sertifika kontrolü
> - Test amaçlı taramalar
> - Tek seferlik envanter güncellemeleri



Manuel Keşif Formu - Hızlı Tarama

Manuel Keşif Parametreleri

Parametre	Açıklama	Seçenekler
IP or CIDR	Taramak istediğiniz IP, CIDR veya domain girin	- Tek IP: `1.1.1.1` - IP aralığı: `1.1.1.0/24` - Domain: `example.com`
Port	Taranacak portları belirtin	- Tek port: `443` - Birden fazla port: `443,844,444`
Discover Type	Keşif yöntemini seçin	- **Network Scan:** IP/Port taraması için - **CT Logs:** Domain taraması için
Status	Sertifika durumunu belirleyin	- **Managed:** Yönetilen - **Monitored:** İzlenen

Formu doldurduktan sonra **Discover** butonuna tıklayarak taramayı hemen başlatın.

> **ÖNEMLİ NOT**
>
> - Manuel keşif sonuçları **otomatik olarak envantere eklenir**
> - Ancak **periyodik tarama oluşturmaz**

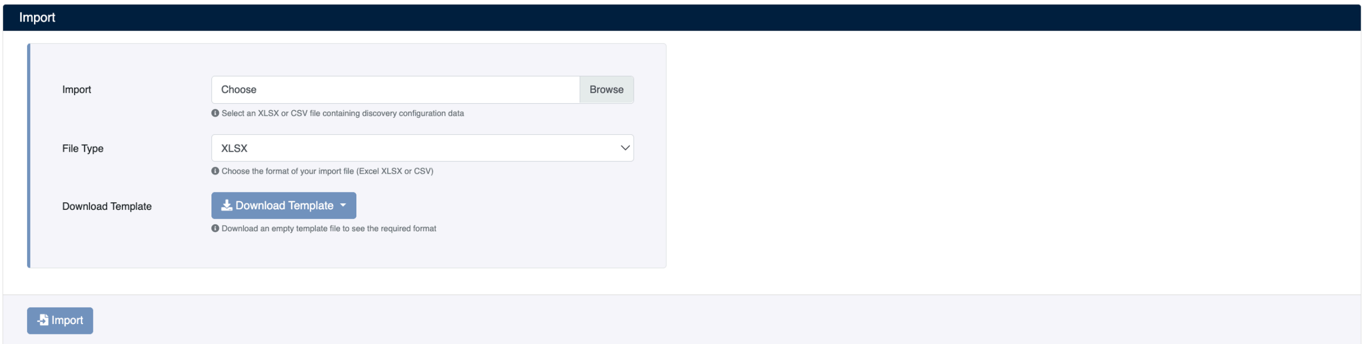
- Düzenli tarama için zamanlanmış keşif yapılandırması oluşturmalısınız

Toplu Keşif Yapılandırması

Birden fazla keşif yapılandırmasını tek seferde oluşturmak için Excel (XLSX) dosyası ile toplu içe aktarma yapabilirsiniz.

TOPLU İÇE AKTARMA NE ZAMAN KULLANILIR?

- Çok sayıda IP aralığı veya domain'i tek seferde eklemek istediğinizde
- Mevcut envanter listesinden keşif yapılandırması oluşturmak istediğinizde
- Farklı departmanların ağ listelerini toplu olarak içe aktarmak istediğinizde



File Import Ekranı - Toplu Keşif Yapılandırması

File Import Nasıl Yapılır?

Discovery -> Automated Discovery -> File Import menüsünden toplu içe aktarma sayfasına erişin.

1. Template'i İndirin ve Doldurun

Download Template butonuna tıklayarak Excel (XLSX) şablon dosyasını indirin. Template'de aşağıdaki sütunları doldurun:

TEMPLATE İPUÇLARI

- Excel'de her satır bir keşif yapılandırmasını temsil eder
- Boş satırları doldurmayın, Excel otomatik olarak atlayacaktır
- Port sütununda birden fazla port için virgülle ayırın: `443,8443,636`
- Network Scan için IP/CIDR kullanın, CT Logs için domain kullanın

2. Dosyayı Yükleyin

1. **Choose File** veya **Browse** butonuna tıklayın
2. Doldurduğunuz Excel dosyasını seçin
3. **File Type** alanından `XLSX` seçili olduğundan emin olun
4. **Import** butonuna tıklayın

3. Sonuçları Kontrol Edin

- [OK] Başarıyla içe aktarılan yapılandırmalar yeşil onay işareti ile gösterilir
- Hata olan satırlar kırmızı ile işaretlenir ve hata mesajı gösterilir
- Keşif yapılandırmaları listesinden tüm eklenen kayıtları kontrol edin

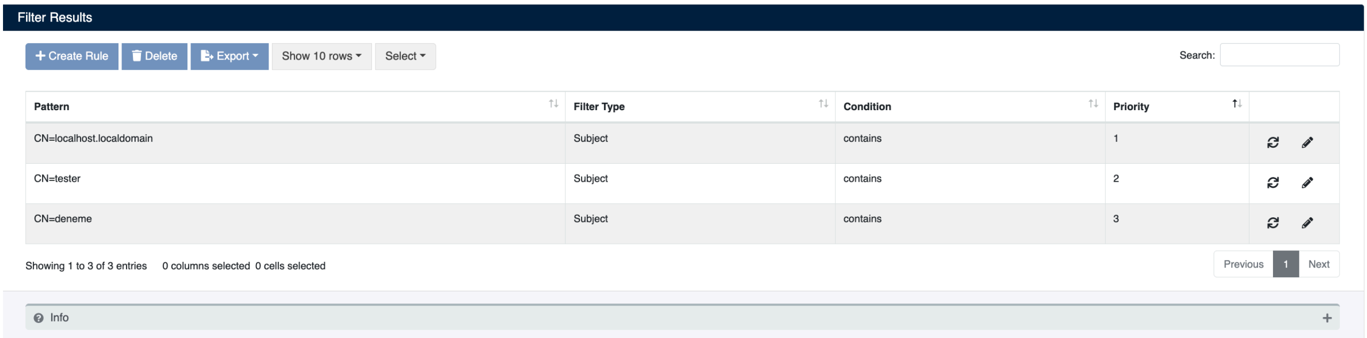
Keşif Filtresi Nasıl Yapılandırılır?

Keşif sırasında belirli IP adresleri, aralıklar veya domainlerin hiçbir şekilde keşfedilmemesini istiyorsanız **Discovery Filter** özelliğini kullanabilirsiniz. Filtreleme kuralı tanımlanan hedefler, tüm keşif işlemlerinden otomatik olarak dışlanır.

> **ERİŞİM YOLU**
>
> **Discovery -> Automated Discovery -> Filter** menüsüne gidin.

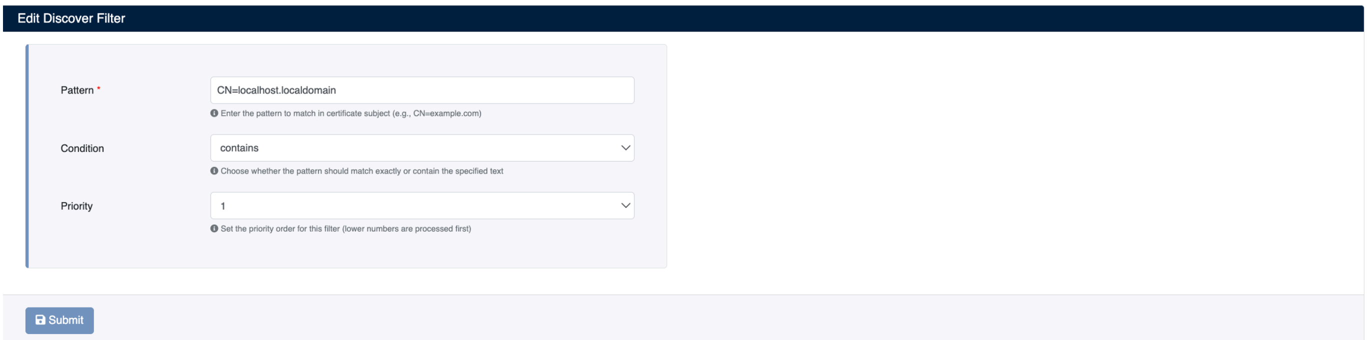
> **NE ZAMAN KULLANILIR?**
>
> - Keşfedilmesini istemediğiniz özel IP adresleri veya aralıklar varsa
> - Belirli sistemlerin envantere dahil edilmemesi gerekiyorsa
> - Tarama dışı tutulması gereken ağ segmentleri için

Filtre Listesi



Tanımlı Keşif Filtreleri Listesi

Yeni Filtre Oluşturma



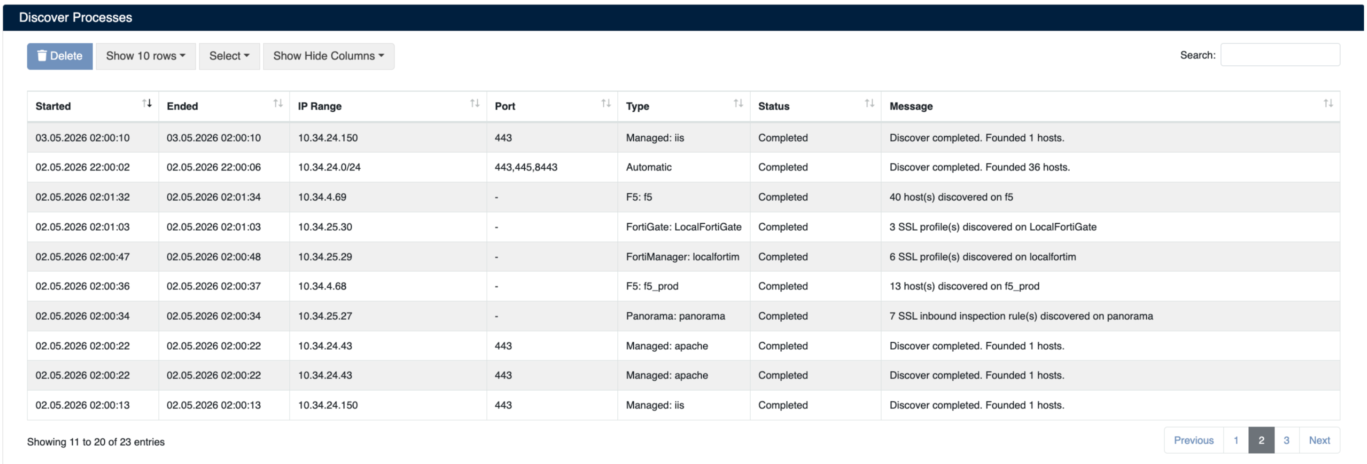
Keşif Filtresi Oluşturma Formu

Parametre	Açıklama	Örnek
IP or CIDR	Keşif dışı bırakılacak IP adresi veya aralığı	`192.168.1.50` , `10.0.0.0/8`
Port	Keşif dışı bırakılacak port (opsiyonel)	`443` , `8443`

Formu doldurup **Submit** butonuna tıkladıktan sonra kural aktif hale gelir ve bir sonraki keşif işleminde bu hedefler atlanır.

Keşif Sonuçlarını İzleme

Tüm keşif işlemlerinin sonuçlarını **Discovery -> Processes** menüsünden takip edebilirsiniz.



Keşif Sonuçları Sayfası - Tarama Durumları ve İstatistikler

Görüntülenen Bilgiler

Bu sayfada her keşif işlemi için aşağıdaki detayları görebilirsiniz:

Tarama Durumu : Devam eden, tamamlanan veya başarısız taramalar

Keşif Türü : Network Scan veya CT Logs

Hedef Bilgisi : Taranan IP aralığı veya domain adı

Başlangıç Zamanı : Taramanın başladığı tarih ve saat

Bitiş Zamanı : Taramanın tamamlandığı tarih ve saat

Süre : Taramanın toplam süresi

Bulunan Sertifika Sayısı : Taramada kaç sertifika bulunduğu

Tarama Detayları : Her taramanın detaylı log kayıtları

Tarama Durumları

Keşif işlemleri aşağıdaki durumlarda olabilir:

Durum	İkon	Açıklama	Yapılması Gereken
In Progress		Tarama şu anda devam ediyor	Tamamlanmasını bekleyin
Completed	[OK]	Tarama başarıyla tamamlandı	Sonuçları inceleyin
Failed	[X]	Tarama hata ile sonuçlandı	Hata loglarını kontrol edin

FAYDALI BİLGİ

Bu sayfadan hem zamanlanmış keşif görevlerinin hem de manuel keşif işlemlerinin sonuçlarını görüntüleyebilirsiniz. Geçmiş tarama kayıtları da saklanır, böylece keşif performansınızı analiz edebilirsiniz.

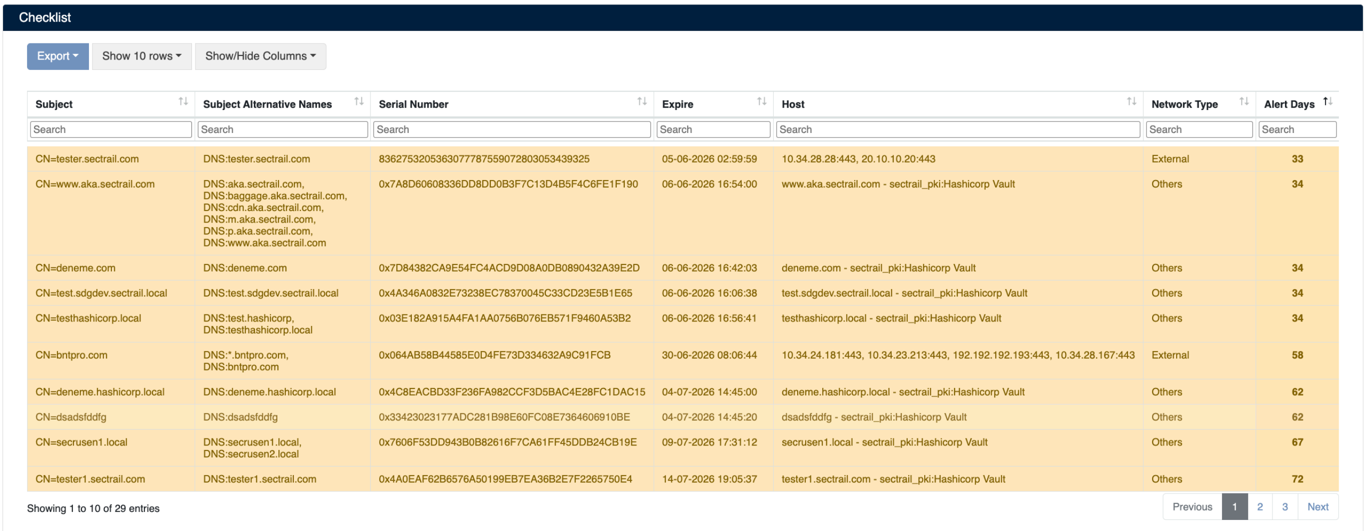
Alarmlar ve Bildirimler

SecTrail CM'de sertifikaların sona erme durumlarını takip edebilir, kritik süreler yaklaştığında otomatik bildirimler alabilir ve alarm yapılandırmaları oluşturabilirsiniz.

> **ERİŞİM YOLU**
>
> Alarm ve bildirim özelliklerine uygulama panelinde şu yollardan erişebilirsiniz:
>
> - **Monitoring -> Checklist** - Sertifika alarm listesi ve yapılandırması

Alarm Listesi

Alarm listesi, sona erme tarihi yaklaşan sertifikaların durumunu renk kodları ile görselleştirerek takip etmenizi sağlar.



Checklist

Export | Show 10 rows | Show/Hide Columns

Subject	Subject Alternative Names	Serial Number	Expire	Host	Network Type	Alert Days
Search	Search	Search	Search	Search	Search	Search
CN=tester.sectrail.com	DNS:tester.sectrail.com	8362753205363077787559072803053439325	05-06-2026 02:59:59	10.34.28.28:443, 20.10.10.20:443	External	33
CN=www.aka.sectrail.com	DNS:aka.sectrail.com, DNS:baggage.aka.sectrail.com, DNS:cdn.aka.sectrail.com, DNS:m.aka.sectrail.com, DNS:p.aka.sectrail.com, DNS:www.aka.sectrail.com	0x7A8D60608336DD8DD0B3F7C13D4B5F4C6FE1F190	06-06-2026 16:54:00	www.aka.sectrail.com - sectrail_pki:Hashicorp Vault	Others	34
CN=deneme.com	DNS:deneme.com	0x7D84382CA9E54FC4ACD9D08A0DB0890432A39E2D	06-06-2026 16:42:03	deneme.com - sectrail_pki:Hashicorp Vault	Others	34
CN=test.sdgdev.sectrail.local	DNS:test.sdgdev.sectrail.local	0x4A346A0832E73238EC78370045C33CD23E5B1E65	06-06-2026 16:06:38	test.sdgdev.sectrail.local - sectrail_pki:Hashicorp Vault	Others	34
CN=testhashicorp.local	DNS:test.hashicorp, DNS:testhashicorp.local	0x03E182A915A4FA1AA0756B076EB571F9460A53B2	06-06-2026 16:56:41	testhashicorp.local - sectrail_pki:Hashicorp Vault	Others	34
CN=bntpro.com	DNS:*.bntpro.com, DNS:bntpro.com	0x064AB58B44585E0D4FE73D334632A9C91FCB	30-06-2026 08:06:44	10.34.24.181:443, 10.34.23.213:443, 192.192.192.193:443, 10.34.28.167:443	External	58
CN=deneme.hashicorp.local	DNS:deneme.hashicorp.local	0x4C8EACBD33F236FA982CCF3D5BAC4E28FC1DAC15	04-07-2026 14:45:00	deneme.hashicorp.local - sectrail_pki:Hashicorp Vault	Others	62
CN=dsadsfddfg	DNS:dsadsfddfg	0x33423023177ADC281B98E60FC08E7364606910BE	04-07-2026 14:45:20	dsadsfddfg - sectrail_pki:Hashicorp Vault	Others	62
CN=secrusen1.local	DNS:secrusen1.local, DNS:secrusen2.local	0x7606F53DD943B0B82616F7CA61FF45DDB24CB19E	09-07-2026 17:31:12	secrusen1.local - sectrail_pki:Hashicorp Vault	Others	67
CN=tester1.sectrail.com	DNS:tester1.sectrail.com	0x4A0EAF62B6576A50199EB7EA36B2E7F2265750E4	14-07-2026 19:05:37	tester1.sectrail.com - sectrail_pki:Hashicorp Vault	Others	72

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

Sona Erme Durumu Alarm Listesi

Liste Bilgileri

Alarm listesinde her sertifika için aşağıdaki bilgiler görüntülenir:

- **Subject** - Sertifikanın Common Name (CN) bilgisi
- **Subject Alternative Names** - Sertifikanın SANs (DNS adları) listesi
- **Serial Number** - Sertifika seri numarası
- **Expire** - Sertifikanın sona erme tarihi ve zamanı
- **Host** - Sertifikanın bulunduğu sunucu adresi ve port bilgisi
- **Issuer** - Sertifikayı imzalayan CA (Certificate Authority)
- **Network Type** - Sertifikanın ağ tipi kategorisi (External, Internal, vb.)
- **Alert Days** - Sertifikanın sona ermesine kalan gün sayısı

Alarm Renk Kodları

Sertifikaların sona erme durumu **Alert Days** sütununda renk kodları ile gösterilir:

Renk	Durum	Açıklama
Kırmızı	Kritik (0-7 gün)	Sertifika son 7 gün içinde sona erecek veya süresi dolmuş
Turuncu	Uyarı (8-30 gün)	Sertifika 8-30 gün içinde sona erecek
Sarı	Dikkat (31-90 gün)	Sertifika 31-90 gün içinde sona erecek

KRİTİK ALARM

Kırmızı renk ile gösterilen sertifikalar acil müdahale gerektirir. Bu sertifikaların süresi dolmadan yenilenmesi veya güncellenmesi gerekmektedir.

Liste Üzerindeki İşlemler

Sayfanın üst kısmında bulunan araç çubuğundan şu işlemleri yapabilirsiniz:

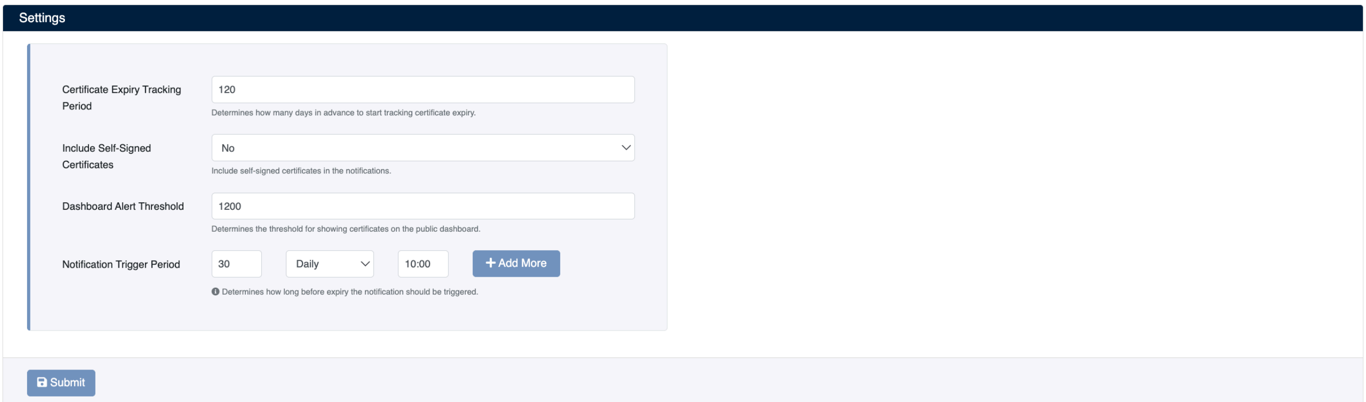
- **Show X entries** - Sayfa başına gösterilecek kayıt sayısını ayarlayın
- **Search** - Sertifika bilgilerine göre arama yapın
- **Alarm Configuration** - Alarm yapılandırma sayfasına geçiş yapın

Alarm Yapılandırması

Alarm Configuration sayfasında sertifika sona erme bildirimlerini özelleştirebilir, otomatik bildirim zamanlarını ayarlayabilirsiniz.

ERİŞİM

Monitoring -> Settings sekmesinden alarm yapılandırma ayarlarına erişebilirsiniz.



Alarm Yapılandırma Sayfası

Yapılandırma Ayarları

Parametre	Açıklama	Seçenekler
Track If Certificates Expires In	Sertifikaların sona erme süresini kaç gün öncesinden takip etmeye başlayacağınızı belirler	Gün sayısı girin
Send Notification If Certificates Expires In	Otomatik bildirim göndermek için zaman periyotlarını ayarlayın	- **Gün sayısı:** Kaç gün önce bildirim gönderilsin - **Periyot:** Her gün veya Haftalık - **Gün:** Haftalık bildirim için hangi gün - **Saat:** Bildirimin hangi saatte gönderileceği
Send Self-Signed Certificate	Self-signed sertifikalar için bildirim gönderilsin mi?	- **Yes:** Self-signed için de bildirim - **No:** Self-signed hariç
Public Dashboard Threshold	Public dashboard'da gösterilecek sertifikaların sona erme eşik değeri	Gün sayısı girin

> **SELF-SİGNED SERTİFİKALAR**
>
> Self-signed sertifikalar genellikle test ortamlarında veya iç sistemlerde kullanılır. Üretim ortamlarında güvenilir CA'lar tarafından imzalanan sertifikalar kullanılması önerilir.

Yapılandırmayı Kaydetme

Tüm ayarları yaptıktan sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

:::success Başarılı Kayıt Yapılandırma kaydedildikten sonra belirlediğiniz periyotlarda otomatik bildirimler gönderilmeye başlanacaktır. :::

Bildirim Entegrasyonları

SecTrail CM, alarm bildirimlerini farklı kanallar üzerinden gönderebilir:

- **E-posta** - Belirlenen e-posta adreslerine otomatik bildirim gönderimi
- **SNMP Trap** - SNMP protokolü üzerinden ağ yönetim sistemlerine alarm gönderimi

Ağ Tipi Alarm Yapılandırması

Ağ Tipi Alarm Yapılandırması, belirli bir ağ tipindeki (Network Type) tüm sertifikaların listesini periyodik olarak e-posta ile göndermenizi sağlar. Bu özellik sayesinde External, Internal veya diğer ağ tiplerindeki sertifikaların tam listesini düzenli olarak alabilir ve hangi domainleri kullandığınızı takip edebilirsiniz.

> **ERİŞİM YOLU**
>
> **Monitoring -> Alert Rules -> Network Type Based** sayfasından ağ tipi bazlı alarm yapılandırmalarına erişebilirsiniz.

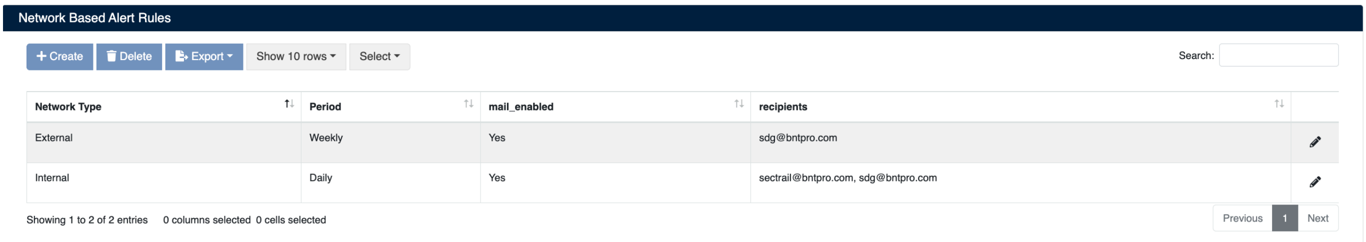
Ağ Tipi Alarm Yapılandırması Nedir?

Ağ Tipi Alarm Yapılandırması, belirli bir ağ tipine ait tüm sertifikaların listesini otomatik olarak e-posta ile gönderir. Bu sayede:

- **External** sertifikaların tam listesini günlük veya haftalık alabilirsiniz
- **Internal** sertifikaların envanterini düzenli olarak takip edebilirsiniz
- Her ağ tipi için farklı ekiplere ayrı listeler gönderebilirsiniz
- Kullanılan tüm domainleri ve sertifikaları raporlayabilirsiniz

> **NETWORK TYPE NEDİR?**
>
> Network Type, sertifikaların hangi ağ kategorisinde olduğunu belirler. Bu değerler **Monitoring -> Alert Rules -> Network Type Based** sayfasından yapılandırılır ve sertifikaları otomatik olarak kategorize eder.

Ağ Tipi Alarm Yapılandırması Listesi



Ağ Tipi Alarm Yapılandırması - Mevcut Yapılandırmalar

Liste Bilgileri

Liste sayfasında tanımlı tüm ağ tipi alarm yapılandırmalarını görebilirsiniz:

- **Network Type** - Ağ tipi kategorisi (External, Internal, vb.)
- **Period** - Bildirim periyodu (Günlük, Haftalık)
- **Mail** - E-posta bildirimi aktif mi? (Yes/No)
- **To Mails** - Bildirim gönderilecek e-posta adresleri

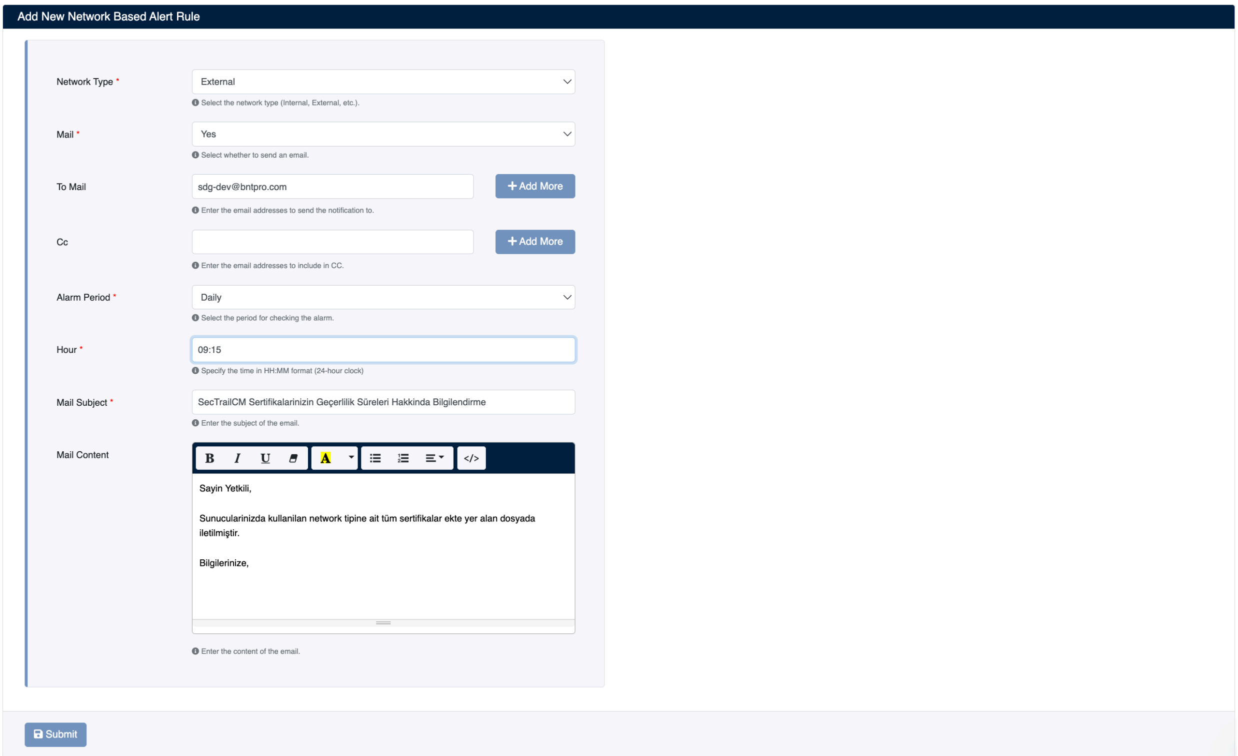
Liste Üzerindeki İşlemler

Her satır için aşağıdaki işlemleri yapabilirsiniz:

- **Edit (Düzenle)** - Mevcut yapılandırmayı düzenleyin
- **Delete (Sil)** - Yapılandırmayı silin

> **YENİ YAPILANDIRMA**
>
> **Create** butonuna tıklayarak yeni bir Ağ Tipi Alarm Yapılandırması oluşturabilirsiniz.

Yeni Ağ Tipi Alarm Yapılandırması Oluşturma



Yeni Ağ Tipi Alarm Yapılandırması Ekleme Formu

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
Network Type	Alarm yapılandırmasının hangi ağ tipi için geçerli olacağını seçin	- **External:** Dış ağ sertifikaları - **Internal:** İç ağ sertifikaları - Network Configuration'da tanımlı özel tipler
Mail	E-posta bildirimi gönderilsin mi?	- **Yes:** E-posta bildirimi aktif - **No:** E-posta bildirimi kapalı
To Mail	Bildirim gönderilecek e-posta adresleri	Birden fazla e-posta adresi eklenebilir (**Add More** ile)
Cc	Kopya alıcıları (opsiyonel)	Birden fazla e-posta adresi eklenebilir
Alarm Period	Bildirimin ne sıklıkta gönderileceği	- **Daily:** Her gün - **Weekly:** Haftalık
Hour	Bildirimin hangi saatte gönderileceği	24 saat formatında (örn: `10:00`)
Mail Subject	E-posta konu satırı	E-posta konusunu girin
Mail Content	E-posta içeriği	E-posta içeriğini girin

> **NETWORK TYPE KURALI**
>
> Her Network Type için sadece bir alarm yapılandırması oluşturabilirsiniz. Mevcut bir Network Type için yeni yapılandırma oluşturamazsınız.

> **OTOMATİK SERTİFİKA LİSTESİ**
>
> E-posta içeriğine, seçilen ağ tipindeki **tüm sertifikaların listesi** otomatik olarak ek dosya (Excel/CSV) olarak eklenir.
>
> Liste şunları içerir:
>
> - Sertifika Subject (CN) bilgileri
> - Sertifika sona erme tarihleri
> - Host ve port bilgileri
> - Kullanılan tüm domain isimleri

Yapılandırmayı Kaydetme

Tüm alanları doldurduktan sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

:::success Başarılı Kayıt Yapılandırma kaydedildikten sonra belirlenen periyotta ve saatte, ilgili ağ tipindeki **tüm sertifikaların listesi** otomatik olarak e-posta ile gönderilmeye başlanacaktır. :::

Alarm Özelleştirme

Alarm Özelleştirme, sertifika alarmlarını çok daha detaylı kriterlere göre özelleştirmenizi sağlar. Bu özellik sayesinde belirli özelliklere sahip sertifikalar için özel alarm kuralları oluşturabilir, farklı ekiplere farklı alarm bildirimleri gönderebilirsiniz.

> **ERİŞİM YOLU**
>
> **Monitoring -> Alert Rules -> Advanced Rules** sekmesinden alarm özelleştirme yapılandırmalarına erişebilirsiniz.

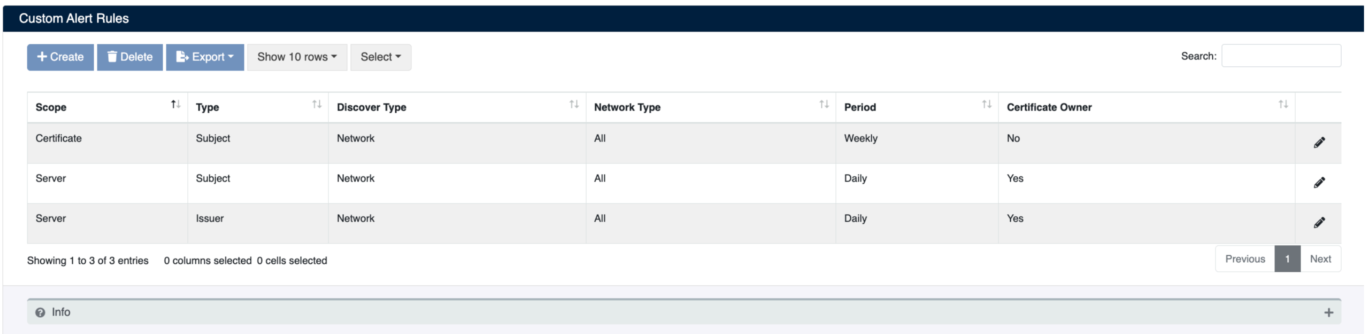
Alarm Özelleştirme Nedir?

Alarm Özelleştirme, standart alarm yapılandırmasının ötesinde, çok daha granüler ve spesifik alarm kuralları oluşturmanıza olanak tanır. Bu sayede:

- **Scope bazlı alarmlar:** Sunucu veya sertifika bazlı ayrı alarmlar
- **Type bazlı alarmlar:** Sunucu veya CA sertifikaları için ayrı kurallar
- **Network Type filtreleme:** Sadece harici, lokal veya belirli ağ tiplerindeki sertifikalar
- **Certificate Owner filtreleme:** Belirli sahiplere ait sertifikalar için özel alarmlar
- **Key Size uyarıları:** Güvensiz anahtar boyutları için otomatik bildirimler
- **Expired sertifikalar:** Süresi geçmiş sertifikalar için ayrı bildirimler
- **Self-signed kontrol:** Self-signed sertifikalar için özel kurallar

oluşturabilirsiniz.

Alarm Özelleştirme Listesi



Alarm Özelleştirme - Mevcut Kurallar

Liste Bilgileri

Liste sayfasında tanımlı tüm özelleştirilmiş alarm kurallarını görebilirsiniz:

- **Type** - Alarm tipi (Subject, Issuer)
- **Scope** - Kapsam (Server, Certificate)
- **Discover Type** - Keşif tipi (Network, TLS vb.)

- **Network Type -** Ağ tipi filtresi (All, External, Internal)
- **Threshold Day -** Kaç gün öncesinden alarm gönderilsin
- **Certificate Owner -** Sertifika sahibi filtresi (Yes/No)
- **To Mails -** Bildirim gönderilecek e-posta adresleri

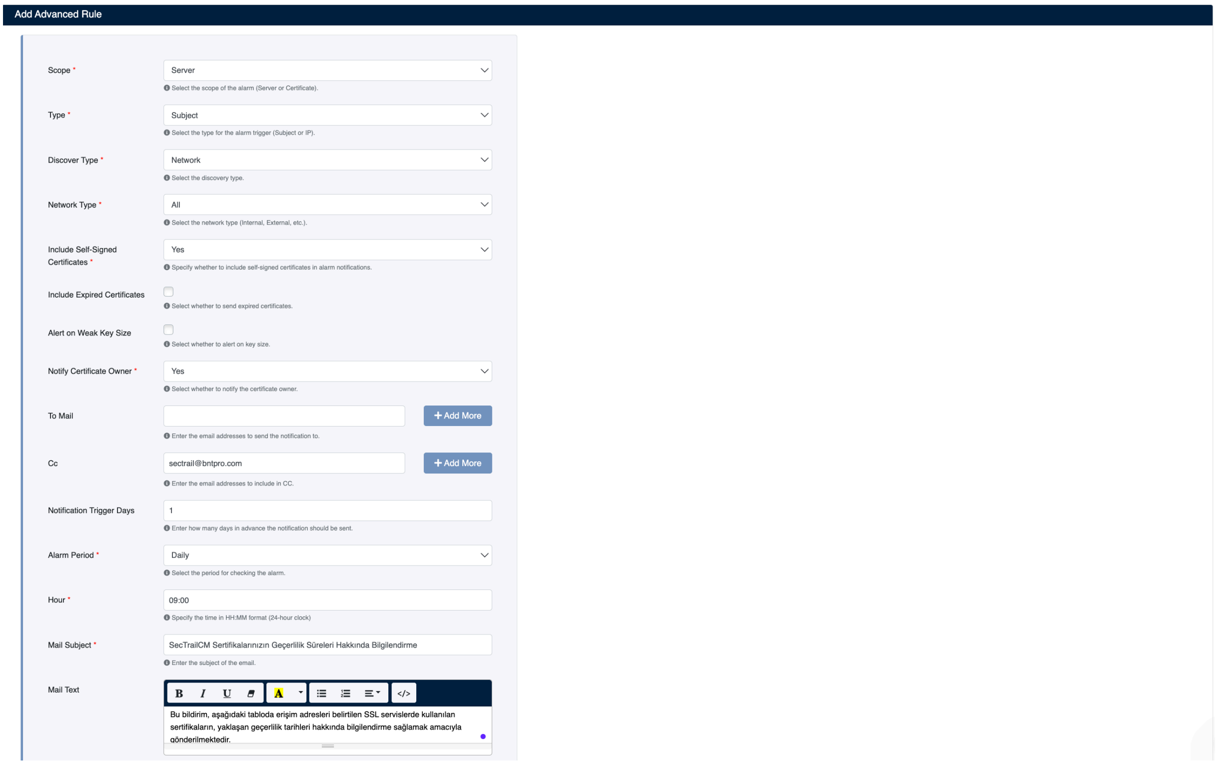
Liste Üzerindeki İşlemler

Her satır için aşağıdaki işlemleri yapabilirsiniz:

- **Edit (Düzenle) -** Mevcut kuralı düzenleyin
- **Delete (Sil) -** Kuralı silin

> **YENİ KURAL**
>
> **Create** butonuna tıklayarak yeni bir özelleştirilmiş alarm kuralı oluşturabilirsiniz.

Yeni Alarm Özelleştirme Kuralı Oluşturma



Yeni Alarm Özelleştirme Kuralı Ekleme Formu

Yapılandırma Parametreleri

Temel Filtreler

Parametre	Açıklama	Seçenekler
Scope	Alarmın hangi kapsamda çalışacağını belirler	- **Server:** Her sunucu için ayrı bildirim - **Certificate:** Benzersiz sertifikalar için bildirim
Type	Hangi tür sertifikalar için alarm oluşturulacağını seçin	- **Subject:** Server sertifikaları - **Issuer:** CA sertifikaları
Discover Type	Sertifikaların nasıl keşfedildiğine göre filtreleyin	- **Network:** Ağ taraması - **TLS:** TLS bağlantısı - **File:** Dosya sistemi
Network Type	Hangi ağ tipindeki sertifikalar için alarm oluşturulacağını seçin	- **All:** Tüm ağ tipleri - **External:** Sadece dış sertifikalar - **Internal:** Sadece iç sertifikalar - Network Configuration'da tanımlı özel tipler

Alarm Kuralları

Parametre	Açıklama	Seçenekler
Send Alarm If Certificate Expires in	Sertifikanın sona ermesine kaç gün kala alarm gönderileceğini belirler	Gün sayısı girin (örn: 30, 15, 7)
Send Expired Certificates	Süresi dolmuş sertifikalar için bildirim gönderilsin mi?	- **Evet:** Süresi geçmiş sertifikalar için de bildirim - **Hayır:** Sadece süresi dolmamış sertifikalar
Key Size Alert	Güvensiz anahtar boyutları için uyarı	- **Evet:** Küçük anahtar boyutları için uyarı (örn: 1024 bit RSA) - **Hayır:** Anahtar boyutu kontrolü yapma
Send Self-Signed Certificate	Self-signed sertifikalar dahil edilsin mi?	- **Yes:** Self-signed için de bildirim - **No:** Self-signed hariç
Certificate Owner	Belirli sahiplere ait sertifikalar için filtre	- **Yes:** Sadece belirli sahiplere ait - **No:** Tüm sertifikalar

Bildirim Ayarları

Parametre	Açıklama	Seçenekler
Alarm Period	Bildirimin ne sıklıkta gönderileceği	- **Günlük:** Her gün - **Haftalık:** Haftalık
Hour	Bildirimin hangi saatte gönderileceği	24 saat formatında (örn: `10:00`)
To Mail	Bildirim gönderilecek e-posta adresleri	Birden fazla e-posta adresi eklenebilir (**Add More** ile)
Cc	Kopya alıcıları (opsiyonel)	Birden fazla e-posta adresi eklenebilir
Mail Subject	E-posta konu satırı	E-posta konusunu girin
Mail Text	E-posta içeriği	E-posta içeriğini girin

Yapılandırmayı Kaydetme

Tüm alanları doldurduktan sonra **Submit** butonuna tıklayarak kuralı kaydedin.

:::success Başarılı Kayıt Kural kaydedildikten sonra belirlenen kriterlere uyan sertifikalar için otomatik bildirimler gönderilmeye başlanacaktır. :::

TLS Alarm Yapılandırması

TLS Alarm Yapılandırması, sunucularınızda kullanılan eski ve güvensiz TLS versiyonları (TLS 1.0, TLS 1.1) hakkında otomatik bildirimler almanızı sağlar. Bu özellik sayesinde güvenlik açığı oluşturan eski TLS versiyonlarını tespit edebilir ve güncelleyebilirsiniz.

> **ERİŞİM YOLU**
>
> **Monitoring -> Alert Rules -> TLS Version Based** sayfasından TLS alarm yapılandırmalarına erişebilirsiniz.

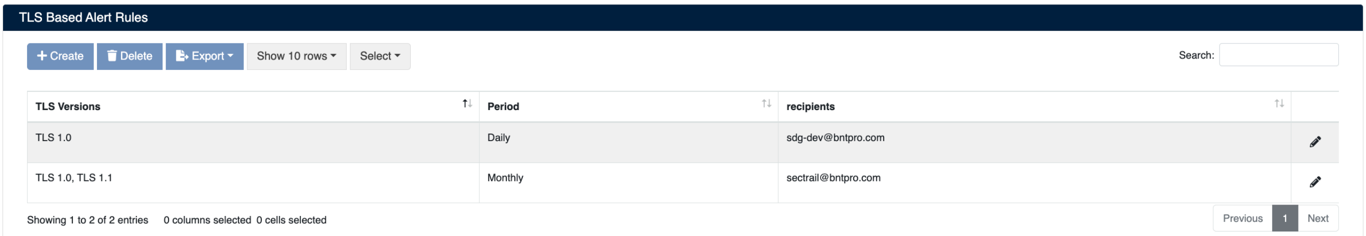
TLS Alarm Yapılandırması Nedir?

TLS Alarm Yapılandırması, sunucularınızda kullanılan TLS protokol versiyonlarını izler ve güvensiz kabul edilen eski versiyonlar için otomatik bildirimler gönderir. Bu sayede:

- **TLS 1.0** kullanan sunucuları tespit edebilirsiniz
- **TLS 1.1** kullanan sunucuları tespit edebilirsiniz
- Güvenlik standartlarına uyumsuz servisleri raporlayabilirsiniz

> **GÜVENLİK UYARISI**
>
> TLS 1.0 ve TLS 1.1 versiyonları güvensiz kabul edilir ve artık kullanılmamalıdır. Modern güvenlik standartları minimum TLS 1.2 veya TLS 1.3 gerektirir.

TLS Alarm Yapılandırması Listesi



TLS Alarm Yapılandırması - Mevcut Yapılandırmalar

Liste Bilgileri

Liste sayfasında tanımlı tüm TLS alarm yapılandırmalarını görebilirsiniz:

- **TLS Versions** - İzlenen TLS versiyonları (TLS 1.0, TLS 1.1)
- **Period** - Bildirim periyodu (Günlük, Haftalık)
- **To Mails** - Bildirim gönderilecek e-posta adresleri

Liste Üzerindeki İşlemler

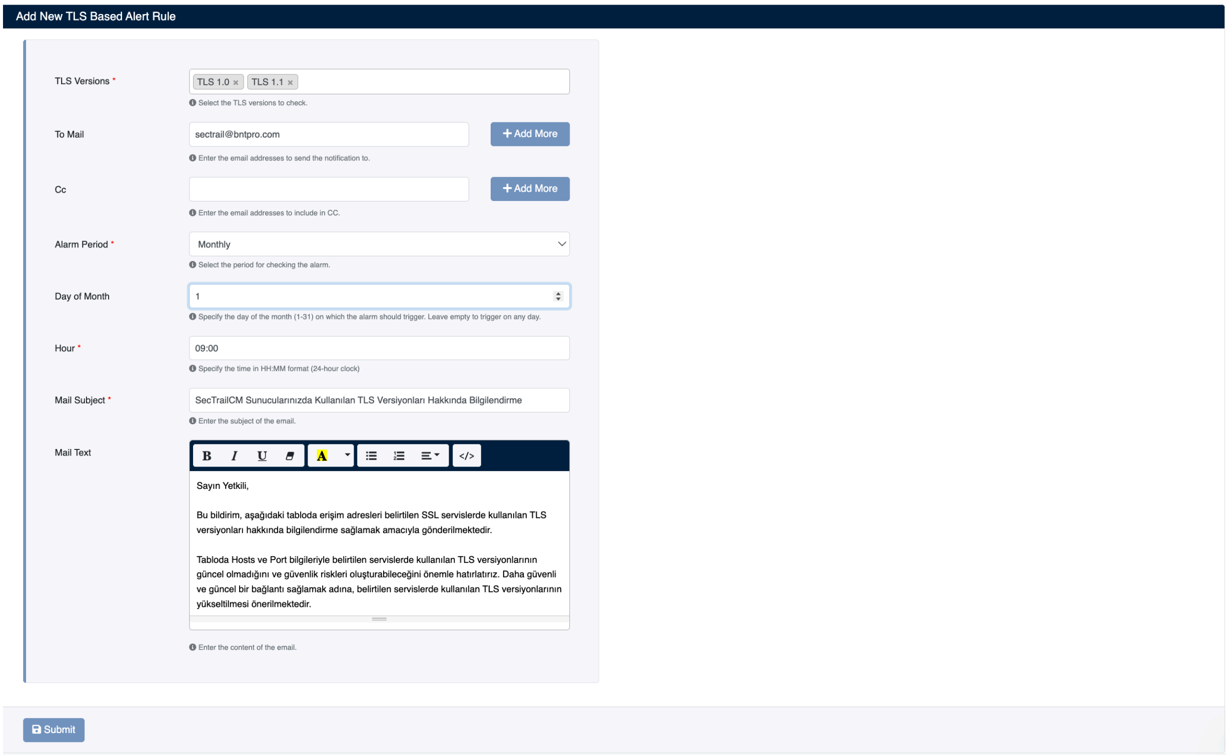
Her satır için aşağıdaki işlemleri yapabilirsiniz:

- **Edit (Düzenle)** - Mevcut yapılandırmayı düzenleyin
- **Delete (Sil)** - Yapılandırmayı silin

YENİ YAPILANDIRMA

Create butonuna tıklayarak yeni bir TLS Alarm Yapılandırması oluşturabilirsiniz.

Yeni TLS Alarm Yapılandırması Oluşturma



Yeni TLS Alarm Yapılandırması Ekleme Formu

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
TLS Versions	İzlenecek TLS versiyonlarını seçin (Birden fazla seçilebilir)	- **TLS 1.0:** Çok eski ve güvensiz (1999) - **TLS 1.1:** Eski ve güvensiz (2006)
To Mail	Bildirim gönderilecek e-posta adresleri	Birden fazla e-posta adresi eklenebilir (**Add More** ile)
Cc	Kopya alıcıları (opsiyonel)	Birden fazla e-posta adresi eklenebilir
Alarm Period	Bildirimin ne sıklıkta gönderileceği	- **Günlük:** Her gün - **Haftalık:** Haftalık
Hour	Bildirimin hangi saatte gönderileceği	24 saat formatında (örn: `11:00`)
Mail Subject	E-posta konu satırı	E-posta konusunu girin
Mail Text	E-posta içeriği	E-posta içeriğini girin

TLS VERSİYON GÜVENLİĞİ

- **TLS 1.0 -** 1999'da yayınlandı, ciddi güvenlik açıkları var

> - **TLS 1.1** - 2006'da yayınlandı, güvenlik açıkları var
> - **TLS 1.2** - 2008'da yayınlandı, güvenli kabul edilir (minimum önerilen)
> - **TLS 1.3** - 2018'de yayınlandı, en güvenli versiyon

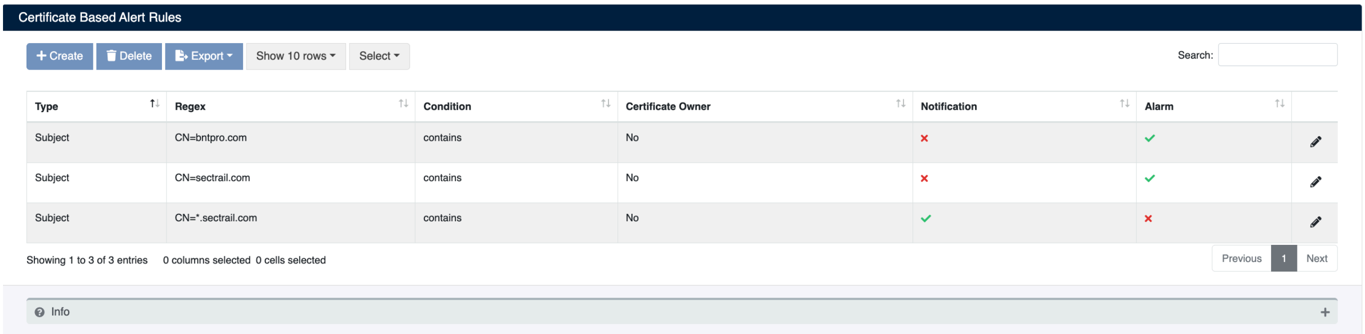
Yapılandırmayı Kaydetme

Tüm alanları doldurduktan sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

:::success Başarılı Kayıt Yapılandırma kaydedildikten sonra belirlenen periyotta ve saatte, seçilen TLS versiyonlarını kullanan sunucular için otomatik bildirimler gönderilmeye başlanacaktır. :::

Sertifika Bazlı Alarm Kuralları

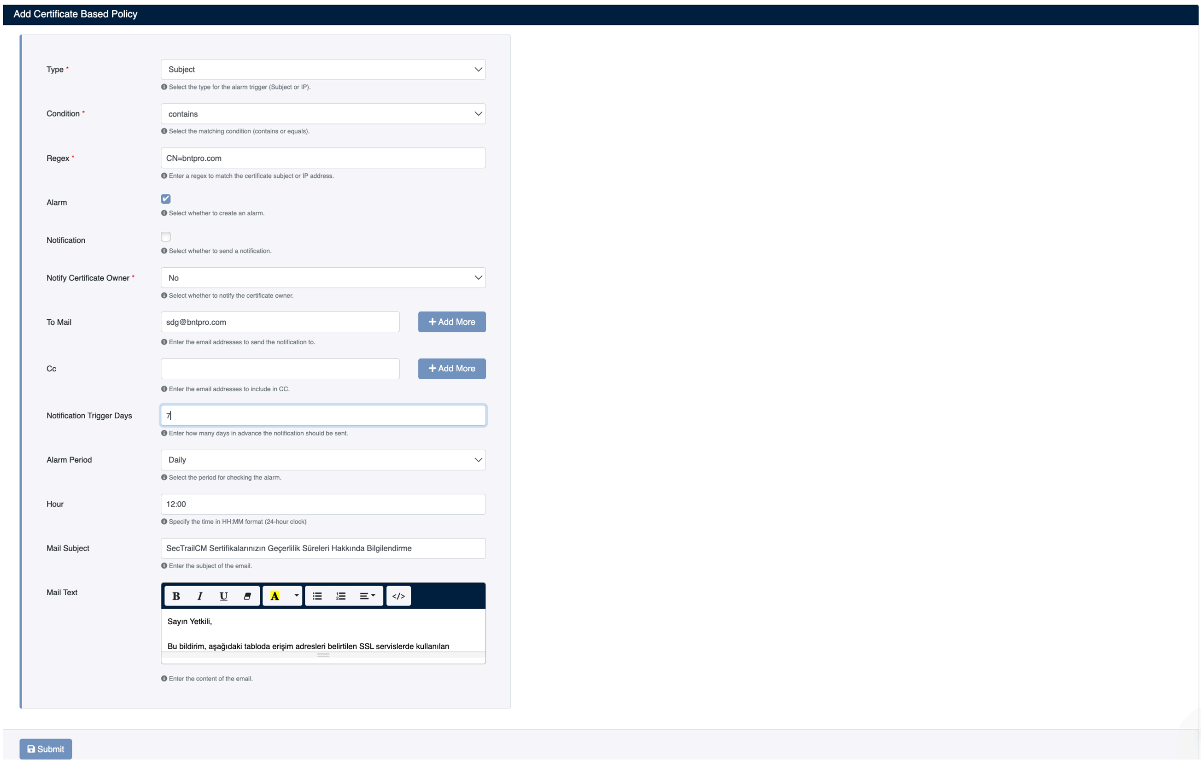
SecTrail CM, sertifika subject'i veya IP adresine göre özelleştirilmiş alarm ve bildirim kuralları tanımlamanıza olanak tanır. **Monitoring -> Alert Rules -> Certificate Based** bölümünden bu kurallara erişebilirsiniz.



Listede tanımlı her kural için **Type**, **Regex**, **Condition**, **Certificate Owner**, **Notification** ve **Alarm** sütunları görüntülenir.

Yeni Kural Oluşturma

+ Create butonuna tıklayarak yeni bir sertifika bazlı alarm kuralı ekleyin:



- **Type**: Alarm tetikleyicisinin tipini seçin (`Subject` veya `IP`)
- **Condition**: Eşleşme koşulunu seçin (`contains` veya `equals`)
- **Regex**: Sertifika subject'i veya IP adresiyle eşleştirilecek ifadeyi girin (örn. `CN=bntpro.com`)
- **Alarm**: Kural eşleştiğinde alarm oluşturulsun mu?
- **Notification**: Sertifika yenilendikten sonra bildirim gönderilsin mi?

> **YENİLEME BİLDİRİMİ**
>
> **Notification** seçeneği aktif olduğunda, eşleşen sertifika yenilendiğinde ilgili kişilere otomatik olarak yenileme bildirimi iletilir.

- **Notify Certificate Owner**: Sertifika sahibine bildirim gönderilsin mi? (`Yes` / `No`)
- **To Mail**: Bildirimin iletileceği e-posta adresleri; **+ Add More** ile birden fazla eklenebilir
- **Cc**: Kopyalanacak e-posta adresleri
- **Notification Trigger Days**: Bildirim kaç gün öncesinden gönderilmeye başlansın?
- **Alarm Period**: Alarm kontrol periyodu (`Daily` , `Weekly` vb.)
- **Hour**: Alarmın kontrol edileceği saat (HH:MM formatında)
- **Mail Subject**: Bildirim e-postasının konu satırı
- **Mail Text**: Bildirim e-postasının içerik şablonu (zengin metin editörü ile düzenlenebilir)

Envanter Yönetimi

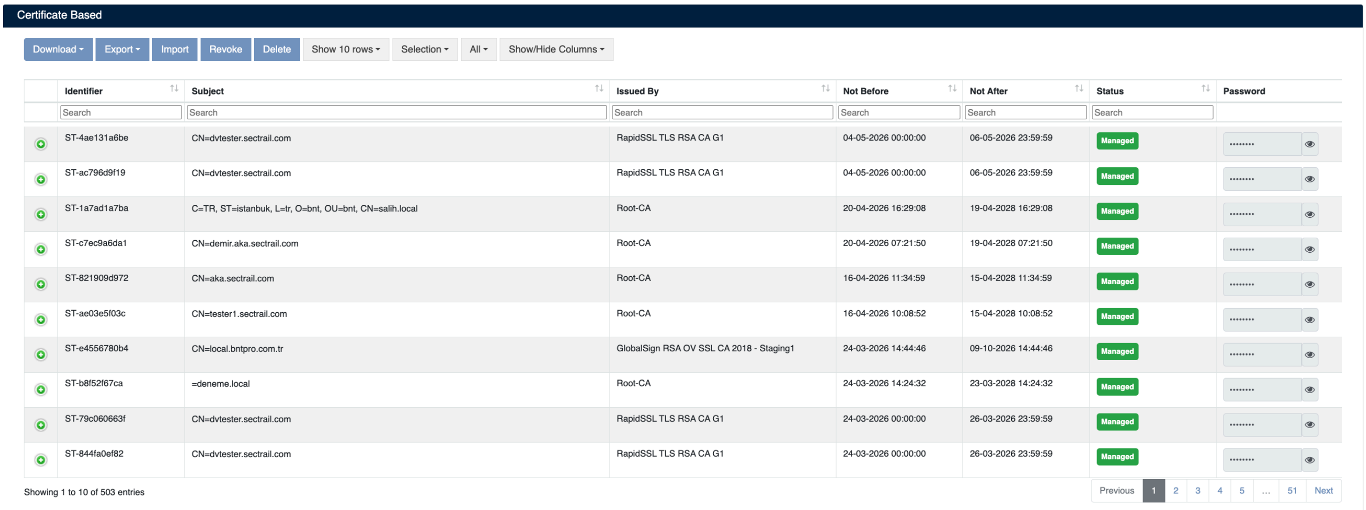
Bu kılavuz, SecTrail CM'de sertifika envanterinin nasıl yönetileceğini, sertifikaların içe aktarılması, CSR (Certificate Signing Request) yönetimi ve sertifika listelerinin takibini adım adım anlatır.

> **ÖZELLİK HAKKINDA**
>
> Envanter yönetimi, SecTrail CM üzerinden imzalanan sertifikaların ve dışarıdan içe aktarılan sertifikaların merkezi listesini görüntülemenizi sağlar. Keşif yoluyla bulunan sertifikalar için Keşif Yapılandırması sayfasını inceleyin.

Sertifika Listesi

Tüm içe aktarılan ve keşfedilen sertifikaları merkezi bir listede görüntüleyin ve yönetin.

> **ERİŞİM YOLU**
>
> Sertifika listesine erişmek için: **Inventory -> Certificate Store -> Certificate&Keys** menüsüne gidin.



Sertifika Listesi - Tüm Sertifikalar ve Durumları

Liste Bilgileri

Sertifika listesinde her sertifika için aşağıdaki detaylar görüntülenir:

Sütun	Açıklama
Identifier	Sertifika için otomatik oluşturulan benzersiz kimlik
Created At	Sertifikanın sisteme eklenme tarihi ve saati
Subject	Sertifikanın subject bilgileri (CN, O, OU, C, ST, L)
Certificate Type	Sertifika tipi (CERT/KEY, Certificate, CSR)
Issued By	Sertifikayı imzalayan CA (Certificate Authority)
Not Before	Sertifikanın geçerlilik başlangıç tarihi ve saati
Not After	Sertifikanın geçerlilik bitiş tarihi ve saati
Status	Sertifikanın yönetim durumu: `Managed` (Yönetilen) veya `Monitored` (İzlenen)
Password	Sertifika özel anahtar parolası

Sertifika Durumları

Her sertifikanın solunda bir durum göstergesi bulunur:

İkon	Durum	Açıklama
	Active	Sertifika geçerli ve aktif
	Expiring Soon	Sertifika yakında sona erecek
	Expired	Sertifikanın süresi dolmuş

Yapılabilecek İşlemler

Üst Menü İşlemleri

- **Show 10 rows** - Sayfa başına gösterilecek sertifika sayısını ayarlayın
- **Selection** - Toplu işlemler için sertifika seçimi
- **Export** - Sertifika listesini dışa aktarma (CSV, Excel, PDF)
- **Import** - Yeni sertifika içe aktarma
- **Revoke** - Seçili sertifikaları iptal etme
- **Delete** - Seçili sertifikaları silme
- **Download** - Seçili sertifikaları farklı formatlarda indirme (Zip, Pfx, Jks, Cer, Chain, Bundle, Der, P7b, Key)
- **Last** - Son eklenen sertifikaları görüntüleme
- **Show/Hide Columns** - Görüntülenecek sütunları özelleştirme

Filtreleme ve Arama

Liste üzerinde her sütun için arama yapabilir ve sayfa başına gösterilecek kayıt sayısını ayarlayabilirsiniz.

Satır Bazlı İşlemler

Her sertifika satırında görüntüleme, indirme, silme ve detay görüntüleme işlemlerini yapabilirsiniz.

Toplu İşlemler

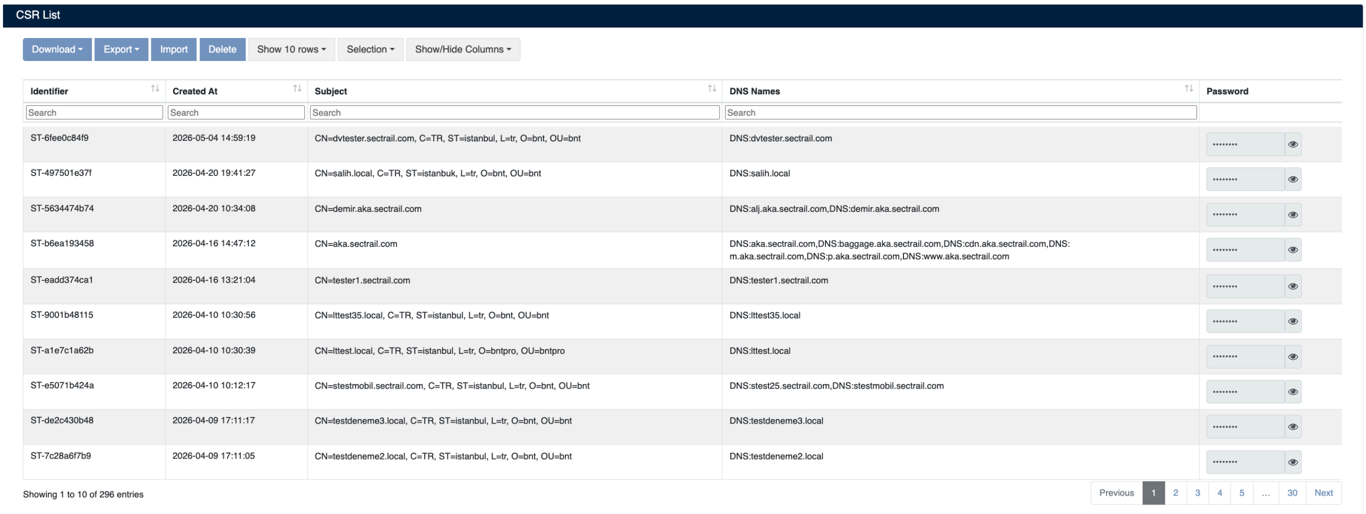
Birden fazla sertifika seçerek toplu olarak Export, Download, Revoke veya Delete işlemleri yapabilirsiniz.

> **DİKKAT**
>
> **Revoke** işlemi sertifikayı CA'dan iptal ettirir ve geri alınamaz. **Delete** işlemi ise sadece SecTrail CM envanterinden kaldırır.

CSR Listesi

Tüm sertifika taleplerini (CSR) merkezi bir listede görüntüleyebilir ve yönetebilirsiniz.

> **ERİŞİM YOLU**
>
> CSR listesine erişmek için: **Inventory -> Certificate&Keys -> CSR List** menüsüne gidin.



CSR Listesi - Sertifika Talepleri

Liste Bilgileri

CSR listesinde her kayıt için aşağıdaki bilgiler görüntülenir:

Sütun	Açıklama
Identifier	CSR için otomatik oluşturulan benzersiz kimlik
Created At	CSR'nin oluşturulma tarihi ve saati
Subject	CSR'de bulunan subject bilgileri (CN, O, OU, C, ST, L)
E-Mail Address	CSR'de tanımlı e-posta adresi
Certificate Type	CSR tipi (genellikle `CSR`)
Password	CSR'nin özel anahtar parolası (varsa gizli gösterilir)

Yapılabilecek İşlemler

Üst Menü İşlemleri

- **Show 10 rows** - Sayfa başına gösterilecek kayıt sayısını ayarlayın
- **Selection** - Toplu işlemler için CSR seçimi
- **Export** - CSR listesini dışa aktarma
- **Import** - Yeni CSR ekleme
- **Delete** - Seçili CSR'leri silme
- **Download** - Seçili CSR'leri indirme

Filtreleme ve Arama

Liste üzerinde her sütun için arama yapabilir ve sayfa başına gösterilecek kayıt sayısını ayarlayabilirsiniz.

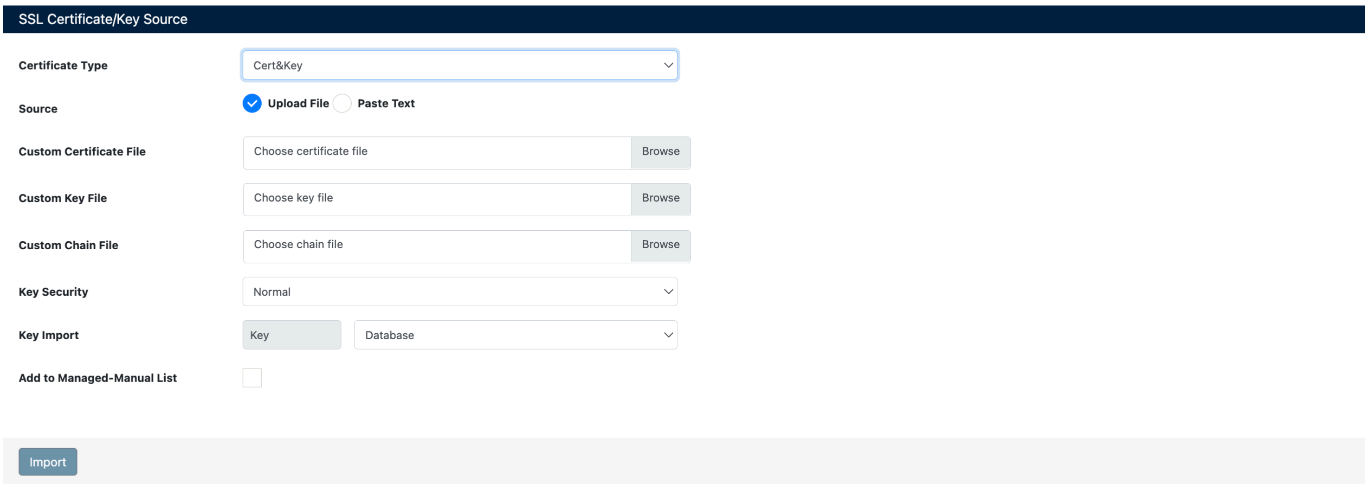
Satır Bazlı İşlemler

Her CSR satırında görüntüleme, indirme ve silme işlemlerini yapabilirsiniz.

Sertifika İçe Aktarma

SecTrail CM, farklı sertifika tiplerini ve kaynaklarını destekleyen esnek içe aktarma seçenekleri sunar.

> **ERİŞİM YOLU**
>
> Sertifika içe aktarmak için: **Inventory -> Certificate Store -> Certificate&Keys** veya **CSR List** sayfasına gidin ve **Import** butonuna tıklayın.



Sertifika İçe Aktarma Ekranı

Sertifika Tipleri

İçe aktarma ekranında aşağıdaki sertifika tiplerinden birini seçebilirsiniz:

Tip	Açıklama	Kullanım Durumu
Cert&Key	Sertifika ve özel anahtar (private key) birlikte	Mevcut aktif sertifikaları ve anahtarlarını içe aktarmak için
Certificate	Sadece sertifika dosyası	İzleme amaçlı veya anahtar olmadan sadece sertifika eklemek için
CSR	Certificate Signing Request	Sertifika talepleri oluşturmak ve yönetmek için
PKCS12	PKCS#12 formatında paketlenmiş sertifika ve anahtar	Windows veya Java ortamlarından export edilen sertifikalar için

Cert&Key İçe Aktarma

Sertifika ve özel anahtarı birlikte içe aktarmak için kullanılır.

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
Certificate Type	İçe aktarılacak veri tipini seçin	`Cert&Key` seçin
Source	Sertifika ve anahtarı nasıl sağlayacağınızı belirleyin	- **Upload File:** Dosya yükleme - **Paste Text:** Metin yapıştırma
Custom Certificate File	Sertifika dosyasını yükleyin	`.crt` , `.cer` , `.pem` formatlarında
Custom Key File	Özel anahtar dosyasını yükleyin	`.key` , `.pem` formatlarında
Custom Chain File	(Opsiyonel) Sertifika zinciri dosyası	Intermediate ve Root CA sertifikaları için
Key Security	Anahtar güvenlik seviyesini belirleyin	- **Normal:** Şifresiz anahtar - **Password:** Şifreli anahtar (passphrase gerekli)
Key Import	Anahtarın nerede saklanacağını seçin	- **Key:** SecTrail CM veritabanında - **Database:** Ayrı database'de saklama
Add to Managed-Manual List	Sertifikayı yönetilen listeye ekle	Manuel yönetim için işaretleyin

> **ÖNEMLİ**
>
> - **Custom Chain File** kullanarak ara CA (Intermediate CA) ve root CA sertifikalarını da eklemelisiniz
> - Şifreli anahtarlar için **Key Security** alanında `Password` seçin ve parolayı girin
> - **Key Import** seçeneği, anahtarların güvenli saklanması için önemlidir

Adımlar

1. **Certificate Type** olarak `Cert&Key` seçin
2. **Source** olarak `Upload File` veya `Paste Text` seçin
3. **Browse** butonları ile sertifika, anahtar ve chain dosyalarını yükleyin veya içeriklerini yapıştırın
4. Anahtar şifreli ise **Key Security** `Password` seçin ve parolayı girin
5. **Key Import** metodunu seçin (Key veya Database)

6. İsteğe bağlı olarak **Add to Managed-Manual List** seçeneğini işaretleyin
7. **Import** butonuna tıklayarak içe aktarmayı tamamlayın

Certificate İçe Aktarma

Sadece sertifika dosyası içe aktarmak için kullanılır (özel anahtar olmadan).

> **NE ZAMAN KULLANILIR?**
>
> - Public sertifikaları izleme amaçlı eklerken
> - Sadece izleme (monitoring) yapılacak sertifikalar için
> - Özel anahtarınız olmayan üçüncü parti sertifikalar için

Yapılandırma

Certificate Type olarak `Certificate` seçin ve sadece sertifika dosyasını yükleyin. Diğer adımlar Cert&Key ile aynıdır.

CSR İçe Aktarma

Sertifika talep dosyalarını (CSR) içe aktarmak için kullanılır.

> **CSR NEDİR?**
>
> Certificate Signing Request (CSR), bir sertifika otoritesinden (CA) SSL/TLS sertifikası talep ederken kullanılan özel bir dosyadır. CSR, domain adı, organizasyon bilgileri ve public key içerir.

Yapılandırma

1. **Certificate Type** olarak `CSR` seçin
2. CSR dosyasını yükleyin veya içeriğini yapıştırın
3. **Import** butonuna tıklayın

PKCS12 İçe Aktarma

PKCS#12 formatında paketlenmiş sertifika ve anahtarları içe aktarır.

> **PKCS12 NEDİR?**
>
> PKCS#12 (genellikle `.pfx` veya `.p12` uzantılı), sertifika, özel anahtar ve chain'i tek bir dosyada paketleyen bir formattır. Windows IIS ve Java Keystore'lardan export edilirken yaygın olarak kullanılır.

Yapılandırma

1. **Certificate Type** olarak `PKCS12` seçin
2. `.pfx` veya `.p12` dosyasını yükleyin
3. PKCS12 dosyasının parolasını girin (varsa)
4. **Import** butonuna tıklayın

Keşfedilen Sertifikalar

Keşif işlemleri sonucunda bulunan tüm sertifikaları görüntüleyebilir, yönetebilir ve kategorize edebilirsiniz.

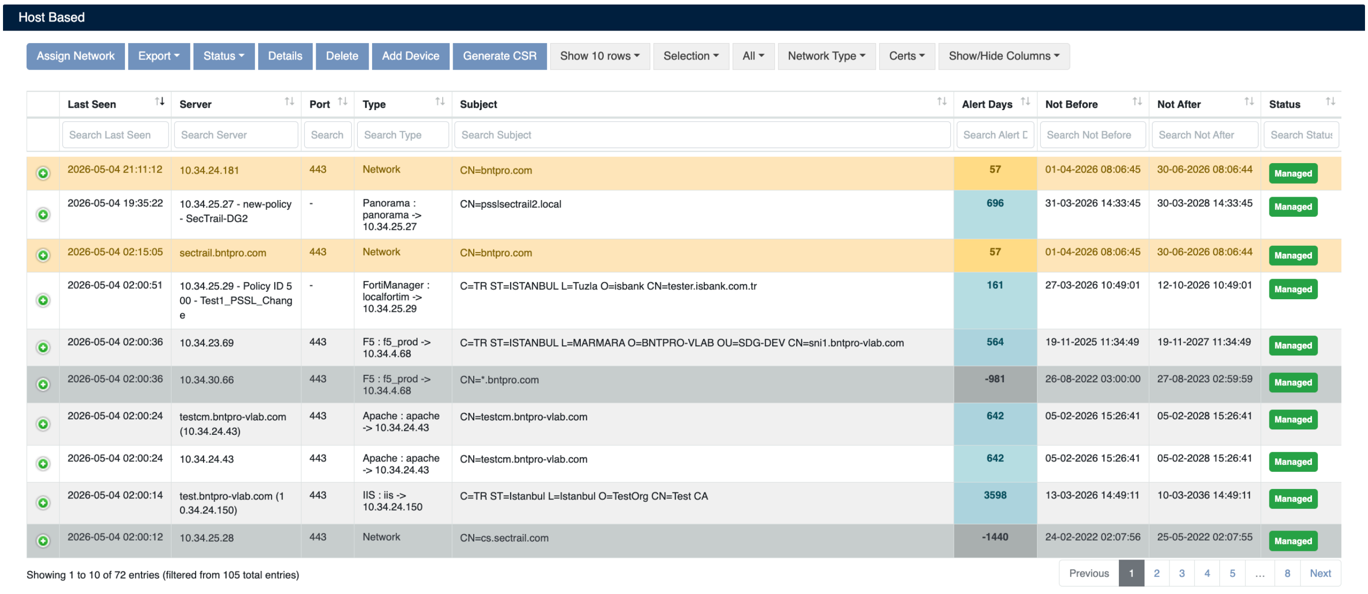
> **ERİŞİM YOLU**
>
> Keşfedilen sertifikaları görüntülemek için uygulama panelinde şu yolları kullanabilirsiniz:
>
> - **Inventory -> Certificate Registry -> Host Based** - Sunucu bazlı görünüm
> - **Inventory -> Certificate Registry -> Certificate Based** - Sertifika bazlı görünüm

Keşfedilen Sertifikalar Listesi

SecTrail CM'de keşfedilen sertifikaları iki farklı görünümde inceleyebilirsiniz:

- **Sertifika Bazlı Liste** - Her benzersiz sertifikayı tek satırda gösterir
- **Sunucu Bazlı Liste** - Sertifikaları bulundukları sunuculara göre listeler

Sunucu Bazlı Liste Görünümü



Keşfedilen Sertifikalar - Sunucu Bazlı Görünüm

Liste Bilgileri

Sunucu bazlı görünümde her satır için aşağıdaki bilgiler görüntülenir:

- **Last Seen** - Sertifikanın son görülme tarihi ve zamanı
- **Server** - Sertifikanın bulunduğu sunucunun IP adresi veya hostname
- **Port** - Sertifikanın hangi portta çalıştığı (örn: `443` , `8443`)
- **Type** - Sertifikanın ağ tipi (`Network` , `External` , `F5` , vb.)
- **Subject** - Sertifikanın Common Name (CN) bilgisi
- **Not Before** - Sertifikanın geçerlilik başlangıç tarihi

- **Not After** - Sertifikanın geçerlilik bitiş tarihi
- **Status** - Sertifikanın lisans durumu (`Managed` veya `Monitored`)

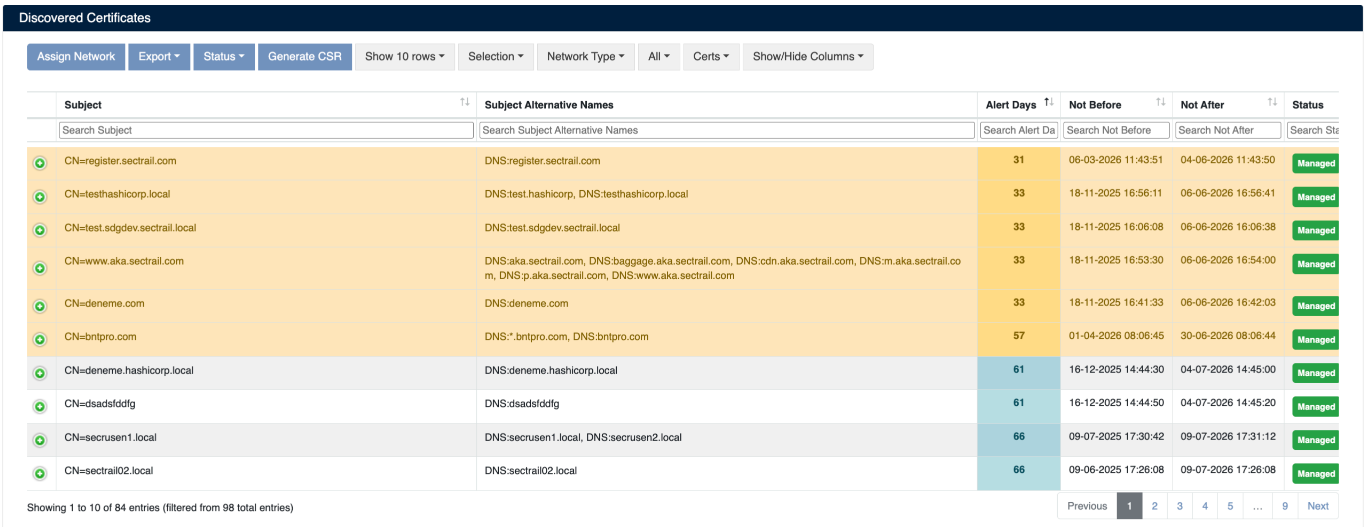
Liste Üzerindeki İşlemler

Sayfanın üst kısmında bulunan araç çubuğundan şu işlemleri yapabilirsiniz:

- **Show X rows** - Sayfa başına gösterilecek satır sayısını ayarlayın (25, 50, 100)
- **Selection** - Birden fazla satırı seçerek toplu işlem yapın
- **Export** - Listeyi dışa aktarın (Excel, CSV, PDF formatlarında)
- **Status** - Lisans durumuna göre filtreleyin (`Managed` , `Monitored`)
- **Details** - Seçili sertifikanın detaylarını görüntüleyin
- **Delete** - Seçili kayıtları silin
- **Add Device** - Yeni cihaz ekleyin
- **Generate CSR** - Sertifika imzalama isteği (CSR) oluşturun
- **Last** - Son görülme zamanına göre filtreleyin
- **Network Type** - Ağ tipine göre filtreleyin
- **Certs** - Sertifika zinciri türüne göre filtreleyin (Sunucu Sertifikası, İmzalayan Sertifikası)
- **Show/Hide Columns** - Görüntülenecek sütunları özelleştirin

> **KOLON ÖZELLEŞTİRME**
>
> **Show/Hide Columns** butonu ile görüntülenen sütunları özelleştirebilirsiniz. İhtiyacınıza göre sütunları ekleyip çıkararak listeyi daha verimli kullanabilirsiniz.

Sertifika Bazlı Liste Görünümü



Keşfedilen Sertifikalar - Sertifika Bazlı Görünüm

Liste Bilgileri

Sertifika bazlı görünümde her satır benzersiz bir sertifikayı temsil eder ve aşağıdaki bilgileri içerir:

- **Subject** - Sertifikanın Common Name (CN) ve DN bilgileri
- **Subject Alternative Names** - Sertifikanın SANs (DNS adları) listesi

- **Not Before** - Sertifikanın geçerlilik başlangıç tarihi
- **Not After** - Sertifikanın geçerlilik bitiş tarihi
- **Status** - Sertifikanın lisans durumu

Status (Lisans Durumu)

Keşfedilen sertifikalar için iki farklı durum bulunur:

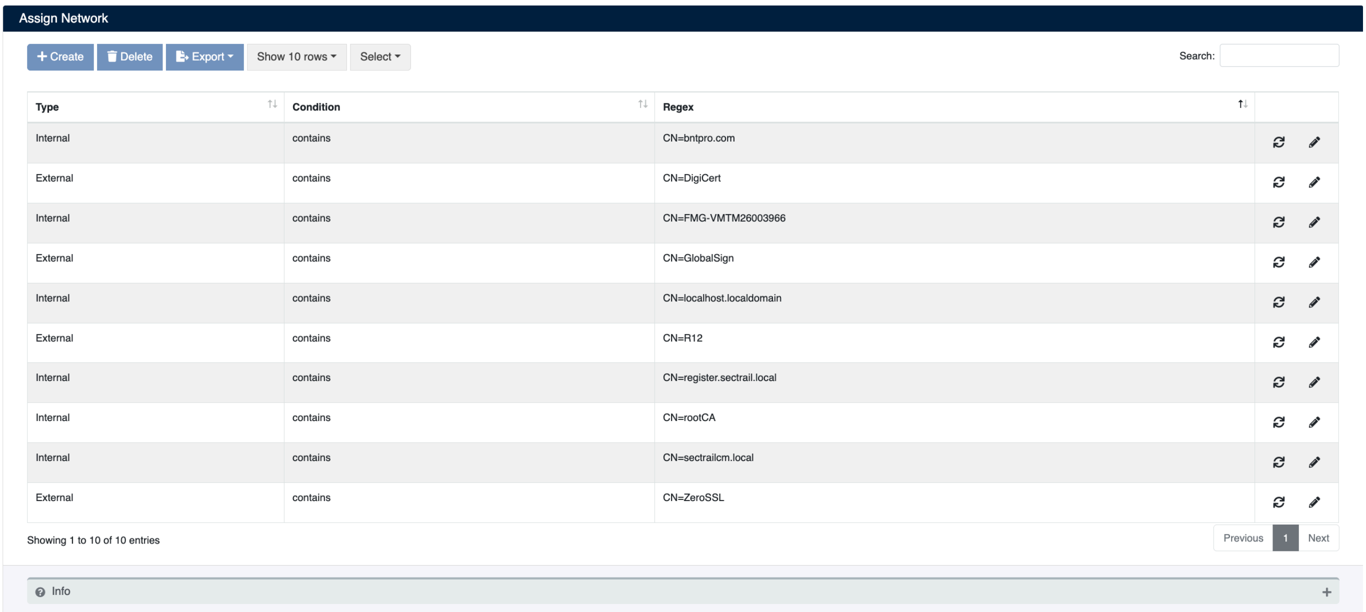
Durum	Açıklama	Kullanım Amacı
Managed	SecTrail CM tarafından tam olarak yönetilen sertifikalar	Otomatik yenileme, deployment, yaşam döngüsü
Monitored	Sadece envanterde görüntülenen sertifikalar (read-only)	Envanter görünürlüğü sağlar, alarm/uyarı yoktur

> **MANAGED VS MONİTORED**
>
> - **Managed:** Sertifikalar üzerinde tam kontrol - oluşturma, yenileme, deployment, rotasyon işlemleri yapılabilir
> - **Monitored:** Sadece envanter görünürlüğü - sertifikalar envanterde görüntülenir, ancak alarm, uyarı ve yönetim işlemleri yapılamaz

Network Configuration (Ağ Tipi Yapılandırması)

Network Type sütunundaki değerler, sertifikaların hangi ağ kategorisinde olduğunu belirler. Bu değerler **Network Configuration** özelliği ile özelleştirilebilir.

> **NETWORK CONFİGURATİON ERİŞİM**
>
> **Inventory -> Certificate Registry -> Certificate Based** veya **Host Based** sayfalarında bulunan **Assign Network** butonuna tıklayarak ağ tipi yapılandırma ayarlarına erişebilirsiniz.



Type	Condition	Regex
Internal	contains	CN=bntpro.com
External	contains	CN=DigiCert
Internal	contains	CN=FMG-VMTM26003966
External	contains	CN=GlobalSign
Internal	contains	CN=localhost.localdomain
External	contains	CN=R12
Internal	contains	CN=register.sectrail.local
Internal	contains	CN=rootCA
Internal	contains	CN=sectrailcm.local
External	contains	CN=ZeroSSL

Network Configuration Yönetimi - Ağ Tipi Tanımlamaları

Network Configuration Nedir?

Network Configuration, sertifikaları Subject (CN) bilgisine göre otomatik olarak kategorize etmenizi sağlar. Bu sayede:

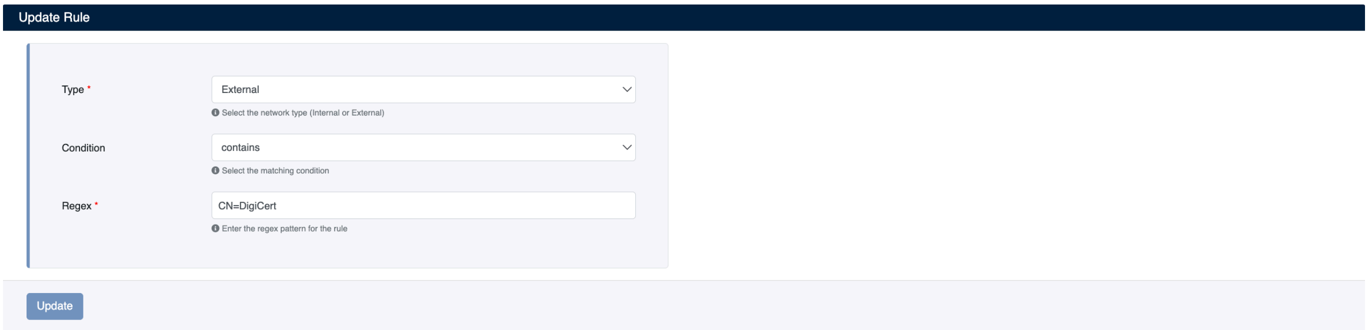
- İç (Internal) ve dış (External) sertifikaları otomatik ayırabilirsiniz
- Belirli imzalayan otoritelere (CA) ait sertifikaları gruplandırabilirsiniz
- Sertifika raporlamalarını daha anlamlı hale getirebilirsiniz
- Filtreleme ve arama işlemlerini hızlandırabilirsiniz

Network Configuration Listesi

Liste sayfasında tanımlı tüm ağ tipi kurallarını görebilirsiniz:

- **Type** - Ağ tipi kategorisi (`External` , `Internal`)
- **Condition** - Eşleştirme koşulu (genellikle `contains` - içerir)
- **Regex** - Eşleştirme kuralı (Subject içinde aranacak metin veya regex)

Yeni Network Configuration Oluşturma



Yeni Network Configuration Ekleme Formu

Yapılandırma Parametreleri

Parametre	Açıklama	Seçenekler
Type	Ağ tipini belirleyin	- **External:** Dış sertifikalar (public CA'lar tarafından imzalanan) - **Internal:** İç sertifikalar (private CA'lar, self-signed)
Condition	Eşleştirme yöntemini seçin	- **contains:** Subject içinde metin aranır (çoğu durumda kullanılır) - **equals:** Tam eşleşme - **regex:** Düzenli ifade ile eşleştirme
Regex	Subject içinde aranacak metni veya regex desenini girin	- `CN=GlobalSign` (GlobalSign'ı içeren tüm sertifikalar) - `CN=localhost` (localhost sertifikaları) - `CN=.*\.mycompany\.com` (mycompany.com altındaki tüm subdomain'ler)

Form bilgilerini girdikten sonra **Submit** butonuna tıklayarak yapılandırmayı kaydedin.

Sertifika Detaylarını Görüntüleme

Herhangi bir sertifika satırına tıklayarak veya **Details** butonuna basarak sertifikanın detaylı bilgilerini görüntüleyebilirsiniz:

- **Subject DN** - Tam Distinguished Name bilgisi
- **Issuer DN** - Sertifikayı imzalayan CA bilgisi
- **Serial Number** - Sertifika seri numarası
- **Signature Algorithm** - İmza algoritması (örn: SHA256withRSA)
- **Public Key** - Public key bilgisi ve algoritması
- **Validity** - Geçerlilik tarihleri (Not Before / Not After)
- **Extensions** - Sertifika uzantıları (SAN, Key Usage, vb.)
- **Thumbprint** - Sertifika parmak izi (SHA1, SHA256)

> **OTOMASYON İPUCU**
>
> Network Configuration kurallarını doğru tanımladığınızda, yeni keşfedilen sertifikalar otomatik olarak doğru kategorilere atanır ve manuel işlem gerekmez.

Yönetilen-Manuel Liste

Bu kılavuz, SecTrail CM'de keşif yapılamayan sertifikaların nasıl manuel olarak yönetilen listeye ekleneceğini ve izleneceğini anlatır.

> **ÖZELLİK HAKKINDA**
>
> Yönetilen-Manuel Liste, network üzerinden keşfedilemeyen sertifikaları alarm ve monitoring sistemine dahil etmenizi sağlar. Bu sayede, tüm sertifikalarınızı merkezi bir noktadan izleyebilir ve süre dolumu alarmları alabilirsiniz.

Genel Bakış

Ne Zaman Kullanılır?

Yönetilen-Manuel Liste, aşağıdaki durumlarda kullanılır:

- Network taraması ile erişilemeyen internal sistemlerdeki sertifikalar
- Firewall arkasındaki sertifikalar
- Offline sistemlerdeki sertifikalar
- Manuel olarak yönetilmesi gereken test sertifikaları

Temel Özellikler

Alarm ve Monitoring : Eklenen sertifikalar için süre dolumu alarmları oluşturulur

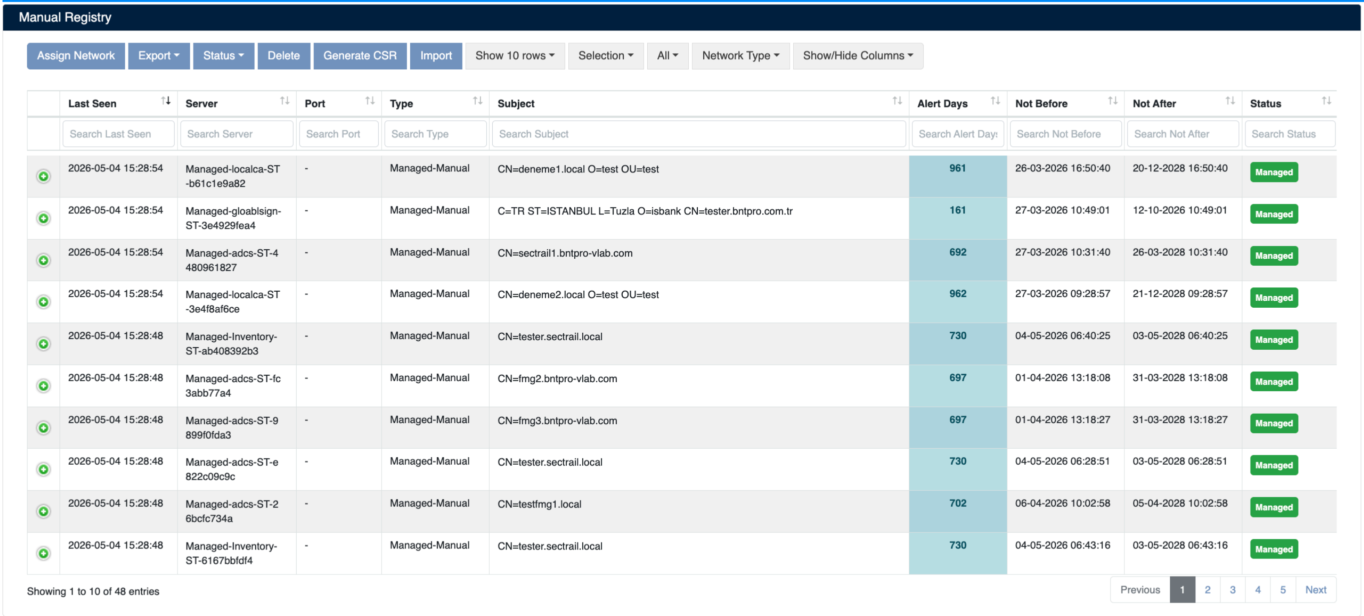
Manuel Yönetim : Network keşfi yapılamayan sertifikaları manuel olarak izleme altına alın

Merkezi İzleme : Tüm sertifikalarınızı tek bir noktadan takip edin

Yönetilen-Manuel Sertifikalar Listesi

Manuel olarak eklenen veya yönetilen listeye dahil edilen sertifikalar bu listede görüntülenir.

> **ERİŞİM YOLU**
>
> Yönetilen-Manuel Sertifikalar listesine erişmek için: **Inventory -> Certificate Registry -> Manual Registry** menüsüne gidin.



Yönetilen-Manuel Sertifikalar Listesi

Liste Bilgileri

Yönetilen-Manuel Sertifikalar listesinde her sertifika için aşağıdaki bilgiler görüntülenir:

Sütun	Açıklama
Last Seen	Sertifikanın son görülme tarihi ve saati
Server	Sertifikanın bulunduğu sunucu bilgisi
Port	Sertifikanın kullanıldığı port numarası
Type	Sertifikanın tipi (Managed-Manual, Discovered vb.)
Subject	Sertifikanın subject bilgileri (CN, O, OU, C, ST, L)
Not Before	Sertifikanın geçerlilik başlangıç tarihi
Not After	Sertifikanın geçerlilik bitiş tarihi

Yapılabilecek İşlemler

Üst Menü İşlemleri

- **Show 25 rows** - Sayfa başına gösterilecek kayıt sayısını ayarlayın
- **Selection** - Toplu işlemler için sertifika seçimi
- **Export** - Listeyi dışa aktarma
- **Import** - Manuel sertifika ekleme
- **Delete** - Seçili sertifikaları listeden kaldırma
- **Last** - Son eklenen sertifikaları görüntüleme
- **Network Type** - Network tipine göre filtreleme
- **Show/Hide Columns** - Görüntülenecek sütunları özelleştirme

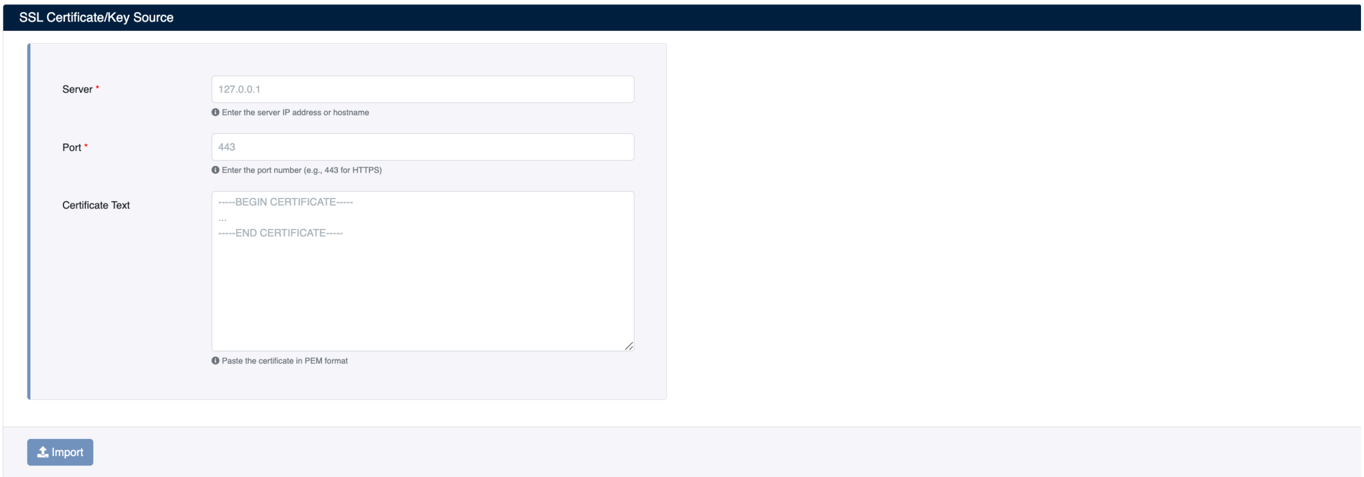
Filtreleme ve Arama

Liste üzerinde her sütun için arama yapabilir ve sayfa başına gösterilecek kayıt sayısını ayarlayabilirsiniz.

Manuel Sertifika Ekleme

Network üzerinden keşfedilemeyen sertifikaları manuel olarak ekleyebilirsiniz. İki farklı yöntem kullanabilirsiniz:

> **ERİŞİM YOLU**
>
> **Inventory -> Certificate Registry -> Manual Registry -> Import** menüsünden ekleme ekranına ulaşın.



Manuel Sertifika Ekleme Ekranı

Ekleme Yöntemleri

Server ve Port ile Otomatik Çekme

Sunucuya erişiminiz varsa, IP adresi ve port bilgisi vererek sertifikayı otomatik olarak çekebilirsiniz:

1. **Server** alanına IP adresi veya hostname girin (örn: `192.168.1.100`, `internal.example.com`)
2. **Port** alanına port numarasını girin (örn: `443`, `8443`)
3. **Import** butonuna tıklayın
4. Sistem otomatik olarak sertifikayı çekip listeye ekler

> **OTOMATİK ÇEKME**
>
> Bu yöntemde SecTrail CM, belirtilen sunucu ve porttan sertifikayı otomatik olarak çeker. Sunucuya erişim mevcut olmalıdır.

Certificate Text ile Manuel Ekleme

Sunucuya erişim yoksa veya sertifika dosyası elinizde varsa, sertifika metnini (PEM formatı) doğrudan yapıştırabilirsiniz:

1. **Certificate Text** alanına sertifika metnini yapıştırın (`-----BEGIN CERTIFICATE-----` ile başlamalı)
2. İsteğe bağlı olarak **Server** ve **Port** bilgilerini girin (açıklama amaçlı)
3. **Import** butonuna tıklayın

Inventory'den Yönetilen-Manuel Listeye Ekleme

Sertifika Listesi'nde bulunan sertifikaları da Yönetilen-Manuel listesine ekleyebilirsiniz.

Adımlar

1. **Inventory -> Certificate Registry** menüsüne gidin
2. Yönetilen-Manuel listesine eklemek istediğiniz sertifikayı seçin
3. Sertifika detay sayfasında **Add to Managed-Manual List** seçeneğini işaretleyin
4. Değişiklikleri kaydedin

> **KULLANIM SENARYOSU**
>
> Bu özellik, içe aktarılan veya başka yöntemlerle eklenen sertifikaları izleme altına almak için kullanılır.

Sertifika Oluşturma

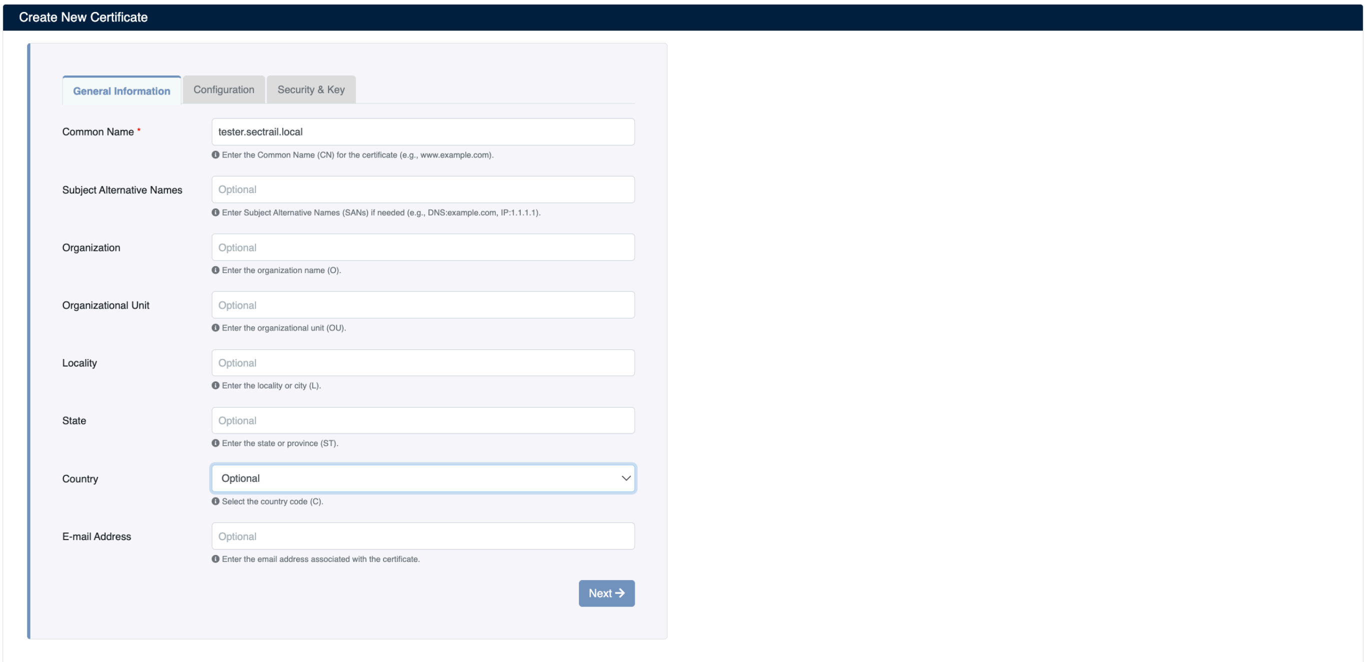
Bu kılavuz, SecTrail CM üzerinden farklı tiplerde sertifika oluşturma işlemlerini adım adım anlatır. SecTrail CM, kendi Certificate Authority (CA) altyapınızı yönetmenizi ve çeşitli amaçlar için sertifika imzalamanızı sağlar.

> **ÖZELLİK HAKKINDA**
>
> Sertifika oluşturma özelliği ile Root CA, Intermediate CA, Self-Signed, CSR ve harici CA ile imzalama işlemlerini gerçekleştirebilirsiniz. Her sertifika tipi farklı kullanım senaryoları için optimize edilmiştir.

Sertifika Oluşturma Ekranı

Yeni bir sertifika oluşturmak için SecTrail CM'de yerleşik sertifika yöneticisini kullanabilirsiniz.

> **ERİŞİM YOLU**
>
> Sertifika oluşturmak için: **Inventory -> Issue Certificate -> New Certificate** menüsüne gidin.



Sertifika Oluşturma Formu - Genel Bilgiler

Sertifika Tipleri

SecTrail CM, farklı kullanım senaryoları için aşağıdaki sertifika tiplerini destekler:

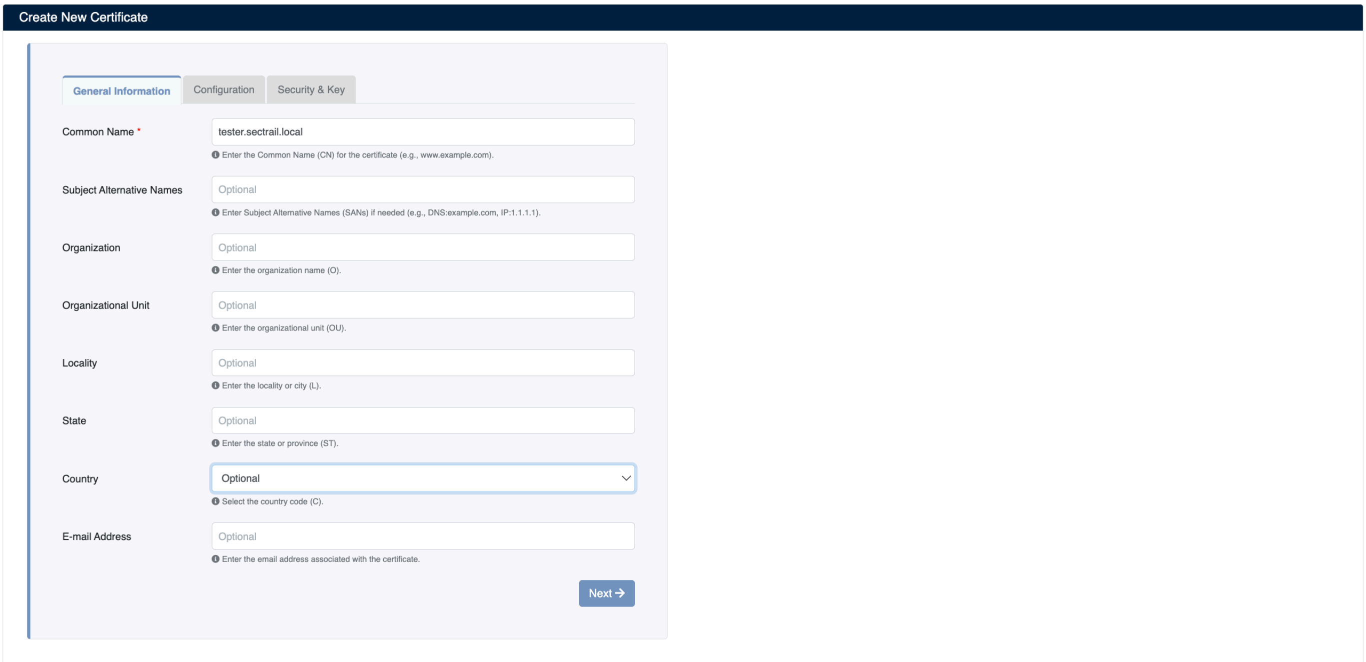
Sertifika Tip Seçenekleri

Sertifika Tipi	Açıklama	Kullanım Amacı
Root CA	Kök sertifika otoritesi	CA altyapınızın en üst seviyesi, diğer tüm sertifikaları imzalar
Intermediate CA	Ara sertifika otoritesi	Root CA'dan imzalanır, son kullanıcı sertifikalarını imzalar
Self-Signed	Kendi kendine imzalı sertifika	Test ortamları, dahili uygulamalar, development için
Sign With Local CA	Yerel CA ile imzalama	SecTrail CM'deki mevcut CA ile yeni sertifika imzalama
CSR	Certificate Signing Request	Harici CA'lardan imzalanmak üzere sertifika talebi oluşturma
External CA	Harici CA ile imzalama	ADCS, GlobalSign, DigiCert, Hashicorp Vault gibi entegre CA'lar ile imzalama

Sertifika Parametreleri

Sertifika oluşturma formu üç sekme halinde sunulur.

Sekme 1: General Information

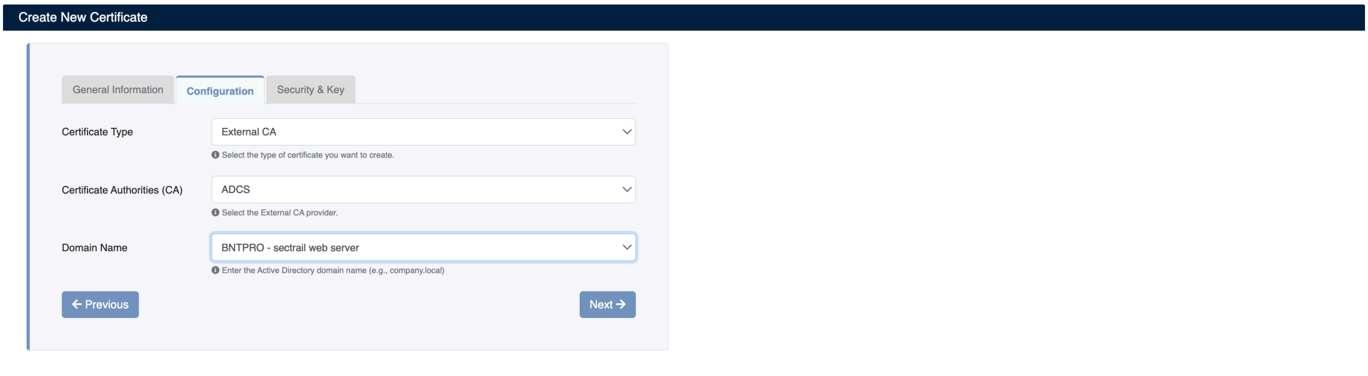


- **Common Name**: Sertifikanın ana alan adı (FQDN) — zorunlu (örn. `example.com`, `*.example.com`)
- **Subject Alternative Names**: Ek alan adları ve IP adresleri (örn. `DNS:example.com,IP:1.1.1.1`)
- **Organization**: Organizasyon adı (O)
- **Organizational Unit**: Departman veya birim (OU)
- **Locality**: Şehir (L)
- **State**: Eyalet veya il (ST)

- **Country**: Ülke kodu — dropdown'dan seçim (C)
- **E-mail Address**: İletişim e-posta adresi

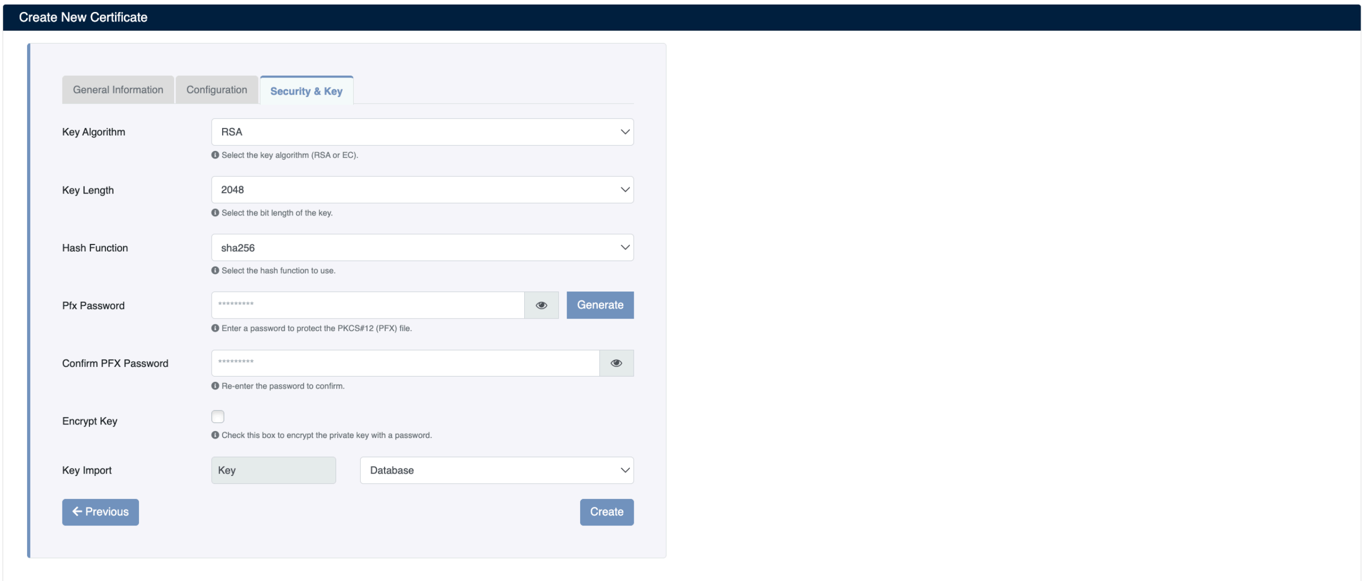
> **SUBJECT ALTERNATİVE NAMES (SAN)**
>
> SAN alanında birden fazla değeri virgülle ayırın: `DNS:example.com,DNS:www.example.com,IP:1.1.1.1`

Sekme 2: Configuration



- **Certificate Type**: Sertifika tipi (External CA, Local CA, Self-Signed, CSR vb.)
- **Certificate Authorities (CA)**: Kullanılacak harici CA sağlayıcısı (örn. `ADCS`, `GlobalSign`, `DigiCert`)
- **Domain Name**: Active Directory domain adı (External CA için)

Sekme 3: Security & Key



- **Key Algorithm**: Anahtar algoritması (`RSA` veya `EC`)
- **Key Length**: Anahtar bit uzunluğu (örn. `2048`, `4096`)
- **Hash Function**: Hash algoritması (örn. `sha256`)
- **Pfx Password**: Private key koruma parolası; **Generate** ile otomatik oluşturulabilir
- **Confirm PFX Password**: Parola doğrulama
- **Encrypt Key**: Private key şifreli saklanacak mı?

- **Key Import**: Anahtarın nerede saklanacağı (`Key` , `Database` , `HSM` , `BeyondTrust`)

> **ANAHTAR SAKLAMA SEÇENEKLERİ**
>
> SecTrail CM, private key'leri güvenli bir şekilde saklamak için birden fazla seçenek sunar:
>
> - **Key:** Private key sertifika ile birlikte saklanır (varsayılan)
> - **Database:** Şifreli olarak SecTrail CM veritabanında saklanır
> - **HSM (Hardware Security Module):** Donanım güvenlik modülünde saklanır (en güvenli, kurumsal ortamlar için önerilir)
> - **BeyondTrust Password Safe:** BeyondTrust entegrasyonu ile merkezi password vault'ta saklanır
>
> HSM ve BeyondTrust entegrasyonlarının yapılandırılması için Entegrasyonlar sayfasını inceleyin.

Extended Key Usage (EKU) Değerleri

Sertifikanın hangi amaçlarla kullanılabileceğini belirler:

EKU Değeri	Açıklama	Kullanım Durumu
serverAuth	Sunucu kimlik doğrulama	Web sunucuları (HTTPS), TLS/SSL
clientAuth	İstemci kimlik doğrulama	VPN, mutual TLS, kullanıcı sertifikaları
codeSigning	Kod imzalama	Yazılım, uygulama imzalama
emailProtection	E-posta koruma	S/MIME, e-posta şifreleme
timeStamping	Zaman damgalama	Belge ve işlem zaman damgası
ocspSigning	OCSP yanıt imzalama	OCSP responder sertifikaları

Sertifika Tipleri ve Oluşturma Adımları

1. Root CA Oluşturma

Root CA, kendi PKI altyapınızın temelini oluşturur. Tüm diğer sertifikaları imzalamak için kullanılır.

> **NE ZAMAN KULLANILIR?**
>
> - Yeni bir PKI altyapısı kurarken
> - Kendi iç sertifika otoritenizi oluştururken
> - Tüm organizasyon sertifikalarını merkezi yönetmek isterken

Adımlar

1. **Certificate Type** alanından `Root CA` seçin
2. **Temel bilgileri** doldurun:

- **Common Name:** CA adı (örn: `MyCompany Root CA`)
- **Organization:** Şirket adı
- **Country:** Ülke kodu

3. **Güvenlik parametrelerini** ayarlayın:

- **Lifetime:** 3650 gün (10 yıl - Root CA'lar uzun ömürlüdür)
- **Key Length:** 4096 bit (maksimum güvenlik)
- **Hash Function:** sha256 veya sha384

4. **Pfx Password** belirleyin ve onaylayın
5. **Extended Key Usage** alanını boş bırakın (Root CA tüm amaçlar için kullanılır)
6. **Submit** butonuna tıklayın

ÇOK ÖNEMLİ

Root CA private key'i son derece kritiktir. Bu anahtarı kaybederseniz veya çaldırırsanız, tüm PKI altyapınız tehlikeye girer. Mutlaka:

- Güçlü bir parola kullanın
- Yedeğini şifreli olarak alın
- Erişimi sınırlı tutun

2. Intermediate CA Oluşturma

Intermediate CA, Root CA ile son kullanıcı sertifikaları arasında köprü görevi görür.

NE ZAMAN KULLANILIR?

- Root CA'yı korumak için (Root CA çevrimdışı tutulabilir)
- Farklı departmanlar veya bölgeler için ayrı CA'lar oluştururken
- İyi bir güvenlik pratiği olarak (önerilir)

Adımlar

1. **Certificate Type** alanından `Intermediate CA` seçin
2. **Temel bilgileri** doldurun:

- **Common Name:** `MyCompany Intermediate CA`
- **Organization, Country** gibi alanları doldurun

3. **Güvenlik parametrelerini** ayarlayın:

- **Lifetime:** 1825 gün (5 yıl)
- **Key Length:** 2048 veya 4096 bit
- **Hash Function:** sha256

4. **Root CA ile imzalatma:** Sistemdeki mevcut Root CA otomatik olarak bu Intermediate CA'yı imzalayacaktır
5. **Pfx Password** belirleyin
6. **Submit** butonuna tıklayın

EN İYİ PRATİK

Günlük sertifika imzalama işlemleri için Intermediate CA kullanın, Root CA'yı çevrimdışı ve güvenli bir yerde saklayın.

3. Self-Signed Sertifika Oluşturma

Kendi kendine imzalı sertifikalar, hızlı test ve geliştirme ortamları için idealdir.

NE ZAMAN KULLANILIR?

- Development ve test ortamları için
- İç ağdaki uygulamalar için
- Proof-of-concept çalışmaları için
- Hızlı prototipleme için

Adımlar

1. **Certificate Type** alanından `Self-Signed` seçin
2. **Temel bilgileri** doldurun:

- **Common Name:** `dev.example.com` veya `*.dev.example.com` (wildcard)
- **Subject Alternative Names:** `DNS:dev.example.com,DNS:*.dev.example.com`

3. **Güvenlik parametrelerini** ayarlayın:

- **Lifetime:** 365 gün
- **Key Length:** 2048 bit (test için yeterli)
- **Hash Function:** sha256

4. **Extended Key Usage:** `serverAuth` (web sunucuları için)
5. **Pfx Password** belirleyin
6. **Submit** butonuna tıklayın

DİKKAT

Self-signed sertifikalar tarayıcılar tarafından güvenilmez olarak işaretlenir. Production ortamlarında kullanmayın.

4. Sign With Local CA (Yerel CA ile İmzalama)

SecTrail CM'de mevcut CA'larınızı kullanarak yeni sertifikalar oluşturun.

NE ZAMAN KULLANILIR?

- Production sunucuları için sertifika oluştururken
- Güvenilen CA'nız ile sertifika imzalarken
- Kurumsal standartlara uygun sertifikalar üretirken

Adımlar

1. **Certificate Type** alanından `Sign With Local CA` seçin

2. **İmzalayacak CA'yı seçin:** Sistemde kayıtlı CA'lardan birini seçin
3. **Temel bilgileri** doldurun:

- **Common Name:** `web.example.com`
- **Subject Alternative Names:** İhtiyaç duyulan tüm domain'leri ekleyin

4. **Güvenlik parametrelerini** ayarlayın:

- **Lifetime:** 365 veya 825 gün (public trust gereksinimlerine göre)
- **Key Length:** 2048 bit
- **Hash Function:** sha256

5. **Extended Key Usage:**

- Web sunucuları için: `serverAuth`
- VPN için: `serverAuth,clientAuth`

6. **Pfx Password** belirleyin
7. **Submit** butonuna tıklayın

5. CSR (Certificate Signing Request) Oluşturma

Harici bir CA'dan (Let's Encrypt, DigiCert, GlobalSign vb.) sertifika almak için CSR oluşturun.

> **NE ZAMAN KULLANILIR?**
> - Public sertifika satın alırken
> - Üçüncü parti CA hizmetleri kullanırken
> - Organizasyonunuzun harici CA anlaşması varsa

Adımlar

1. **Certificate Type** alanından `CSR` seçin
2. **Temel bilgileri** dikkatli doldurun:

- **Common Name:** Sertifika talep edeceğiniz domain
- **Organization:** CA tarafından doğrulanacak şirket adı
- **Organizational Unit, Locality, State, Country:** Doğrulama için gerekli
- **E-mail Address:** İletişim e-postası

3. **Güvenlik parametrelerini** ayarlayın:

- **Key Length:** 2048 bit (çoğu CA tarafından kabul edilir)
- **Hash Function:** sha256

4. **Pfx Password** belirleyin (private key koruma için)
5. **Submit** butonuna tıklayın
6. Oluşan **CSR'yi indirin** ve CA'ya gönderin

> **CSR SONRASI ADIMLAR**

1. SecTrail CM'den CSR'yi indirin
2. CA sağlayıcınızın web sitesine gidin
3. CSR'yi yükleyin veya yapıştırın
4. Domain doğrulama sürecini tamamlayın
5. CA'dan imzalı sertifikayı alın
6. Sertifikayı SecTrail CM'e içe aktarın (İçe Aktarma)

6. External CA (Harici CA ile İmzalama)

SecTrail CM'e entegre edilmiş harici CA sistemleri ile doğrudan sertifika imzalayın.

NE ZAMAN KULLANILIR?

- Microsoft ADCS (Active Directory Certificate Services) entegrasyonu varsa
- GlobalSign, DigiCert gibi kurumsal CA anlaşmaları varsa
- Hashicorp Vault PKI kullanıyorsanız
- Otomatik sertifika yönetimi istiyorsanız

Desteklenen Harici CA'lar

SecTrail CM aşağıdaki harici CA entegrasyonlarını destekler:

CA Sağlayıcısı	Açıklama	Kullanım
ADCS	Microsoft Active Directory Certificate Services	Windows ortamları, kurumsal PKI
GlobalSign	GlobalSign HVCA (Managed PKI)	Kurumsal, yüksek hacimli sertifika yönetimi
DigiCert	DigiCert CertCentral API	Public SSL/TLS sertifikaları
Hashicorp Vault	Vault PKI Secrets Engine	Cloud-native, dinamik sertifika yönetimi

ÖN GEREKSİNİM: CA ENTEGRASYONU

Harici CA ile sertifika imzalamadan **önce** ilgili CA entegrasyonunu yapılandırmanız gerekir.

Entegrasyon Kurulumu için:

1. **Settings -> Integrations -> CA Integrations** bölümüne gidin
2. Kullanmak istediğiniz CA'yı seçin (ADCS, GlobalSign, DigiCert, Hashicorp Vault)
3. API bilgilerini ve bağlantı ayarlarını yapılandırın
4. Bağlantıyı test edin

Detaylı kurulum talimatları için Entegrasyonlar sayfasını inceleyin.

ADCS ile İmzalama Adımları

1. **Certificate Type:** `External CA` seçin
2. **External CA Dropdown'dan:** `ADCS` seçin

3. **ADCS Yapılandırması:**

- **CA Server:** ADCS sunucu adresi
- **Certificate Template:** Kullanılacak template adı
- **Credentials:** Yetki bilgileri

4. **Sertifika bilgilerini** doldurun (Common Name, SAN, vb.)
5. **Submit** butonuna tıklayın

GlobalSign ile İmzalama Adımları

1. **Certificate Type:** `External CA` seçin
2. **External CA Dropdown'dan:** `GlobalSign` seçin
3. **GlobalSign Yapılandırması:**

- **API Key:** GlobalSign HVCA API key
- **API Secret:** API secret key
- **Profile:** Sertifika profili

4. **Sertifika bilgilerini** doldurun
5. **Submit** butonuna tıklayın

DigiCert ile İmzalama Adımları

1. **Certificate Type:** `External CA` seçin
2. **External CA Dropdown'dan:** `DigiCert` seçin
3. **DigiCert Yapılandırması:**

- **API Key:** DigiCert CertCentral API key
- **Organization ID:** DigiCert'teki org ID
- **Certificate Type:** OV, EV, DV seçimi

4. **Sertifika bilgilerini** doldurun
5. **Submit** butonuna tıklayın

Hashicorp Vault ile İmzalama Adımları

1. **Certificate Type:** `External CA` seçin
2. **External CA Dropdown'dan:** `Hashicorp Vault` seçin
3. **Vault Yapılandırması:**

- **Vault Address:** Vault sunucu adresi
- **PKI Path:** PKI secrets engine path
- **Token:** Vault authentication token
- **Role:** Vault PKI role adı

4. **Sertifika bilgilerini** doldurun
5. **Submit** butonuna tıklayın

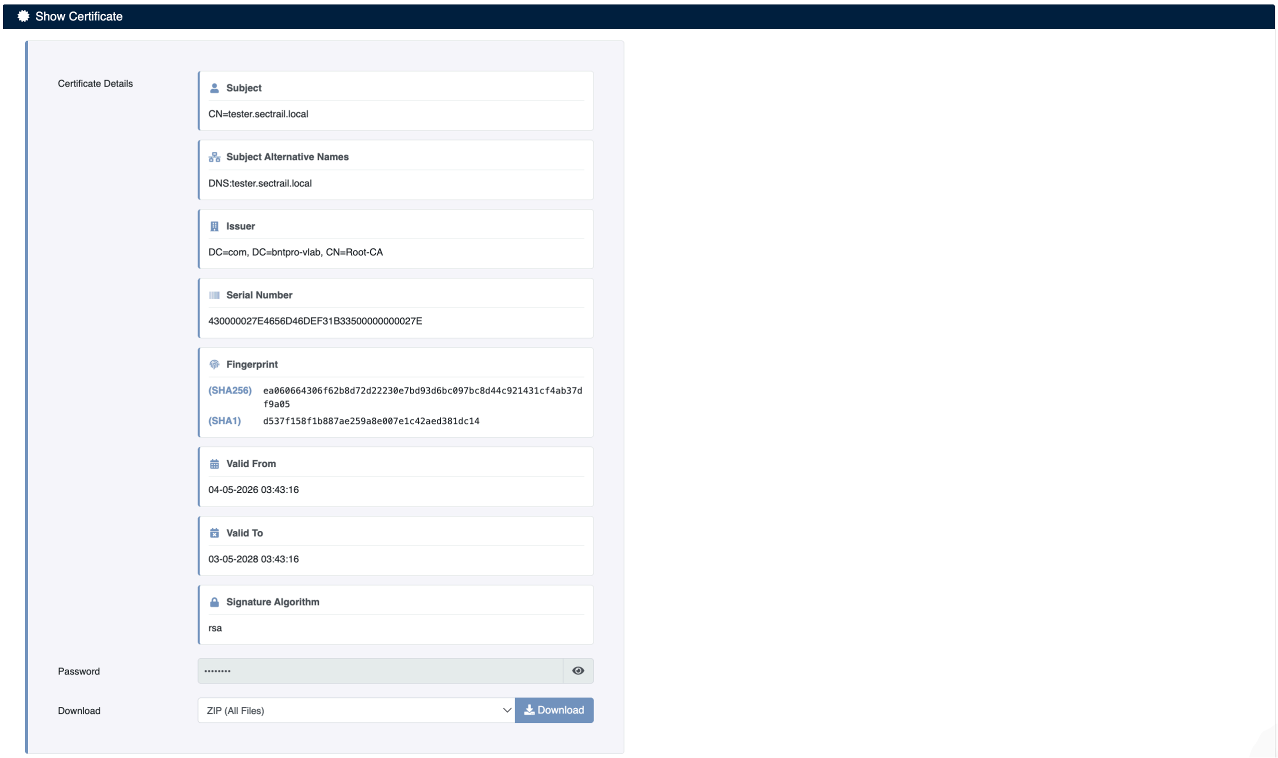
Sertifika Oluşturma Sonrası İşlemler

Sertifika başarıyla oluşturulduktan sonra otomatik olarak envantere eklenir ve çeşitli işlemler yapabilirsiniz.

> **OTOMATİK ENVANTER KAYDI**
>
> Oluşturduğunuz her sertifika otomatik olarak **Inventory -> Certificate Store -> Certificates & Keys** sayfasındaki envanter listesine eklenir. Buradan tüm sertifikalarınızı görüntüleyebilir, yönetebilir ve takip edebilirsiniz. Envanter listesi hakkında detaylı bilgi için Envanter Yönetimi sayfasını inceleyin.

Sertifika Görüntüleme ve İndirme

Sertifika oluşturulduktan hemen sonra **Show Certificate** ekranı açılır ve sertifika bilgilerini görüntüleyebilirsiniz:



Sertifika Detayları ve İndirme Seçenekleri

Görüntülenen Bilgiler

Alan	Açıklama
Name	Sertifikanın Common Name (CN) değeri (örn: `sectrail.local`)
Certificate	Sertifikanın PEM formatındaki tam içeriği (`-----BEGIN CERTIFICATE-----` ile başlar)
Password	Sertifika private key parolası (güvenlik için gizli gösterilir, göz ikonuna tıklayarak görüntülenebilir)

Sertifikayı İndirme

Sertifika oluşturulduktan sonra ekranda bulunan indirme butonları ile farklı formatlarda indirebilirsiniz:

- **Download Zip -** Tüm dosyaları (cert, key, chain, pfx, der, jks, bundle) içeren arşiv
- **Download Pfx -** Windows IIS ve Exchange için PFX/P12 formatı

- **Download Jks** - Java/Tomcat için Java KeyStore formatı
- **Download Crt** - Sadece sertifika dosyası (public key)
- **Download Chain** - CA zinciri dosyaları
- **Download Bundle** - Tam sertifika zinciri (cert + intermediate + root)
- **Download Key** - Sadece private key

> **ÖNEMLİ NOT**
>
> İndirilen sertifikaları kullanmak için belirlediğiniz **Pfx Password** değerine ihtiyacınız olacaktır.

Envanter Listesinden Erişim

Sertifika oluşturulduktan sonra **Inventory -> Certificate Store -> Certificates & Keys** sayfasından da erişebilir ve yönetebilirsiniz. Liste üzerinde sertifikalarınızı görüntüleyebilir, filtreleyebilir ve çeşitli işlemler yapabilirsiniz.

CSR İmzalama

Bu kılavuz, SecTrail CM üzerinden CSR (Certificate Signing Request) imzalama işlemlerini adım adım anlatır. CSR'leri yerel CA veya harici CA entegrasyonları ile imzalayabilirsiniz.

> **ÖZELLİK HAKKINDA**
>
> CSR imzalama özelliği, private key'i paylaşmadan sertifika almanızı sağlar. Kendi uygulamanızda oluşturduğunuz CSR'yi SecTrail CM'e yükleyerek veya SecTrail CM üzerinden CSR oluşturarak imzalama işlemini gerçekleştirebilirsiniz.

CSR İmzalama Senaryoları

SecTrail CM, iki farklı CSR imzalama senaryosunu destekler:

1. Harici CSR İmzalama (Önerilen)

Private key'i paylaşmak istemediğiniz durumlarda kullanılır:

1. **Kendi sunucunuzda/uygulamanızda CSR oluşturun** (private key sunucunuzda kalır)
2. **CSR'yi SecTrail CM'e import edin**
3. **SecTrail CM üzerinden CSR'yi imzalayın**
4. **İmzalı sertifikayı indirip sunucunuza kurun**

> **GÜVENLİK AVANTAJI**
>
> Bu yöntemde private key asla paylaşılmaz ve sadece kendi sunucunuzda kalır. En güvenli yöntemdir.

2. SecTrail CM Üzerinde CSR Oluşturma

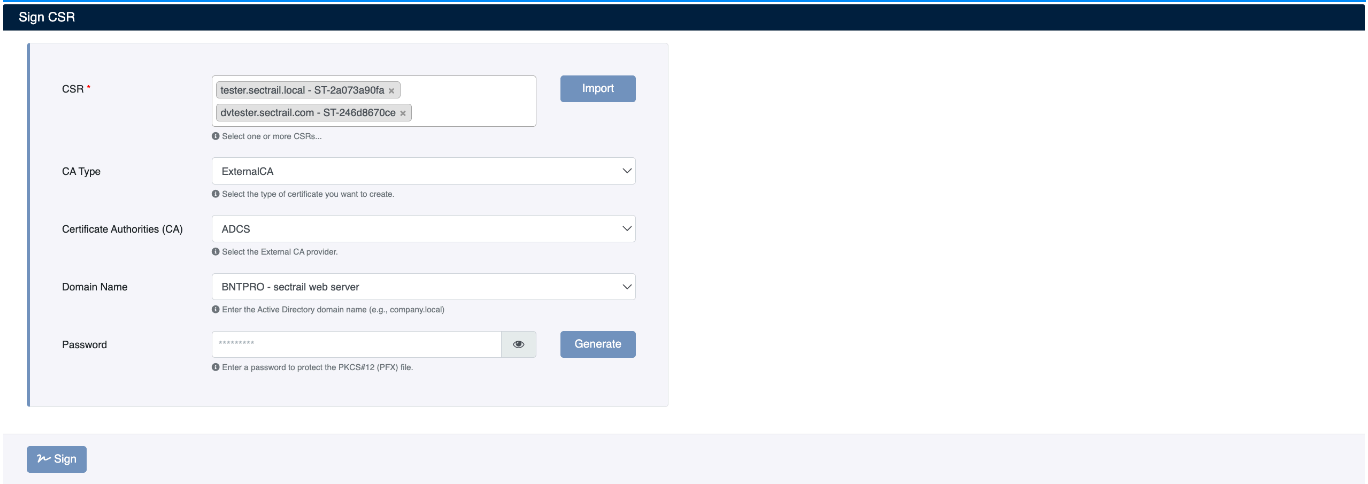
Merkezi yönetim için kullanılır:

1. **SecTrail CM üzerinden CSR oluşturun**
2. **Oluşan CSR'yi hemen imzalayın**
3. **Sertifika ve private key'i birlikte indirin**

CSR İmzalama Ekranı

CSR imzalama işlemi için SecTrail CM'de özel bir arayüz bulunur.

> **ERİŞİM YOLU**
>
> CSR imzalamak için: **Inventory -> Issue Certificate -> Sign CSR** menüsüne gidin.



CSR İmzalama Formu

CSR İmzalama Parametreleri

Temel Bilgiler

Alan	Açıklama	Örnek
CSR	İmzalanacak CSR seçimi	Dropdown'dan mevcut CSR'yi seçin
CA Type	İmzalama tipi	Local CA, External CA
External CA	Harici CA seçimi (CA Type: External CA ise)	ADCS, GlobalSign, DigiCert, Hashicorp Vault
Domain Name	Sertifika alan adı (opsiyonel)	Tanımlayıcı isim
Password	Sertifika private key parolası	Güçlü parola

> **CSR SEÇİMİ**
>
> CSR dropdown'ında SecTrail CM envanterindeki tüm CSR'ler listelenir. Format: `[Organization] - [Identifier]` (örn: `bntpro.com - ST-5cc54e0593`)

CA Type Seçenekleri

1. Local CA (Yerel CA)

SecTrail CM'deki mevcut CA'larınız ile CSR imzalama:

Kullanım Senaryoları:

- Internal/kurumsal sertifikalar için
- Test ve development ortamları için
- Kendi PKI altyapınızla yönetilen sertifikalar için

Avantajları:

- Hızlı imzalama

- Tam kontrol
- Ek maliyet yok
- Offline çalışabilir

2. External CA (Harici CA)

ADCS, GlobalSign, DigiCert, Hashicorp Vault gibi entegre CA'lar ile imzalama:

Kullanım Senaryoları:

- Public sertifikalar için
- Tarayıcı güvenilirliği gereken sertifikalar için
- Compliance gereksinimleri için
- Kurumsal CA entegrasyonları için

Desteklenen External CA'lar:

CA Sağlayıcısı	Açıklama	Kullanım
ADCS	Microsoft Active Directory Certificate Services	Windows ortamları, kurumsal PKI
GlobalSign	GlobalSign HVCA (Managed PKI)	Kurumsal, yüksek hacimli sertifika yönetimi
DigiCert	DigiCert CertCentral API	Public SSL/TLS sertifikaları
Hashicorp Vault	Vault PKI Secrets Engine	Cloud-native, dinamik sertifika yönetimi

ÖN GEREKSİNİM: CA ENTEGRASYONU

External CA kullanmadan **önce** ilgili CA entegrasyonunu yapılandırmanız gerekir.

Detaylı kurulum talimatları için Entegrasyonlar sayfasını inceleyin.

CSR İmzalama Adımları

Yöntem 1: Harici CSR İmzalama (Private Key Paylaşılmaz)

Bu yöntem, private key'i paylaşmadan sertifika almak için kullanılır.

Adım 1: Kendi Sunucunuzda CSR Oluşturma

Önce kendi sunucunuzda/uygulamanızda CSR ve private key oluşturun:

Windows/IIS ile CSR Oluşturma:

1. IIS Manager -> Server Certificates
2. Create Certificate Request
3. Distinguished Name bilgilerini doldurun
4. Cryptographic Service Provider: Microsoft RSA SChannel, 2048 bit
5. CSR dosyasını kaydedin

Adım 2: CSR'yi SecTrail CM'e Import Etme

1. **Inventory -> Import Certificate** menüsüne gidin
2. **Certificate Type** olarak `CSR` seçin
3. CSR dosyanızı yükleyin veya içeriğini yapıştırın
4. **Import** butonuna tıklayın

CSR başarıyla import edildikten sonra envantere eklenir ve bir identifier atanır (örn: `ST-5cc54e0593`).

Adım 3: CSR'yi İmzalama

1. **Inventory -> Issue Certificate -> Sign CSR** menüsüne gidin
2. **CSR Seçimi:**

- Dropdown'dan import ettiğiniz CSR'yi seçin
- Format: `[Organization] - [Identifier]`

3. **CA Type Seçimi:**

- **Local CA:** SecTrail CM'deki CA ile imzalama
- **External CA:** Harici CA ile imzalama

4. **External CA Seçimi** (External CA seçildi ise):

- ADCS, GlobalSign, DigiCert veya Hashicorp Vault

5. **Domain Name** (Opsiyonel):

- Tanımlayıcı bir isim girin (örn: `bntpro.local - copy of sectrail webserver`)

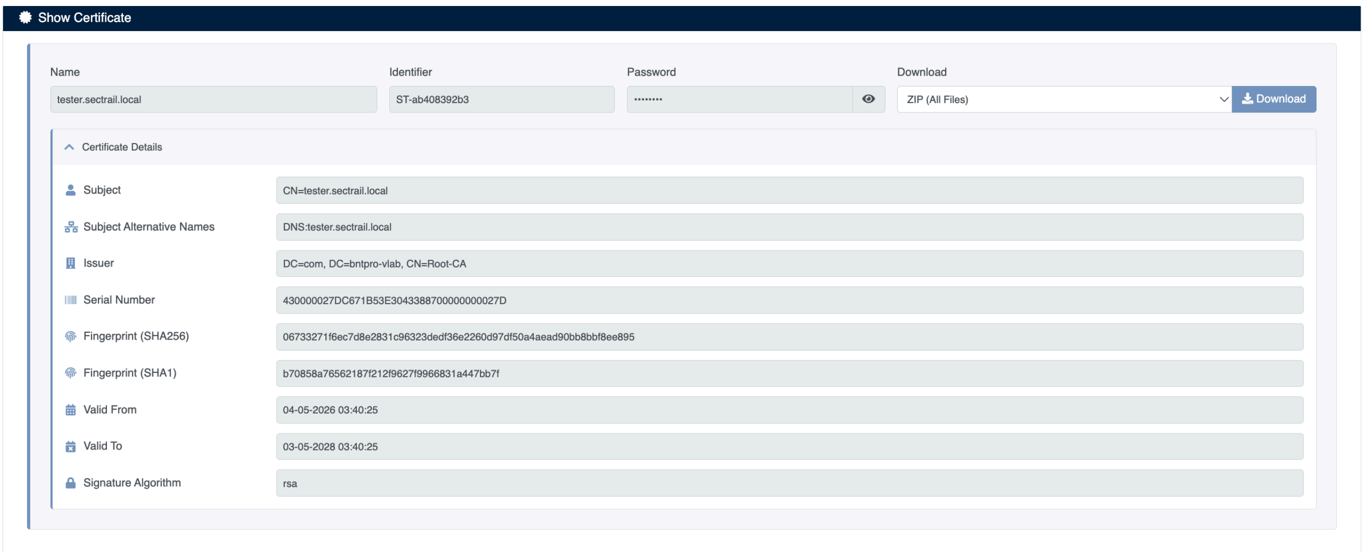
6. **Password:**

- Sertifika için güçlü bir parola belirleyin
- Generate butonu ile otomatik parola oluşturabilirsiniz

7. **Sign** butonuna tıklayın

Adım 4: İmzalı Sertifikayı İndirme

İmzalama tamamlandıktan sonra **Show Key** ekranı açılır:



İmzalı Sertifika ve İndirme Seçenekleri

İndirme Butonları:

- **Download Zip** - Tüm dosyalar (cert, chain, bundle)
- **Download Jks** - Java KeyStore formatı
- **Download Crt** - Sadece sertifika dosyası
- **Download Chain** - CA zinciri
- **Download Bundle** - Tam sertifika zinciri
- **Download Key** - Private key (sadece SecTrail CM'de oluşturulan CSR'ler için)

> **ÖNEMLİ**
>
> Harici CSR'ler için **Download Key** butonu **çalışmaz** çünkü private key SecTrail CM'de değil, kendi sunucunuzdadır. Bu güvenlik özelliğidir.

Yöntem 2: SecTrail CM Üzerinde CSR Oluşturma

Bu yöntem merkezi yönetim için uygundur ancak private key de SecTrail CM'de oluşturulur.

Adım 1: CSR Oluşturma

1. **Inventory -> Create Certificate** menüsüne gidin
2. **Certificate Type** olarak `CSR` seçin
3. Sertifika bilgilerini doldurun:

- Common Name, Organization, Country vb.

4. **Key Length:** 2048 veya 4096 bit
5. **Pfx Password** belirleyin
6. **Submit** butonuna tıklayın

CSR ve private key oluşturulur ve envantere eklenir.

Adım 2: CSR'yi İmzalama

Yukarıdaki **Adım 3: CSR'yi İmzalama** bölümündeki adımları izleyin.

Adım 3: Sertifika ve Private Key'i İndirme

Bu senaryoda private key de SecTrail CM'de olduğundan **Download Key** butonu çalışır ve tüm dosyaları indirebilirsiniz.

Domain Name Alanı

Domain Name alanı opsiyoneldir ve tanımlayıcı amaçlı kullanılır:

```
Örnek: bntpro.local - copy of sectrail webserver
```

Bu alan:

- Sertifikayı envanterde tanımlamaya yardımcı olur
- Birden fazla benzer sertifikayı ayırt etmek için kullanılır

- Raporlarda ve loglamalarda görünür

Password Oluşturma

Password alanı için:

1. **Manuel Girdi:** Kendi parolanızı yazın
2. **Otomatik Oluşturma:** `GENERATE` butonuna tıklayın

- Güçlü, rastgele parola oluşturur
- Minimum 16 karakter
- Büyük/küçük harf, rakam ve özel karakterler içerir

3. **Görüntüleme:** Göz ikonu ile parolayı görebilirsiniz

> **PAROLA GÜVENLİĞİ**
>
> Parolayı güvenli bir password manager'da saklayın ve her sertifika için farklı parola kullanın.

Sertifika Template Yönetimi

Bu kılavuz, SecTrail CM üzerinde sertifika şablonlarının nasıl oluşturulacağını ve yönetileceğini anlatır. Sertifika template'leri, organizasyon bilgileri, anahtar algoritması ve diğer parametreleri önceden tanımlayarak sertifika oluşturma işlemini hızlandırır ve standartlaştırır.

ÖZELLİK HAKKINDA

Template kullanarak her seferinde aynı bilgileri (Organization, OU, Country vb.) tekrar tekrar girmek yerine, hazır şablonlardan sertifika oluşturabilirsiniz. Bu sayede hem zaman tasarrufu sağlar hem de kurumsal standartlara uyumluluğu garanti edersiniz.

Template Nedir?

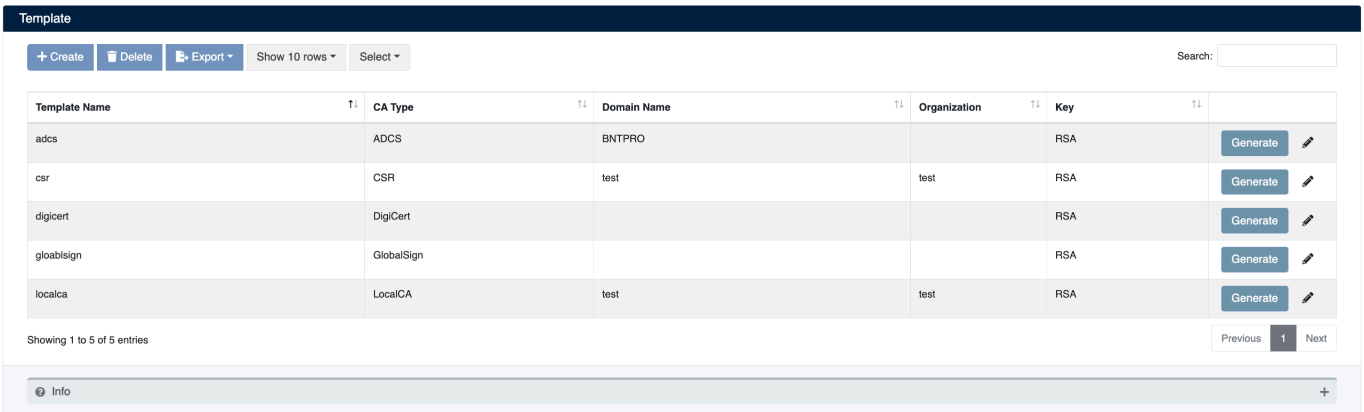
Template (Şablon), sertifika oluşturma parametrelerini önceden tanımlanmış bir yapıdır. Template kullanarak:

- **Hızlı sertifika üretimi:** Sadece Common Name ve SAN alanlarını doldurun, diğer tüm alanlar otomatik doldurulur
- **Standartlaşma:** Tüm sertifikaların aynı organizasyon bilgileri ve güvenlik parametreleri ile oluşturulmasını sağlayın
- **Hata azaltma:** Manuel giriş hatalarını önleyin
- **CA Entegrasyonu:** ADCS, GlobalSign, DigiCert gibi harici CA'lar ile entegre çalışın

Template Listesi

ERİŞİM YOLU

Template yönetimi için: **Inventory -> Issue Certificate -> Templates** menüsüne gidin.



Template Listesi ve İşlemler

Template listesinde mevcut tüm şablonlarınızı görüntüleyebilir ve yönetebilirsiniz.

Liste Kolonları

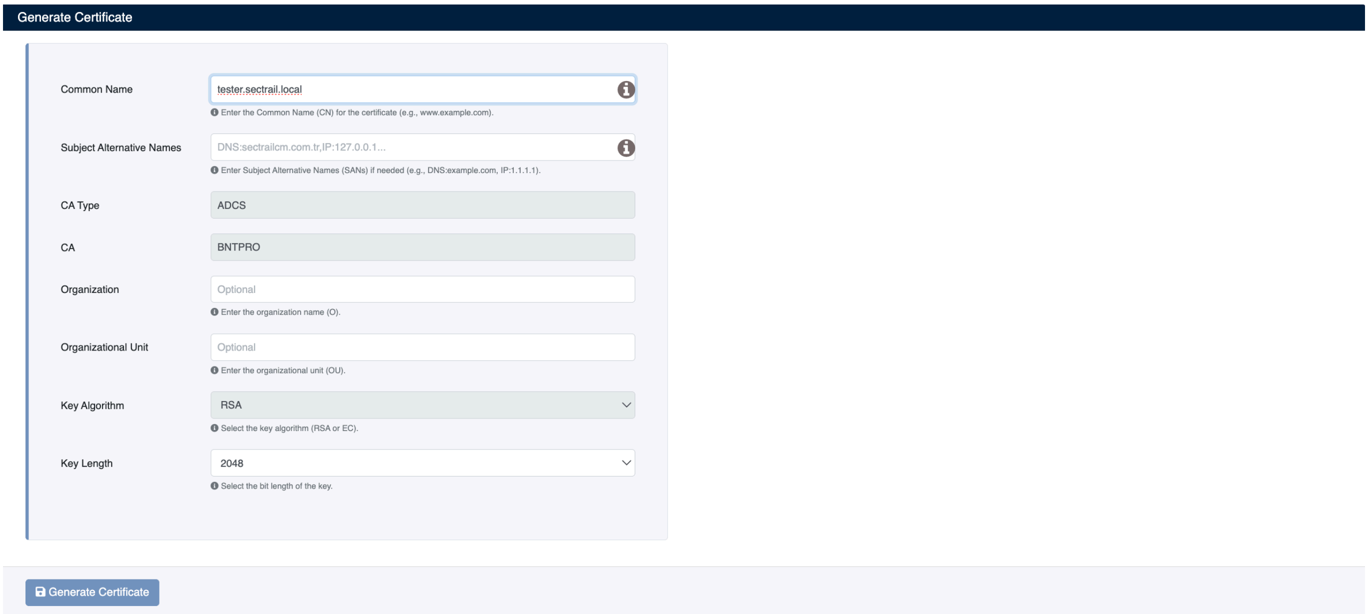
Kolon	Açıklama
Template Name	Şablonun benzersiz adı (örn: `acme` , `adcs` , `csr`)
CA Type	Sertifika otoritesi tipi (ACME, ADCS, CSR, DigiCert, GlobalSign, Hashicorp, LocalCA)
Domain Name	Şablonun bağlı olduğu domain/organizasyon domain'i
Organization	Organizasyon adı
E-mail	İletişim e-posta adresi
Key	Anahtar algoritması (RSA, ECDSA)
Actions	İşlem butonları (Generate, Edit, Delete)

Template İşlemleri

Her template için üç temel işlem yapabilirsiniz:

1. Generate (Sertifika Oluştur)

Generate butonuna tıkladığınızda, template parametreleri önceden doldurulmuş halde sertifika oluşturma ekranı açılır. Sadece Common Name ve Subject Alternative Names (SAN) alanlarını doldurmanız yeterlidir.



Template ile Sertifika Oluşturma

Template ile sertifika oluştururken:

1. Template listesinden istediğiniz şablonun **Generate** butonuna tıklayın
2. Açılan formda otomatik doldurulan alanları kontrol edin:

- CA Type, Organization, OU, Locality, State, Country
- Key Algorithm, Key Length, Hash Function
- Lifetime, E-mail Address

3. **Common Name** alanını doldurun (örn: `test.sectrail.local`)
4. **Subject Alternative Names** alanına ek domain veya IP ekleyin (opsiyonel)
5. **Generate** butonuna tıklayın

> **ZAMAN TASARRUFU**
>
> Template kullanarak sadece 2 alan (Common Name ve SAN) doldurarak anında sertifika oluşturabilirsiniz. Normal sertifika oluşturma işleminde 15+ alan doldurmanız gerekir.

2. Edit (Düzenle)

Mevcut template'i düzenlemek için **Edit** butonuna tıklayın. Template parametrelerini güncelleyebilirsiniz.

3. Delete (Sil)

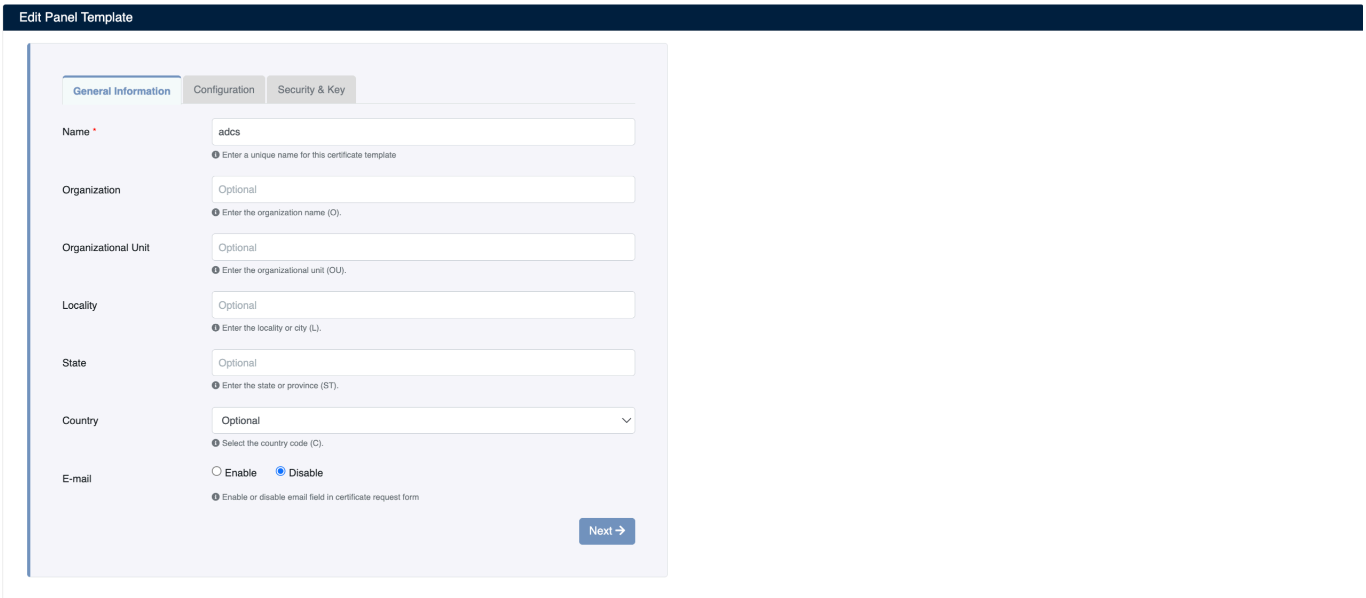
Template'i sistemden tamamen kaldırmak için **Delete** butonuna tıklayın.

> **DİKKAT**
>
> Template silindiğinde, bu template ile daha önce oluşturulmuş sertifikalar etkilenmez. Sadece gelecekteki sertifika oluşturma işlemlerinde bu template kullanılamaz.

Yeni Template Oluşturma

Yeni bir sertifika şablonu oluşturmak için **Create** butonuna tıklayın. Form üç sekme halinde sunulur.

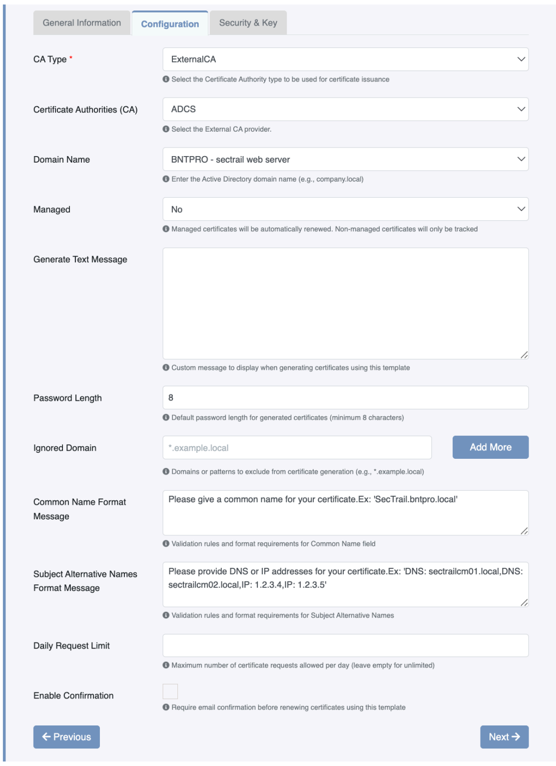
Sekme 1: General Information



- **Name**: Template'in benzersiz adı (örn. `adcs`, `prod-ssl`)
- **Organization**: Organizasyon adı (O)
- **Organizational Unit**: Departman veya birim (OU)
- **Locality**: Şehir (L)
- **State**: Eyalet veya il (ST)

- **Country**: Ülke kodu (dropdown'dan seçim)
- **E-mail**: Sertifika oluşturma formunda e-posta alanı gösterilsin mi? (`Enable` / `Disable`)

Sekme 2: Configuration

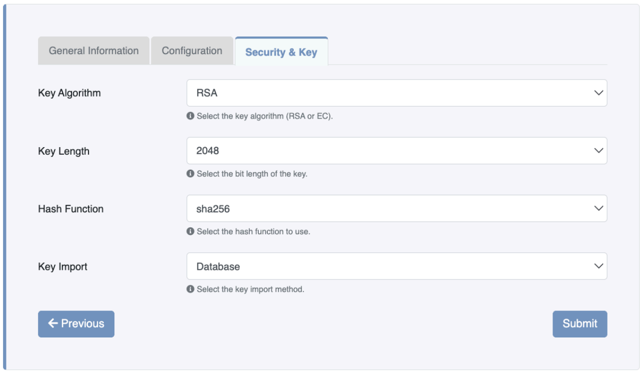


- **CA Type**: Sertifika otoritesi tipi (ExternalCA, LocalCA vb.)
- **Certificate Authorities (CA)**: Kullanılacak harici CA sağlayıcısı (örn. `ADCS`)
- **Domain Name**: Active Directory domain adı (örn. `company.local`)
- **Managed**: Sertifikalar otomatik yönetilsin mi? (`Yes` / `No`)

> **MANAGED (YÖNETİLEN) SERTİFİKALAR**
>
> **Managed** seçeneğini `Yes` yaparsanız sertifikalar otomatik olarak izlenir, yenileme alarmları iletilir. Detaylar için: Yönetilen Sertifikalar

- **Generate Text Message**: Sertifika oluşturulduğunda gösterilecek özel mesaj
- **Password Length**: Otomatik oluşturulacak parola uzunluğu (karakter)
- **Ignored Domain**: Sertifika oluşturması engellenecek domain'ler (örn. `*.example.local`)
- **Common Name Format Message**: Common Name formatı için kullanıcıya gösterilecek yönlendirme mesajı
- **Subject Alternative Names Format Message**: SAN formatı için yönlendirme mesajı
- **Daily Request Limit**: Günlük maksimum sertifika talep sayısı
- **Enable Confirmation**: Sertifika oluşturmadan önce onay alınsın mı?

Sekme 3: Security & Key



- **Key Algorithm**: Anahtar algoritması (`RSA` veya `EC`)
- **Key Length**: Anahtar bit uzunluğu (örn. `2048`)
- **Hash Function**: Hash algoritması (örn. `sha256`)
- **Key Import**: Private key'in saklanacağı yer (`Database` , `Key` , `HSM` , `BeyondTrust`)

Template Tipleri

SecTrail CM farklı kullanım senaryoları için çeşitli CA tiplerini destekler:

1. LocalCA Template

Kendi yerel Certificate Authority'niz ile sertifika imzalamak için kullanılır.

Ne Zaman Kullanılır:

- İç ağ uygulamaları için
- Kurumsal standartlara uygun sertifikalar üretirken
- SecTrail CM'de oluşturduğunuz Root/Intermediate CA'lar ile imzalama

Örnek Yapılandırma:

- **Name:** `localca`
- **CA Type:** `LocalCA`
- **Organization:** `secrusen`
- **Key Algorithm:** RSA
- **Key Length:** 2048
- **Lifetime:** 365 gün

2. ADCS Template

Microsoft Active Directory Certificate Services entegrasyonu ile sertifika oluşturur.

Ne Zaman Kullanılır:

- Windows ortamlarında
- Active Directory entegrasyonu olan kurumsal PKI'da
- Otomatik domain doğrulaması gerektiğinde

Örnek Yapılandırma:

- **Name:** `adcs`
- **CA Type:** `ADCS`
- **Organization:** `bntpro`
- **Domain Name:** `bntpro.local`
- **Key Algorithm:** RSA
- **Key Length:** 2048

3. CSR Template

Certificate Signing Request oluşturmak için kullanılır. Harici CA'lardan sertifika almak istediğinizde kullanılır.

Ne Zaman Kullanılır:

- Harici bir CA'dan (Let's Encrypt, DigiCert vb.) sertifika alırken
- Public SSL/TLS sertifikaları için
- Üçüncü parti doğrulama gerektiğinde

Örnek Yapılandırma:

- **Name:** `csr`
- **CA Type:** `CSR`
- **Organization:** `sectrail`

4. ACME Template

ACME protokolü (Let's Encrypt, ZeroSSL vb.) ile otomatik sertifika oluşturur.

Ne Zaman Kullanılır:

- Let's Encrypt ile ücretsiz SSL sertifikaları için
- Otomatik yenileme istediğinizde
- Public domain'ler için

Örnek Yapılandırma:

- **Name:** `acme`
- **CA Type:** `ACME`
- **Organization:** `bntpro`
- **Managed:** Yes (otomatik yenileme için)
- **Lifetime:** 90 gün (Let's Encrypt standardı)

5. DigiCert Template

DigiCert CertCentral API entegrasyonu ile sertifika oluşturur.

Ne Zaman Kullanılır:

- DigiCert müşterisiyseniz
- OV (Organization Validated) veya EV (Extended Validation) sertifikalar için

- Kurumsal SSL sertifikaları için

6. GlobalSign Template

GlobalSign HVCA (Managed PKI) entegrasyonu ile sertifika oluşturur.

Ne Zaman Kullanılır:

- GlobalSign anlaşmanız varsa
- Yüksek hacimli sertifika yönetimi için
- Managed PKI hizmeti kullanıyorsanız

7. Hashicorp Vault Template

Hashicorp Vault PKI Secrets Engine ile dinamik sertifika oluşturur.

Ne Zaman Kullanılır:

- Cloud-native ortamlarda
- Kubernetes, microservices mimarilerinde
- Dinamik, kısa ömürlü sertifikalar için

Sistem Entegrasyonları

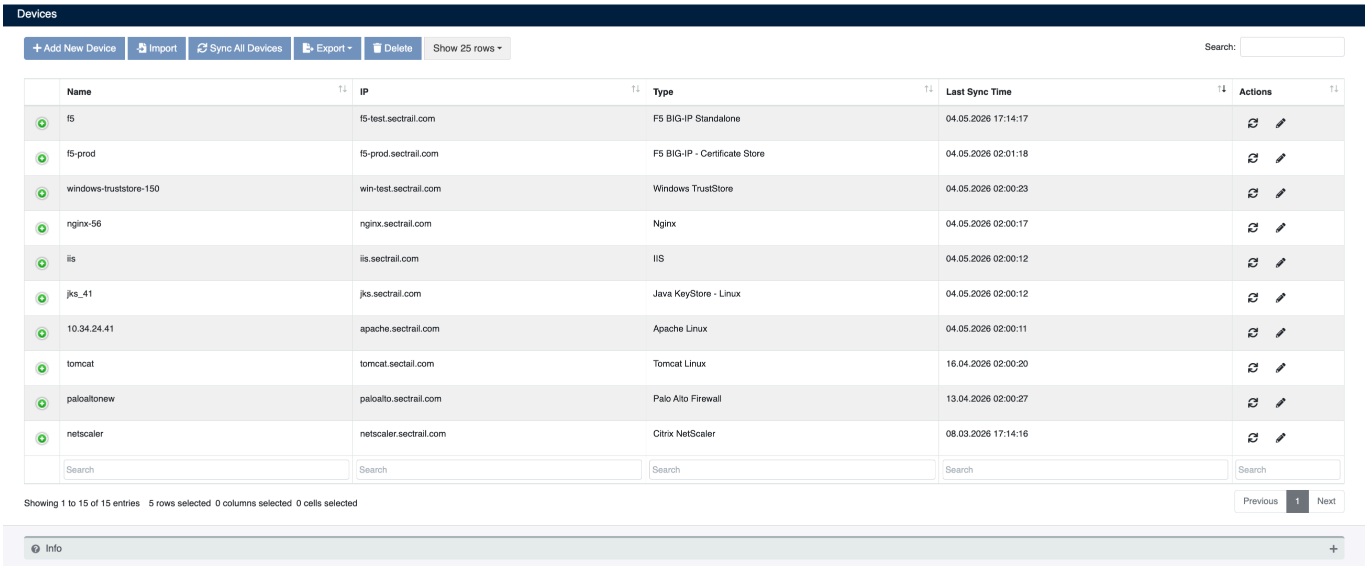
SecTrail CM üzerinden entegre etmek istediğiniz sistem uygulamalarının yapılandırmalarını ve dağıtım işlemlerini bu bölümden yönetebilirsiniz. Desteklenen sistemler:

- 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

> **ENTEGRASYON YAPILANDIRMALARI**
>
> Tüm sistem entegrasyonları için genel yapılandırma adımlarına Entegrasyonlar -> Sistem sayfasından ulaşabilirsiniz.

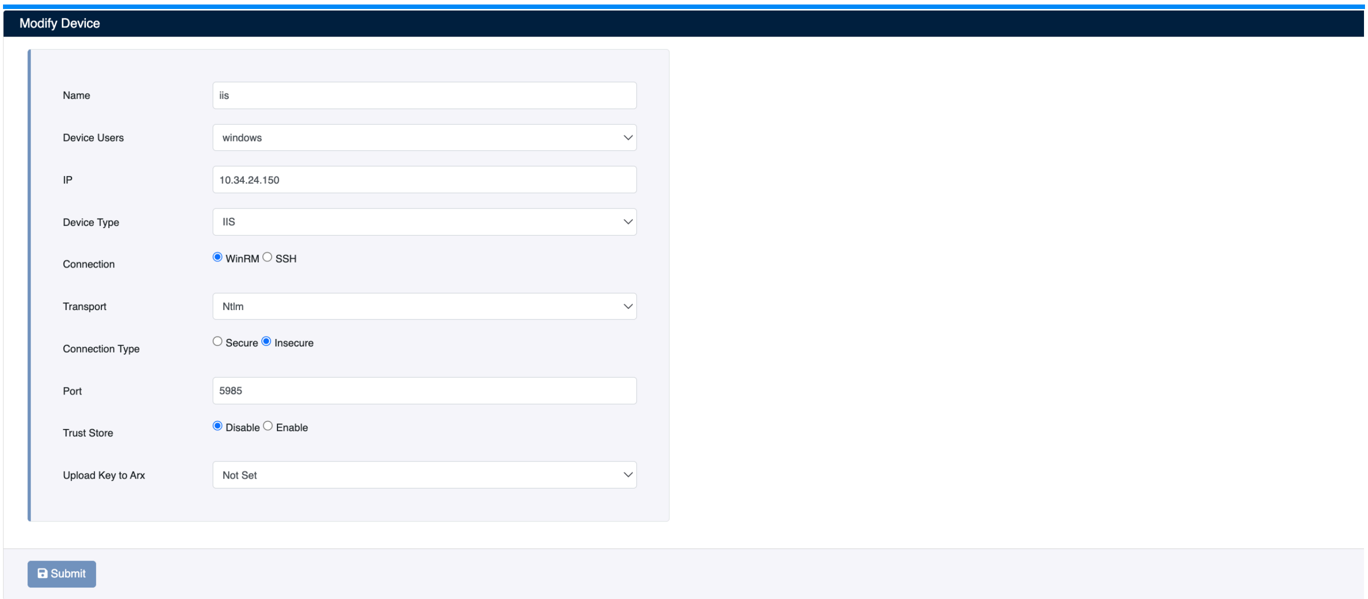
Sistemler

Entegre etmek istediğiniz sistem uygulamalarının yapılandırmaları **Automation -> Devices** sayfasında listelenir.



Tanımlı Cihaz Listesi

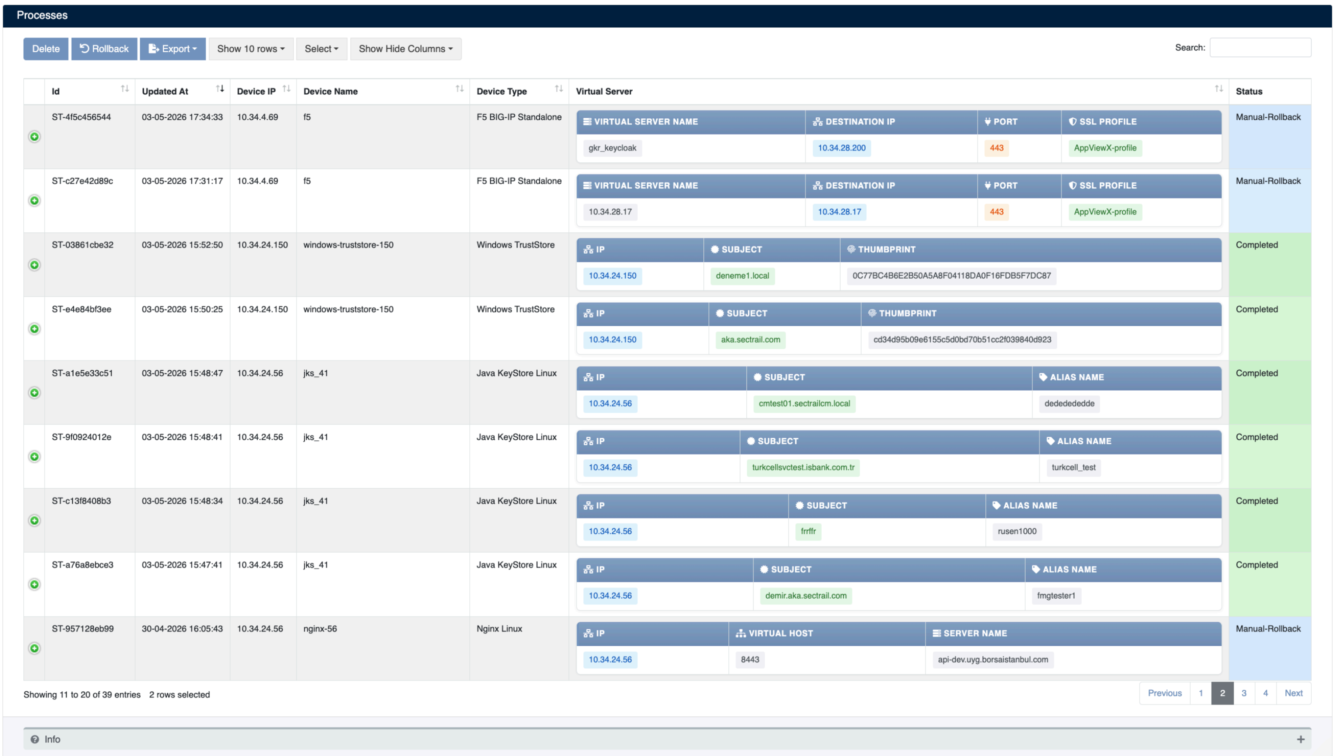
Create butonuna tıklayarak yeni bir cihaz yapılandırması ekleyebilirsiniz.



Yeni Cihaz Yapılandırma Formu

İşlem Geçmişi

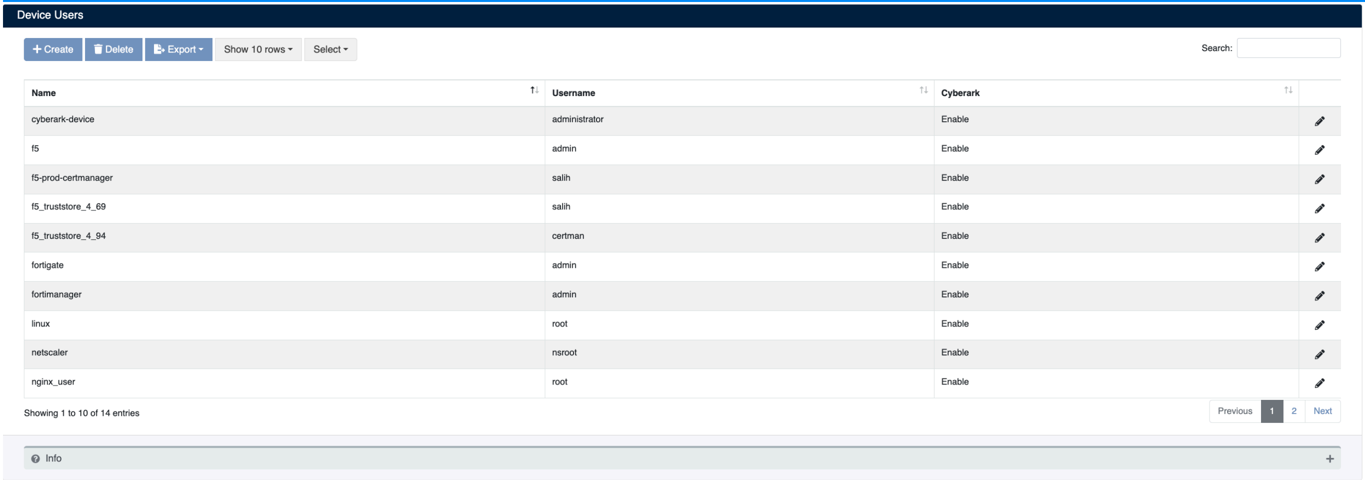
Automation -> Process alanından cihazlar üzerinde gerçekleştirilen tüm işlemler (sertifika yükleme, deployment vb.) detaylı biçimde görüntülenebilir.



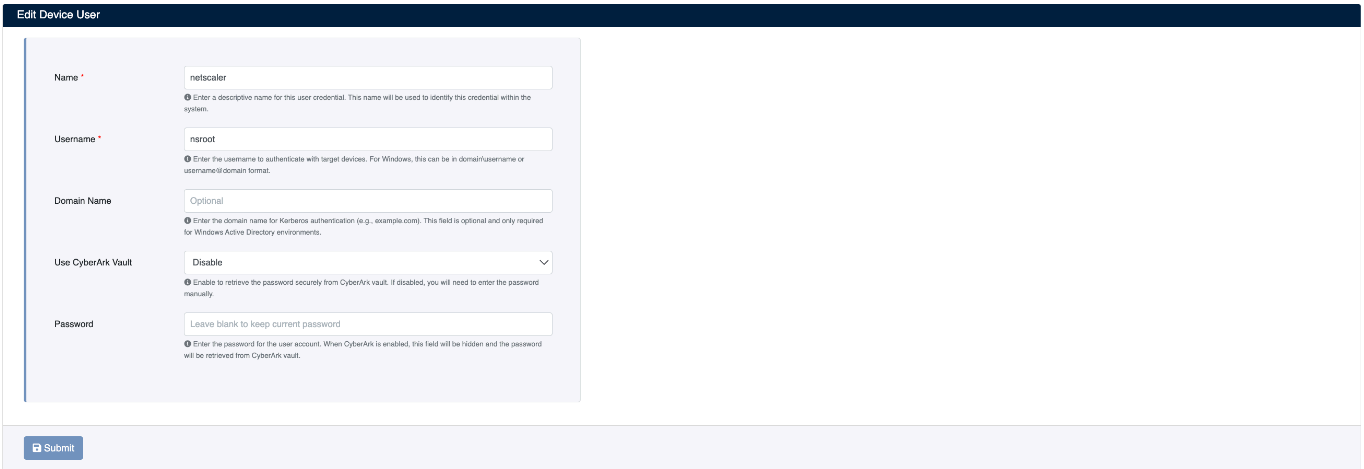
İşlem Geçmişi - Tüm Cihaz İşlemleri

Sistem Kullanıcıları

Automation -> Device Users alanından cihaz bağlantılarında kullanılacak kullanıcı tanımlamaları oluşturabilirsiniz.



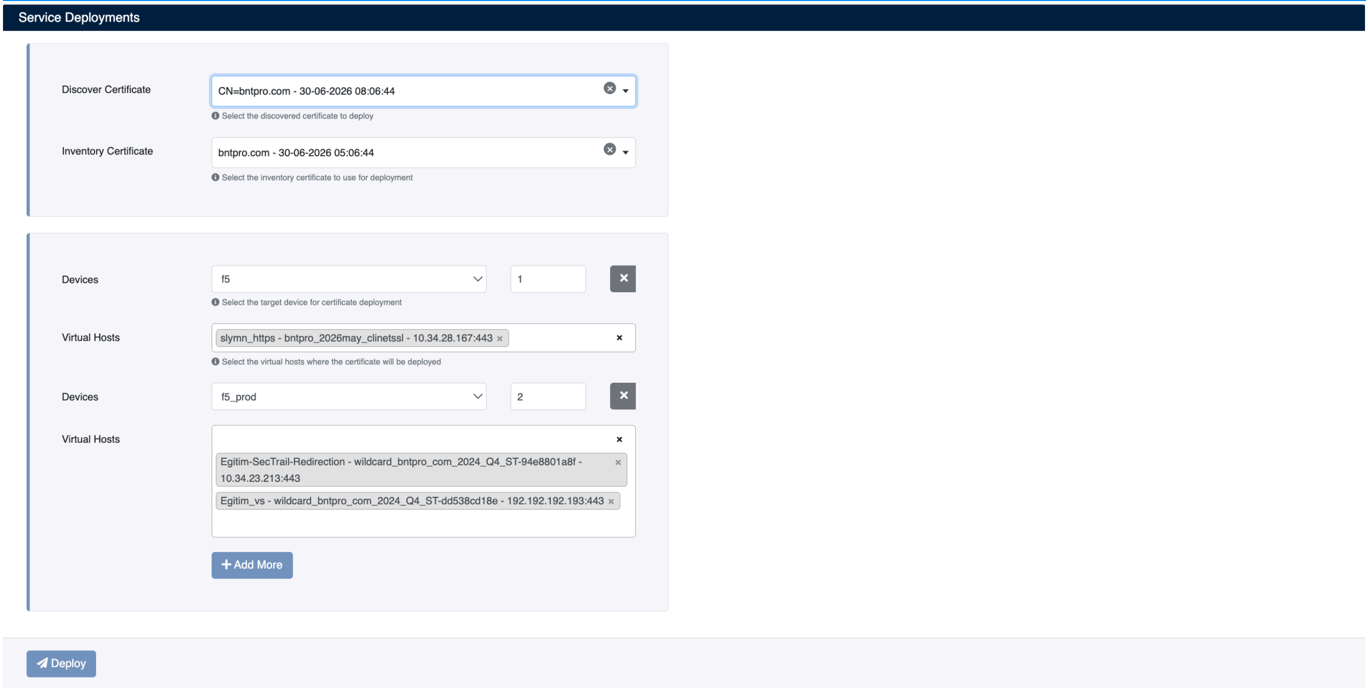
Cihaz Kullanıcıları Listesi



Yeni Cihaz Kullanıcısı Oluşturma

Anlık Servis Dağıtımı

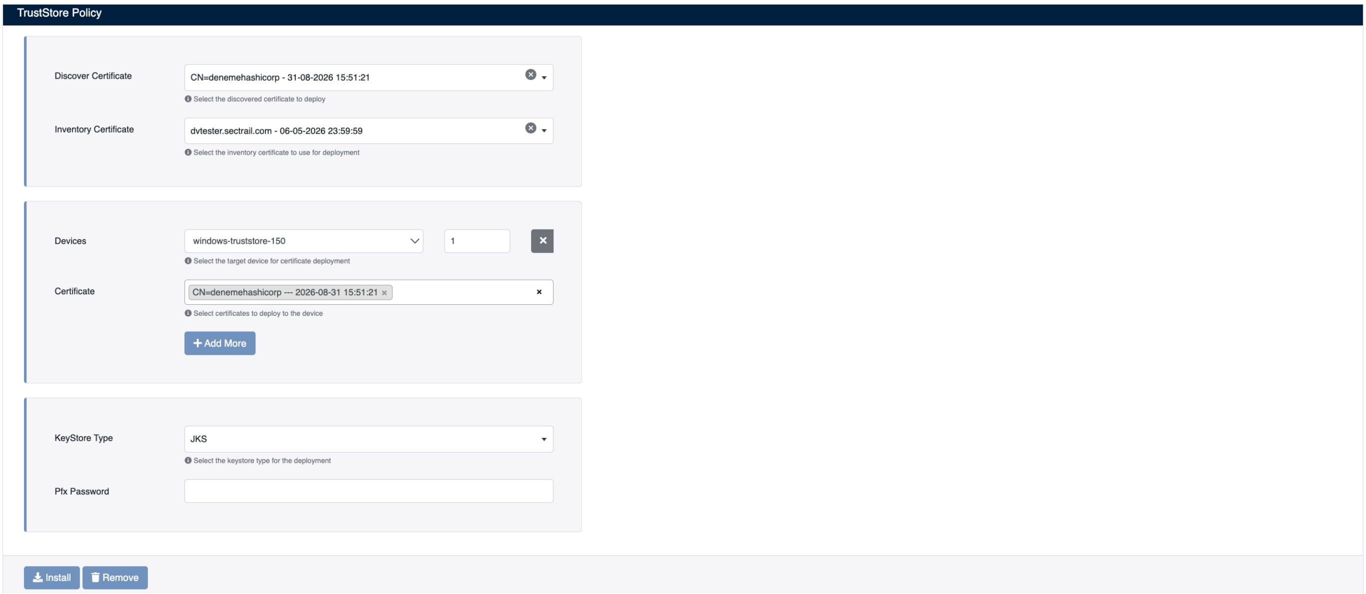
Automation -> Deployments -> Service Deployments sayfasından seçili cihazlara anlık sertifika yükleme işlemi başlatabilirsiniz.



Anlık Servis Sertifika Dağıtımı

Anlık TrustStore Dağıtımı

Automation -> Deployments -> TrustStore Deployments sayfasından seçili cihazlara anlık TrustStore deployment işlemi başlatabilirsiniz.



Anlık TrustStore Dağıtımı

İş Akışı Yönetimi

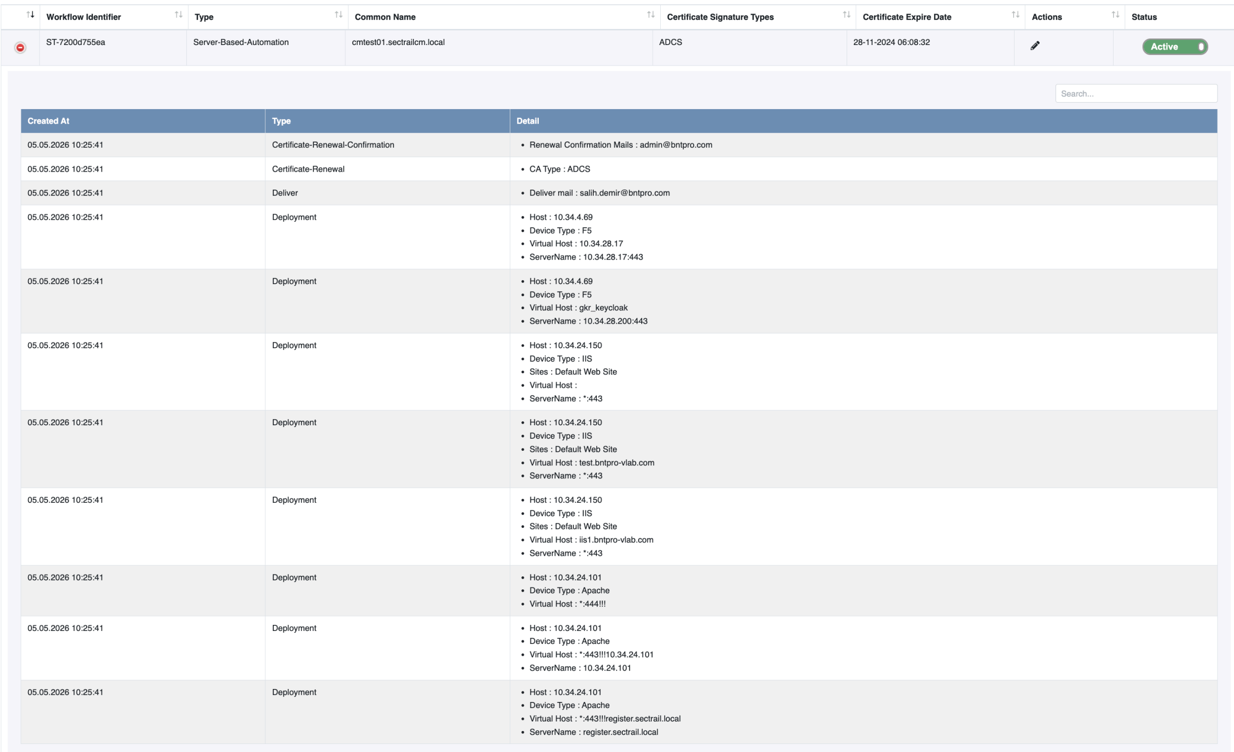
Bu kılavuz, SecTrail CM'de sertifika yaşam döngüsü otomasyon kurallarının nasıl yapılandırılacağını, iş akışlarının nasıl oluşturulacağını ve yönetileceğini adım adım anlatır.

> **ÖZELLİK HAKKINDA**
>
> İş akışı (Workflow) yönetimi, sertifika yenileme, dağıtım ve bildirim süreçlerini otomatikleştirmenizi sağlar. Sunucu tabanlı otomasyon kuralları ile sertifikaların yaşam döngüsünü merkezi olarak yönetebilirsiniz.
>
> **Otomatik Çalışma Prensibi:** Bir kez yapılandırdıktan sonra, sistem belirlediğiniz yenileme eşik değerine göre (örn: 15 gün) sertifika süresini düzenli olarak izler. Süre dolmaya yaklaştığında, tanımladığınız iş akışı adımlarını (onay, yenileme, dağıtım) otomatik olarak başlatır ve zamanı geldiğinde sertifika yenileme ve yükleme işlemlerini gerçekleştirir.

İş Akışı Politikaları Listesi

Tüm oluşturulmuş iş akışı politikalarını görüntüleyin ve yönetin.

> **ERİŞİM YOLU**
>
> İş akışı politikalarına erişmek için: **Workflow -> Policy** menüsüne gidin.



	Workflow Identifier	Type	Common Name	Certificate Signature Types	Certificate Expire Date	Actions	Status
	ST-7200d755ea	Server-Based-Automation	cmtest01.sectrailcm.local	ADCS	28-11-2024 06:08:32		Active

Created At	Type	Detail
05.05.2026 10:25:41	Certificate-Renewal-Confirmation	• Renewal Confirmation Mails : admin@bntpro.com
05.05.2026 10:25:41	Certificate-Renewal	• CA Type : ADCS
05.05.2026 10:25:41	Deliver	• Deliver mail : salih.demir@bntpro.com
05.05.2026 10:25:41	Deployment	• Host : 10.34.4.69 • Device Type : F5 • Virtual Host : 10.34.28.17 • ServerName : 10.34.28.17:443
05.05.2026 10:25:41	Deployment	• Host : 10.34.4.69 • Device Type : F5 • Virtual Host : gkr_keycloak • ServerName : 10.34.28.200:443
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.150 • Device Type : IIS • Sites : Default Web Site • Virtual Host : • ServerName : *:443
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.150 • Device Type : IIS • Sites : Default Web Site • Virtual Host : test.bntpro-vlab.com • ServerName : *:443
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.150 • Device Type : IIS • Sites : Default Web Site • Virtual Host : iis1.bntpro-vlab.com • ServerName : *:443
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.101 • Device Type : Apache • Virtual Host : *:444!!!
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.101 • Device Type : Apache • Virtual Host : *:443!!!10.34.24.101 • ServerName : 10.34.24.101
05.05.2026 10:25:41	Deployment	• Host : 10.34.24.101 • Device Type : Apache • Virtual Host : *:443!!!register.sectrail.local • ServerName : register.sectrail.local

İş Akışı Politikaları - Tüm Otomasyon Kuralları

Liste Bilgileri

İş akışı listesinde her politika için aşağıdaki detaylar görüntülenir:

Sütun	Açıklama
Workflow Identifier	İş akışı için otomatik oluşturulan benzersiz kimlik (Örn: ST-0b6c4befb1)
Created At	Politikanın oluşturulma tarihi ve saati
Type	İş akışı tipi (Certificate-Renewal-Confirmation, Certificate-Renewal, Deliver, Deployment)
Common Name	İş akışının uygulanacağı sertifikanın common name bilgisi
Certificate Signature Types	Sertifika imza türü (ACME, RSA, ECDSA)
Certificate Expire Date	İlişkili sertifikanın son geçerlilik tarihi
Actions	Düzenleme ve silme işlemleri için aksiyon butonları
Status	İş akışının durumu: `Active` (Aktif) veya `Inactive` (Pasif)

İş Akışı Detayları

Her iş akışı kaydı genişletilerek detaylı bilgiler görüntülenebilir:

Detay Alanları

- **Renewal Confirmation Mails:** Yenileme onay bildirimleri için e-posta adresleri
- **CA Type:** Kullanılan sertifika otoritesi tipi (ACME, Internal CA)
- **Deliver mails:** Sertifika teslim bildirimi gönderilecek e-posta adresleri
- **Host:** Dağıtım yapılacak sunucu IP adresi
- **Device Type:** Hedef cihaz tipi (Apache, Nginx, F5, vb.)
- **Virtual Host:** Virtual host yapılandırması
- **ServerName:** Sunucu adı bilgisi

Yapılabilecek İşlemler

Üst Menü İşlemleri

- **Add New Flow** - Yeni iş akışı politikası oluşturma
- **Search** - İş akışlarını kimlik numarasına göre arama
- **Edit** - Mevcut politikayı düzenleme (kalem ikonu)
- **Delete** - Politikayı silme (çöp kutusu ikonu)
- **Expand/Collapse** - Detay bilgilerini görüntüleme/gizleme

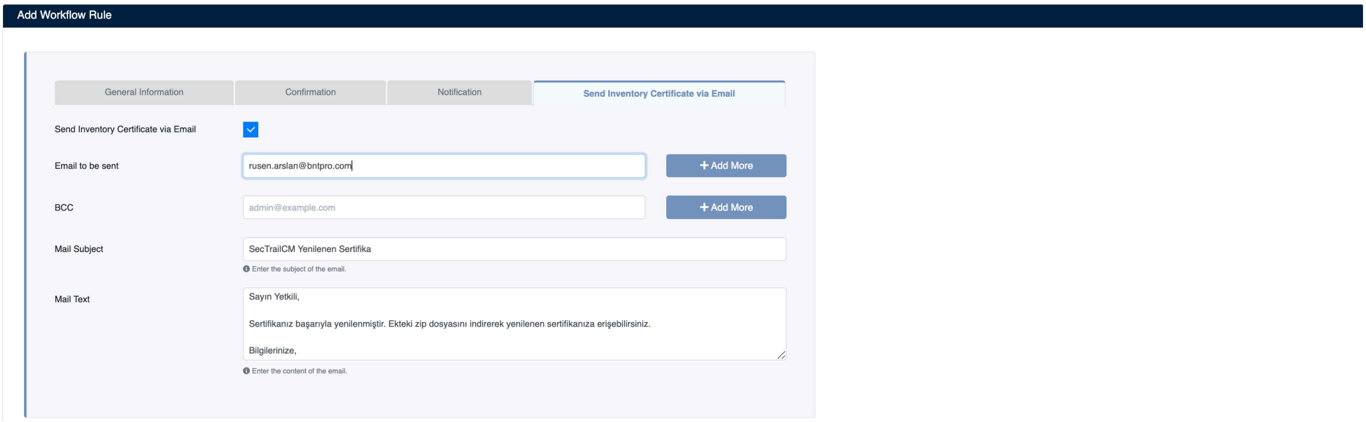
> **DİKKAT**
>
> Aktif bir iş akışını silmek, otomatik sertifika yenileme ve dağıtım süreçlerini durdurur. Silme işleminden önce emin olun.

Yeni İş Akışı Oluşturma

Sertifika yaşam döngüsü otomasyon kuralları oluşturun.

> **ERİŞİM YOLU**

Yeni iş akışı oluşturmak için: **Workflow -> Policy** sayfasında **Add New Flow** butonuna tıklayın.



Yeni İş Akışı Kuralı Oluşturma

Temel Yapılandırma

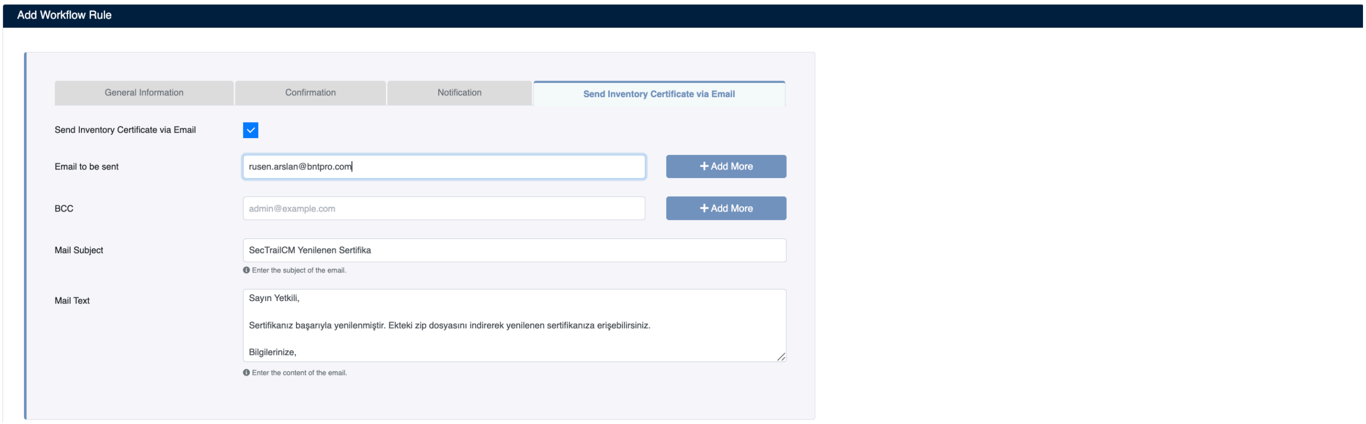
1. İş Akışı Tipi ve Sertifika Seçimi

Parametre	Açıklama	Seçenekler
Workflow Type	Otomasyon kuralı tipini belirleyin	`Server Based Automation`
Discover Certificate	İş akışının uygulanacağı keşfedilmiş sertifikayı seçin	Keşif listesinden sertifika seçimi
Select Servers	Otomasyonun çalışacağı sunucuları belirleyin	IP adresi veya hostname seçimi (çoklu seçim destekler)
Renewal Threshold	Sertifika yenileme eşik değeri (gün)	Sertifika süresinin kaç gün kala yenileneceği (varsayılan: 15)
Template	Kullanılacak sertifika şablonu	Önceden tanımlı şablonlardan seçim

Adımlar

1. **Workflow Type** olarak `Server Based Automation` seçin
2. **Discover Certificate** dropdown'ından ilgili sertifikayı seçin
3. **Select Servers** alanında hedef sunucuları seçin (çoklu sunucu seçilebilir)
4. **Renewal Threshold** için gün sayısı girin (örn: 15)
5. **Template** dropdown'ından uygun şablonu seçin

2. Dağıtım Yapılandırması



Dağıtım Ayarları

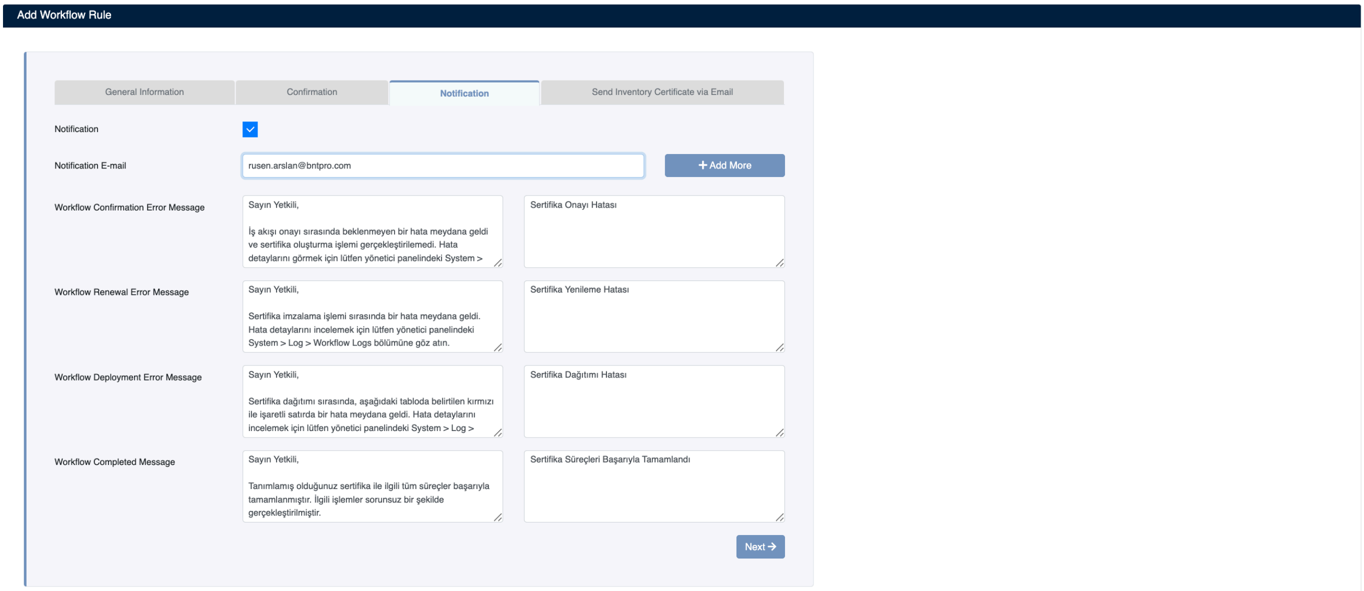
Sertifika dağıtım parametrelerini yapılandırın.

Parametre	Açıklama
Deployment	Otomatik dağıtımı etkinleştirin (checkbox)
Devices	Hedef cihaz tipini seçin (F5, Apache, Nginx, vb.)
Virtual Hosts	Dağıtım yapılacak virtual host yapılandırmalarını seçin
Devices (Secondary)	İkincil cihazlar için IP adresi
Virtual Hosts (Secondary)	İkincil virtual host yapılandırmaları
Deployment Time	Dağıtımın yapılacağı saat (HH:MM formatında)
Retry Limit	Başarısız dağıtım için yeniden deneme sayısı

Yapılandırma Adımları

1. **Deployment** checkbox'ını işaretleyin
2. **Devices** dropdown'ından cihaz tipini seçin
3. **Virtual Hosts** için ilgili yapılandırmaları seçin
4. İkincil cihazlar için IP adresi girin
5. **Deployment Time** alanına saat bilgisi girin (örn: 01:00)
6. **Retry Limit** için deneme sayısı belirleyin (örn: 1)

3. Onay Yapılandırması



Onay Bildirimleri Ayarları

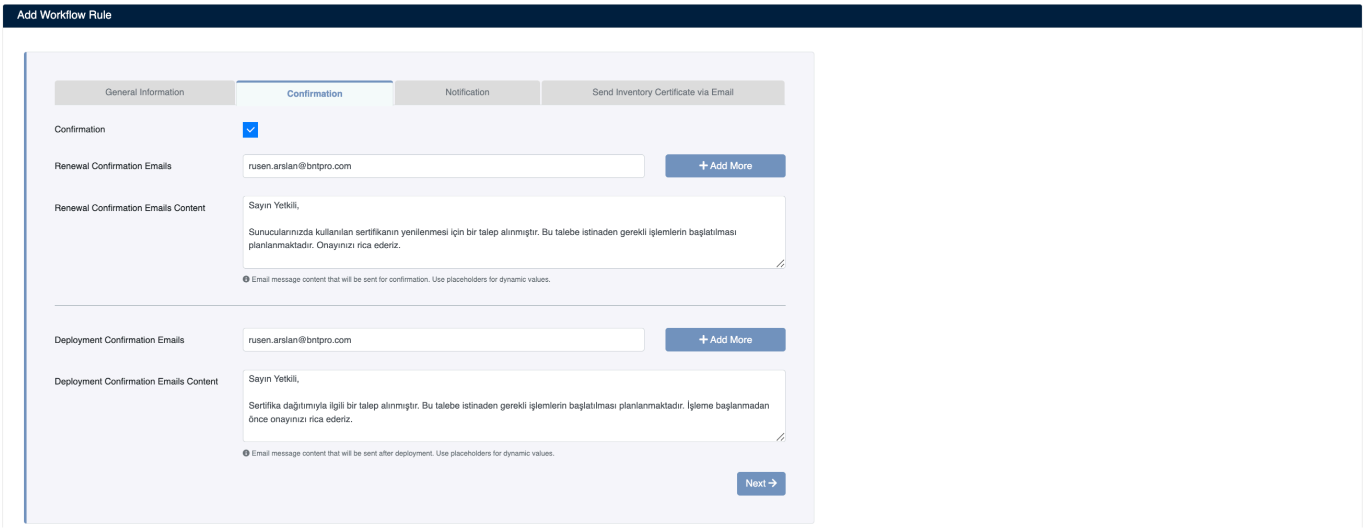
Sertifika yenileme ve dağıtım için onay süreçlerini yapılandırın.

Parametre	Açıklama
Confirmation	Onay mekanizmasını etkinleştirin
Renewal Confirmation Emails	Yenileme onayı için e-posta adresleri (virgülle ayrılmış)
Renewal Confirmation Emails Content	Yenileme onay e-postasının içeriği
Deployment Confirmation Emails	Dağıtım onayı için e-posta adresleri
Deployment Confirmation Emails Content	Dağıtım onay e-postasının içeriği

Yapılandırma Adımları

1. **Confirmation** checkbox'ını işaretleyin
2. **Renewal Confirmation Emails** alanına e-posta adreslerini girin
3. İlgili içerik alanına e-posta metnini yazın
4. **Deployment Confirmation Emails** için de aynı adımları tekrarlayın
5. **Add More** butonuyla ek e-posta adresleri ekleyin

4. Bildirim Yapılandırması

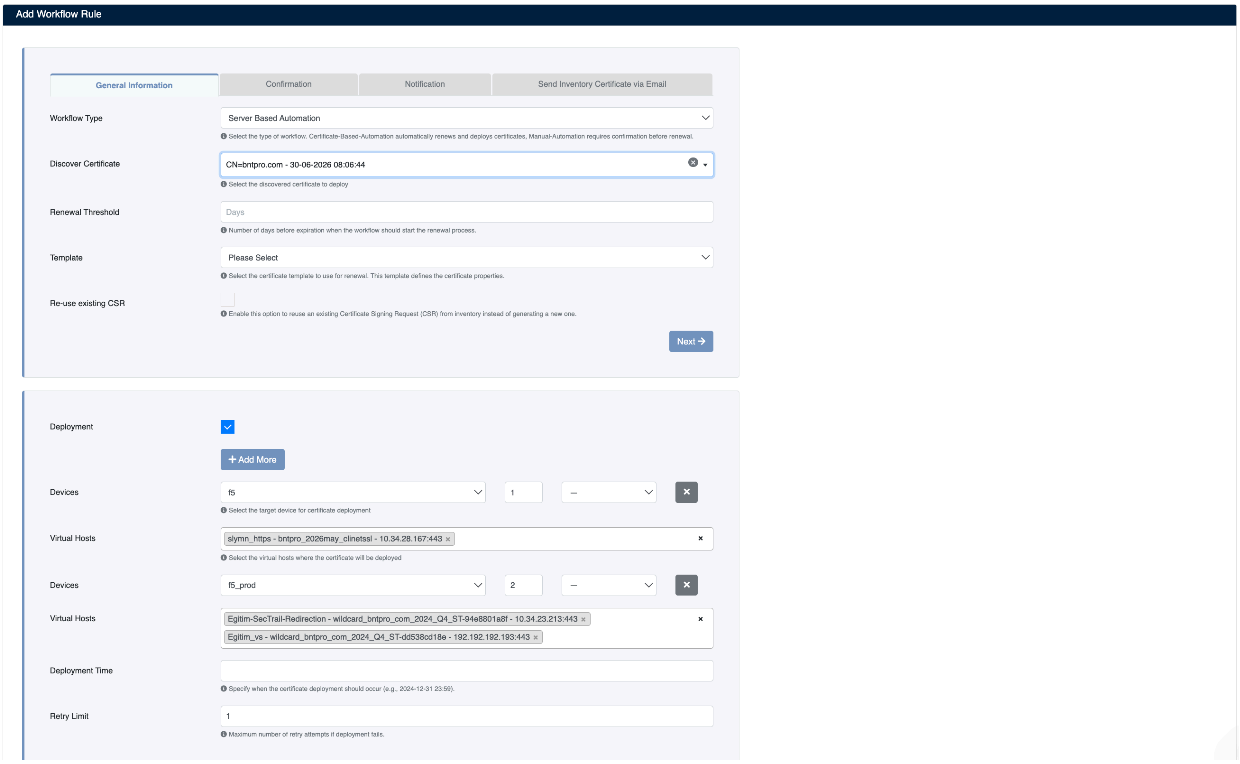


Bildirim Ayarları

İş akışı süreçleri için bildirim parametrelerini yapılandırın.

Parametre	Açıklama
Notification	Bildirim mekanizmasını etkinleştirin
Notification E-mail	Bildirim gönderilecek e-posta adresleri
Workflow Confirmation Error Message/Mail Subject	Onay hatası e-posta başlığı ve içeriği
Workflow Renewal Error Message/Mail Subject	Yenileme hatası e-posta başlığı ve içeriği
Workflow Deployment Error Message/Mail Subject	Dağıtım hatası e-posta başlığı ve içeriği
Workflow Completed Message/Mail Subject	Başarılı tamamlanma e-posta başlığı ve içeriği

5. E-posta ile Sertifika Gönderimi



E-posta ile Sertifika Gönderimi

Yenilenen sertifikaları otomatik olarak e-posta ile gönderin.

Parametre	Açıklama
Send Inventory Certificate via Email	E-posta gönderim özelliğini etkinleştirin
Email to be sent	Sertifikanın gönderileceği e-posta adresleri
BCC	Gizli kopya alacak e-posta adresleri
Mail Subject	E-posta konu başlığı
Mail Text	E-posta içerik metni

Yapılandırma Adımları

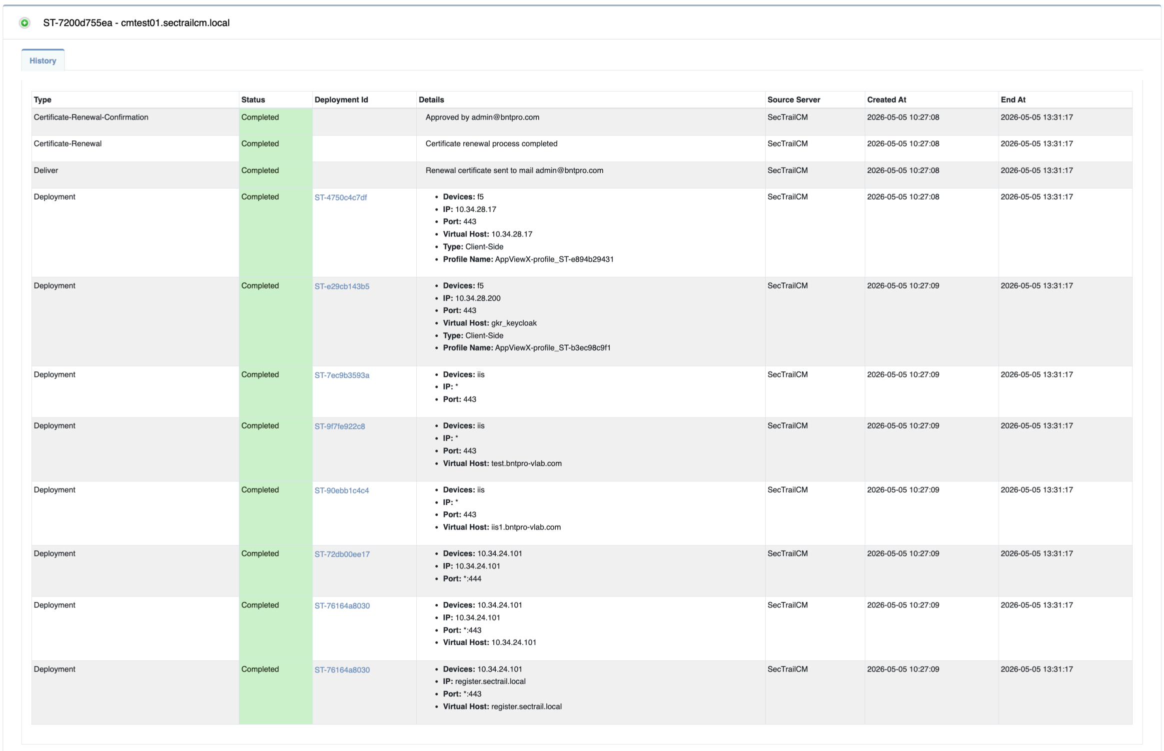
1. **Send Inventory Certificate via Email** checkbox'ını işaretleyin
2. **Email to be sent** alanına alıcı e-posta adreslerini girin
3. **BCC** alanına gizli kopya alacak adresleri ekleyin
4. **Mail Subject** için uygun bir başlık yazın (örn: "SecTrailCM Yenilenen Sertifika")
5. **Mail Text** alanına e-posta içeriğini girin
6. **Create** butonuna tıklayarak iş akışını kaydedin

İş Akışı Geçmişi

Oluşturulan iş akışlarının çalışma geçmişini ve detaylarını görüntüleyin.

ERİŞİM YOLU

İş akışı geçmişine erişmek için: **Workflow -> Processes** listesinde bir workflow identifier'a tıklayın.



İş Akışı Geçmişi - Süreç Adımları

Geçmiş Bilgileri

Her iş akışı çalıştırması için aşağıdaki bilgiler görüntülenir:

Sütun	Açıklama
Type	İşlem tipi (Certificate-Renewal-Confirmation, Certificate-Renewal, Deliver, Deployment)
Status	İşlem durumu (`Completed` , `Failed` , `Pending`)
Deployment Id	Dağıtım kimlik numarası
Details	İşlem detayları ve açıklamalar
Created At	İşlemin başlatılma tarihi ve saati
End At	İşlemin tamamlanma tarihi ve saati

Durum Göstergeleri

Durum	Açıklama
Completed	İşlem başarıyla tamamlandı
Failed	İşlem başarısız oldu
Pending	İşlem devam ediyor

Deployment Detayları

Deployment kayıtları genişletildiğinde aşağıdaki detaylar görüntülenir:

- **Devices:** Hedef cihaz listesi (örn: f5_prod)
- **IP:** Hedef sunucu IP adresi
- **Port:** Hedef port numarası
- **Virtual Host:** İlgili virtual host yapılandırması
- **Type:** Deployment tipi (Client-Side, Server-Side)
- **Profile Name:** Kullanılan profil adı

Örnek Deployment Kaydı

```
- 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
```

Arama ve Filtreleme

- **Search:** Workflow identifier ile arama yapın
- **Date Filter:** Tarih aralığına göre geçmiş kayıtlarını filtreleyin
- **Status Filter:** Duruma göre kayıtları filtreleyin

> **SAYFALAMA**
>
> Liste altında "Showing 1 to 5 of 5 entries" bilgisi ve sayfa numaraları ile gezinebilirsiniz.

İş Akışı Senaryosu Örneği

Aşağıda, gerçek bir kullanım senaryosu ile iş akışı yapılandırması adım adım anlatılmaktadır.

Senaryo: Wildcard Sertifika Otomatik Yenileme ve Dağıtım

Durum: Şirketinizde `*.bntpro.com` için bir wildcard sertifikası kullanılmaktadır. Bu sertifika birden fazla sunucuda (Apache, F5 load balancer) kullanılmaktadır.

Gereksinim: Sertifika süresi dolmadan otomatik olarak yenilenmeli ve tüm sunuculara dağıtılmalıdır.

Adım 1: Sertifika Keşfi

1. **Discovery -> Discovery List** menüsünden sertifika keşif kuralı oluşturun
2. Hedef sunucuları ekleyin (`10.34.23.213` , `10.34.24.181` , `cm.bntpro.com:443`)
3. Keşif başlatın ve sertifikaların tespit edilmesini bekleyin

Adım 2: İş Akışı Oluşturma

1. **Workflow -> Workflow Policies** sayfasından **Add New Flow** butonuna tıklayın
2. **Workflow Type:** `Server Based Automation` seçin

3. **Discover Certificate:** `CN=bntpro.com - 21-01-2026 09:52:47` seçin
4. **Select Servers:** Tüm sunucuları seçin

- `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:** `15` gün olarak ayarlayın
6. **Template:** `lets_encrypt_template` seçin

Adım 3: Dağıtım Yapılandırması

1. **Deployment** checkbox'ını işaretleyin
2. **Devices (Primary):** `f5_prod` seçin
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` (gece 1:00)
7. **Retry Limit:** `1`

Adım 4: Onay Mekanizması

1. **Confirmation** checkbox'ını işaretleyin
2. **Renewal Confirmation Emails:** `admin@example.com, sdg-dev@bntpro.com, destek@bntpro.com`.
3. **Deployment Confirmation Emails:** `admin@example.com`

Adım 5: Bildirim Yapılandırması

1. **Notification** checkbox'ını işaretleyin
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**

Adım 6: E-posta ile Teslimat

1. **Send Inventory Certificate via Email** checkbox'ını işaretleyin
2. **Email to be sent:** `admin@example.com, sdg-dev@bntpro.com, destek@bntpro.com`
3. **BCC:** `admin@example.com`

4. **Mail Subject:** `SecTrailCM Yenilenen Sertifika`

Adım 7: Kaydetme ve Aktivasyon

1. **Create** butonuna tıklayarak iş akışını kaydedin
2. İş akışı otomatik olarak `Active` duruma geçer
3. Sistem, sertifika süresinin bitmesine 15 gün kala otomatik olarak yenileme sürecini başlatır

İş Akışı Çalışma Sırası

Oluşturulan iş akışı aşağıdaki sırayla çalışır:

1. **Gün 0-15:** Sistem sertifika süresini kontrol eder
2. **Gün 15 (Yenileme Başlangıcı):**

- Yenileme onay e-postası gönderilir
- Onay bekler

3. **Onay Sonrası:**

- Sertifika yenileme işlemi başlar (ACME/Let's Encrypt)
- Yeni sertifika oluşturulur

4. **Dağıtım Onayı:**

- Dağıtım onay e-postası gönderilir
- Onay bekler

5. **Saat 01:00 (Dağıtım):**

- F5 load balancer'a dağıtım yapılır
- Apache sunucusuna dağıtım yapılır
- Her dağıtım için retry yapılır (başarısız olursa)

6. **Tamamlanma:**

- Tüm işlemler başarılı ise bildirim e-postası gönderilir
- Yeni sertifika e-posta ile paylaşılır

7. **Hata Durumu:**

- Herhangi bir adımda hata oluşursa, ilgili hata bildirimi gönderilir
- Workflow Logs'da detaylı log kaydı oluşturulur

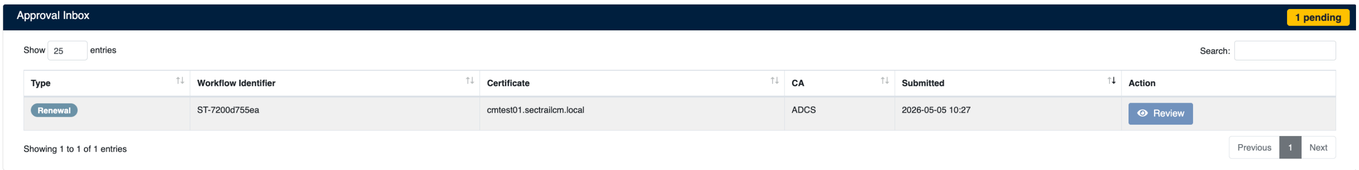
EN İYİ UYGULAMALAR

- **Deployment Time:** Dağıtım saatini düşük trafikli saatlere (gece 01:00-04:00) ayarlayın
- **Retry Limit:** Kritik sistemler için retry limit'i artırın
- **Notification:** Birden fazla yönetici e-postası ekleyin
- **BCC:** Tüm e-posta bildirimlerinde arşivleme için BCC kullanın
- **Testing:** İlk kurulumda test sertifikası ile deneme yapın

Onay Bekleyen İş Akışları

Onay mekanizması etkinleştirilmiş iş akışlarında, yenileme veya dağıtım adımları başlamadan önce kullanıcı onayı beklenir. Onay bekleyen iş akışlarını bu ekrandan görüntüleyebilir ve yönetebilirsiniz.

> **ERİŞİM YOLU**
>
> Onay bekleyen iş akışlarına erişmek için: **Workflow -> Approval** menüsüne gidin.



Onay Bekleyen İş Akışları Listesi

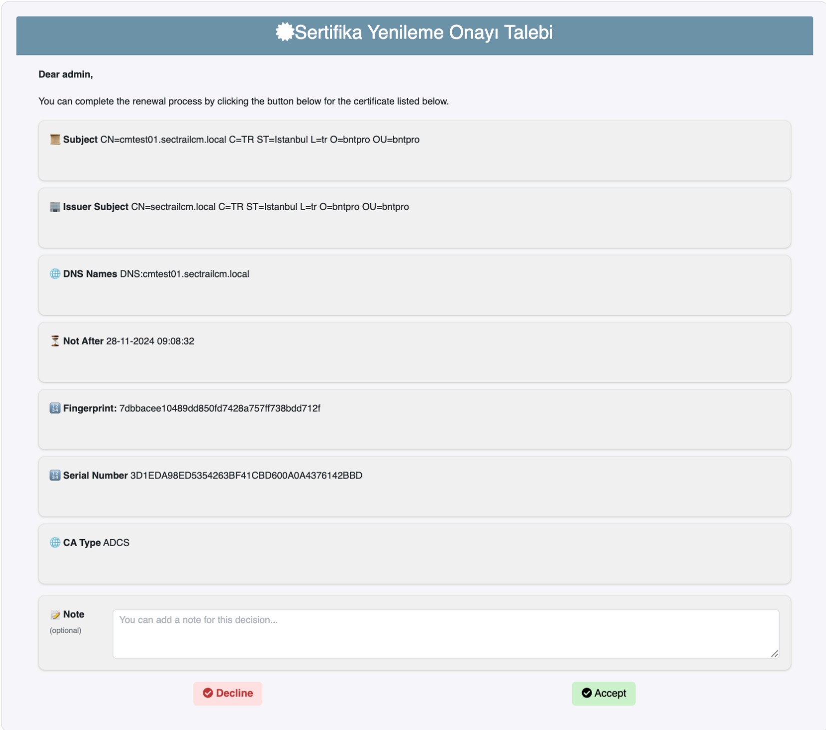
Liste Bilgileri

Onay listesinde her kayıt için aşağıdaki bilgiler görüntülenir:

Sütun	Açıklama
Workflow Identifier	İş akışının benzersiz kimlik numarası
Type	Onay tipi (Certificate-Renewal-Confirmation, Deployment-Confirmation)
Common Name	İlgili sertifikanın common name bilgisi
Created At	Onay talebinin oluşturulma tarihi ve saati
Actions	Onaylama veya reddetme işlemleri

Onay İşlemi

Onay bekleyen bir iş akışını onaylamak için ilgili kayıt üzerindeki **Approve** butonuna tıklayın. Onay verildiğinde iş akışı kaldığı adımdan devam eder.



Onay Detay Ekranı

> **DİKKAT**
>
> Onay talebini reddetmeniz durumunda ilgili iş akışı adımı iptal edilir ve süreç durdurulur.

Sahiplik Yönetimi

SecTrail Certificate Manager, sunucu veya sertifika özniteliklerine göre sertifikalara otomatik olarak sahiplik atama imkanı sunar. Bu sayede alarmlar ve bildirimler doğru ekiplere ve kişilere yönlendirilir.

Genel Bakış

Sahiplik yönetimi sistemi ile:

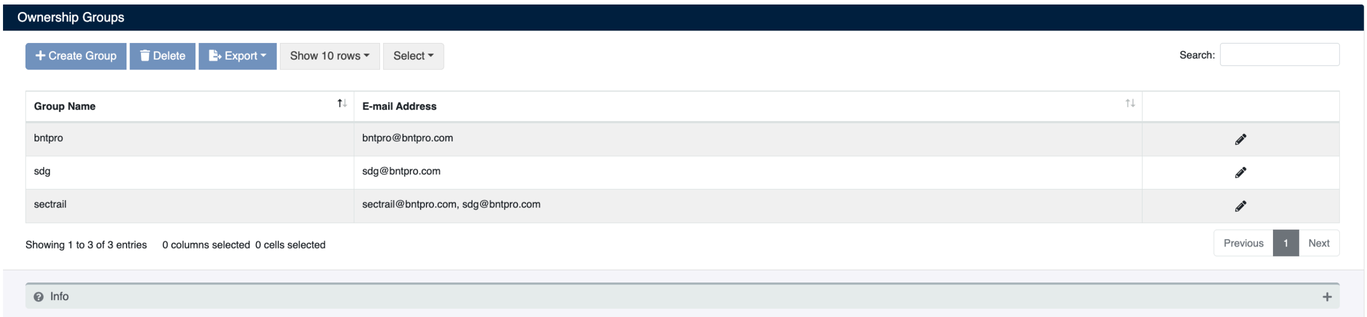
- Sunucu IP adresleri veya sertifika özniteliklerine göre sahiplik atayabilirsiniz
- Keşif listelerini sahiplik bilgileri ile otomatik güncelleyebilirsiniz
- Alarmları ilgili ekiplere yönlendirebilirsiniz
- Harici envanter sistemleriyle API aracılığıyla entegre olabilirsiniz
- Regex kuralları kullanarak sahiplik kuralları tanımlayabilirsiniz

Sahiplik Bileşenleri

Sahiplik Grupları

Sahiplik Grupları, sertifikalardan sorumlu ekipleri veya kişileri tanımlar. Her grup şunlardan oluşur:

- **Grup Adı**: Grup için benzersiz bir tanımlayıcı
- **E-posta Adresleri**: Bildirimleri alacak bir veya daha fazla e-posta adresi

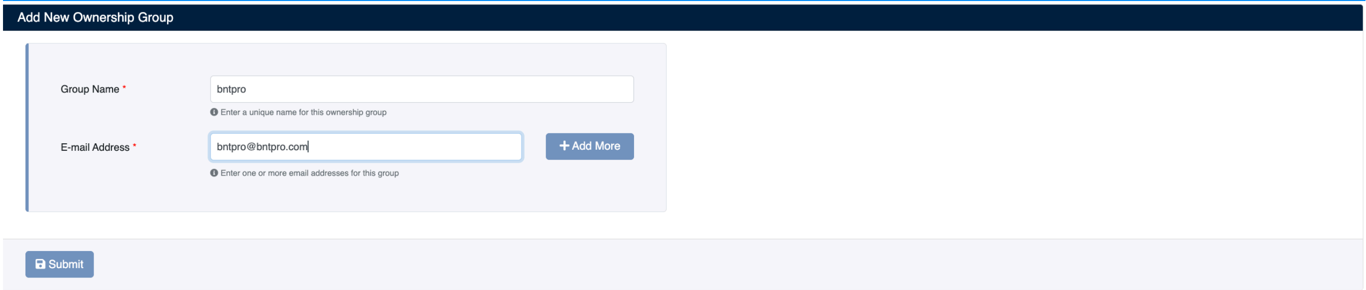


Sahiplik Grubu Oluşturma

1. **Ownership Groups** bölümüne gidin
2. **Create Group** butonuna tıklayın
3. Aşağıdaki bilgileri girin:

- **Group Name**: Ekip veya grup için açıklayıcı bir isim
- **E-mail Address**: "Add More" butonu ile bir veya daha fazla e-posta adresi ekleyin

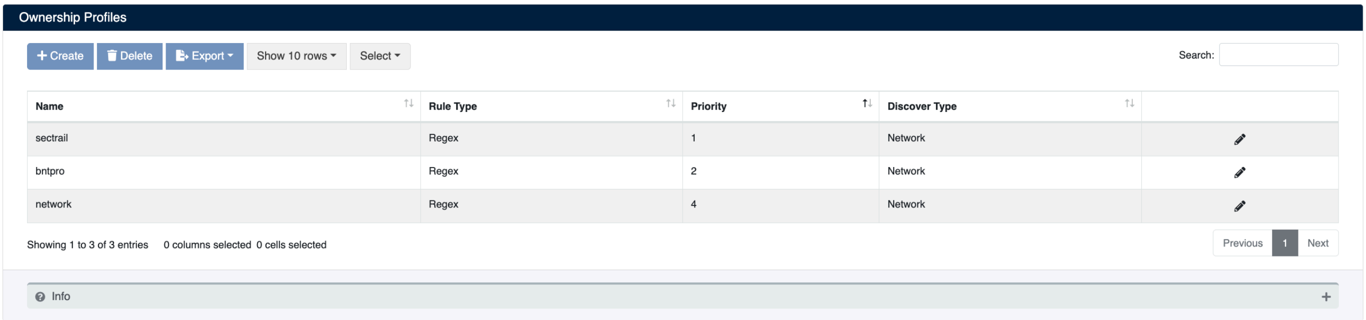
4. Grubu oluşturmak için **Submit** butonuna tıklayın



Sahiplik Profilleri

Sahiplik Profilleri, hangi sertifika veya sunucuların hangi sahiplik grubuna ait olacağını belirleyen kuralları tanımlar. Aşağıdaki kriterlere göre profiller oluşturabilirsiniz:

- Ağ tabanlı keşif (IP adresleri)
- Sertifika öznitelikleri (subject, issuer, SAN, vb.)



Sahiplik Profili Oluşturma

1. **Ownership Profiles** bölümüne gidin
2. **Create** butonuna tıklayın
3. Aşağıdaki alanları yapılandırın:

Temel Bilgiler:

- **Name**: Profil için açıklayıcı bir isim
- **Discover Type**: Network veya DataPower seçeneklerinden birini seçin
- **Rule Type**: Eşleştirme yöntemini seçin (Regex, Service)
- **Type**: Eşleştirilecek özniteliği seçin (Subject, IP Address)
- **Condition**: Eşleştirme koşulunu seçin (contains, equals)
- **Regex**: Eşleştirilecek regex desenini girin. "Add More" ile birden fazla desen ekleyebilirsiniz
- Sertifikalar için örnek: `CN=example.com.tr,OU=Security...`
- IP adresleri için örnek: `192.168.1..*`

Grup Ataması:

- **Ownership Groups**: Kural eşleştiğinde atanacak sahiplik grubunu seçin

Sertifika E-posta Kullanımı:

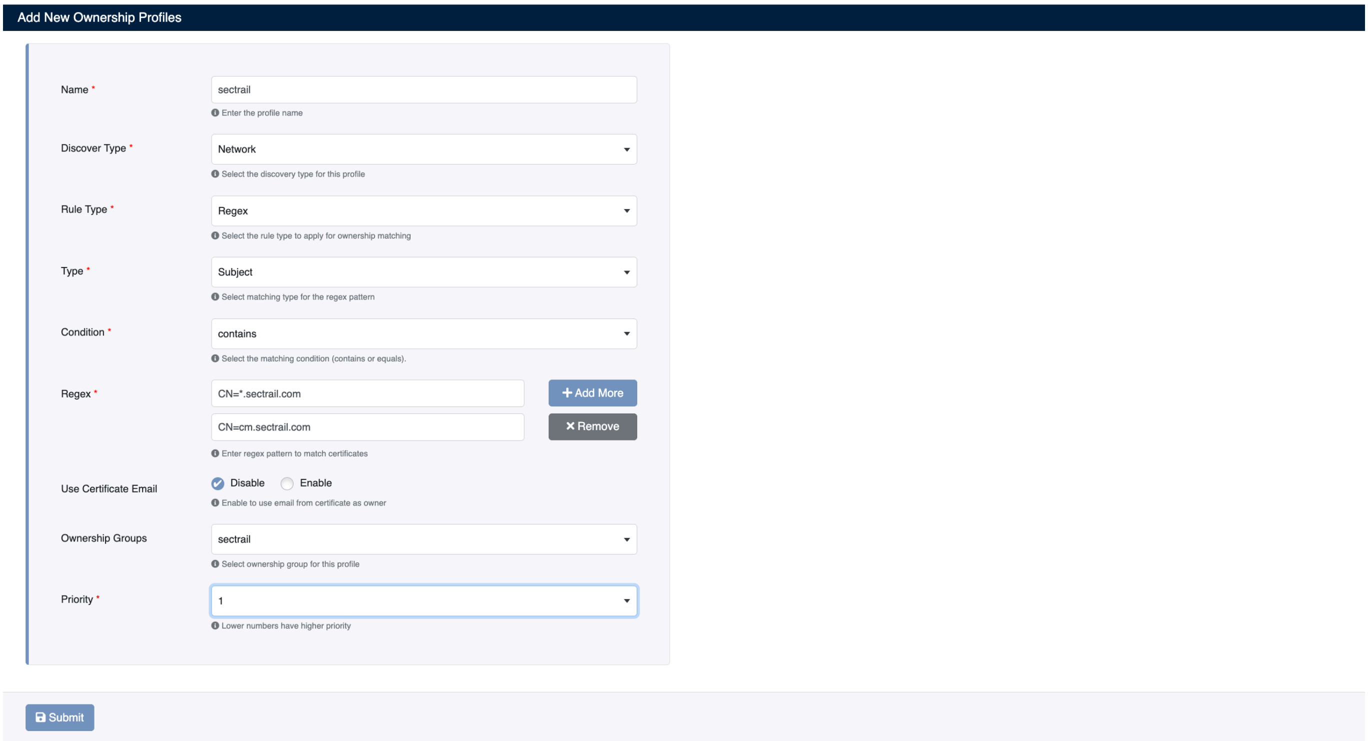
- **Utilize the email address found in the certificate**:
- Enable: Sertifikada bulunan e-posta adreslerini kullan

- Disable: Sadece sahiplik grubu e-postalarını kullan

Öncelik:

- Bu kural için öncelik seviyesini belirleyin (1 = en yüksek öncelik)
- Birden fazla kural eşleştiğinde, en yüksek önceliğe sahip kural uygulanır

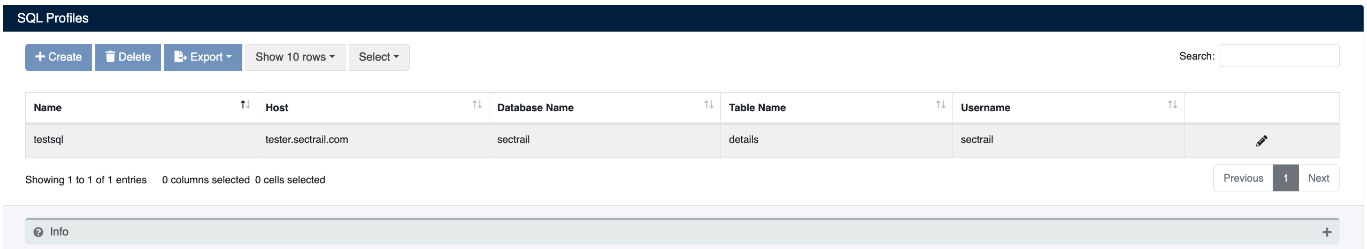
4. Profili oluşturmak için **Submit** butonuna tıklayın



Sahiplik Servis Profilleri

Organizasyonunuzun kendi içinde bir envanter sistemi varsa ve sahiplik bilgilerini bu sistemde tutuyorsanız, SecTrail CM'yi kendi API'niz ile entegre edebilirsiniz. Bu entegrasyon ile:

- SecTrail CM, keşfedilen sertifikalar için sahiplik bilgilerini otomatik olarak sorgulamak üzere sizin sağladığınız API'yi çağırır
- Teknik ekibiniz, kendi envanter sisteminizde bir API endpoint hazırlar
- API üzerinden sahiplik bilgileri SecTrail CM ile senkronize edilir
- Manuel sahiplik ataması yapmaya gerek kalmaz



Sahiplik Servis Profili Oluşturma

1. **Ownership Service Profiles** bölümüne gidin
2. **Create** butonuna tıklayın

3. Aşağıdaki entegrasyon bilgilerini girin:

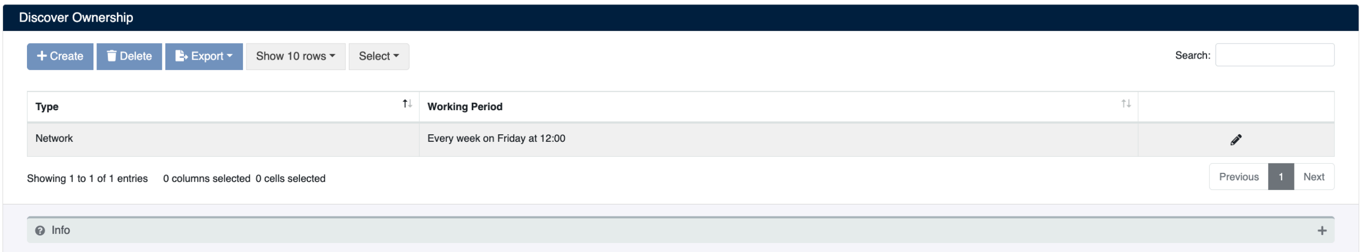
- **Name**: Servis profili için açıklayıcı bir isim (örn: "CMDB API", "Envanter Sistemi")
- **URL**: Kendi envanter sisteminizin API endpoint adresi (örn: `https://cmdb.sirketiniz.com/api/ownership`)
- **Username**: API için kimlik doğrulama kullanıcı adı (credential bilgisi)
- **Password**: API için kimlik doğrulama parolası (credential bilgisi)

4. Servis profilini oluşturmak için **Submit** butonuna tıklayın

> **API ENTEGRASYONU İÇİN**
>
> Teknik ekibinizle iletişime geçerek, kendi envanter sisteminizde SecTrail CM'nin sorgulama yapabileceği bir API endpoint hazırlatmanız gerekmektedir. API, sertifika bilgilerini alıp ilgili sahiplik grubunu döndürmelidir.

Keşif Ayarları

Sahiplik bilgilerinin envanterdeki sertifikalara yansıtılabilmesi için **Ownership -> Discovery Settings** bölümünden keşif zamanlaması yapılandırılmalıdır. Bu sayede SecTrail CM, belirlenen periyotta sahiplik profillerini sertifikalarla otomatik olarak eşleştirir ve envanter güncel tutulur.



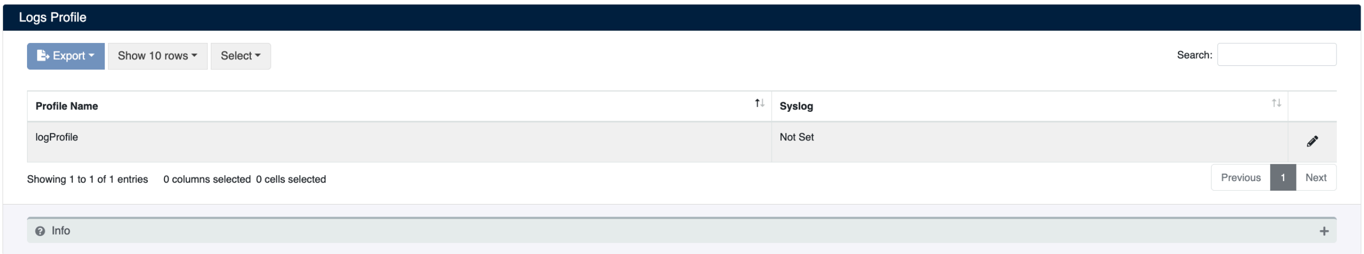
- **Type**: Keşif tipini belirtir (örn. `Network`)
- **Working Period**: Sahiplik eşleştirmesinin çalışacağı periyot (örn. `Every week on Friday at 12:00`)

Sistem Logları

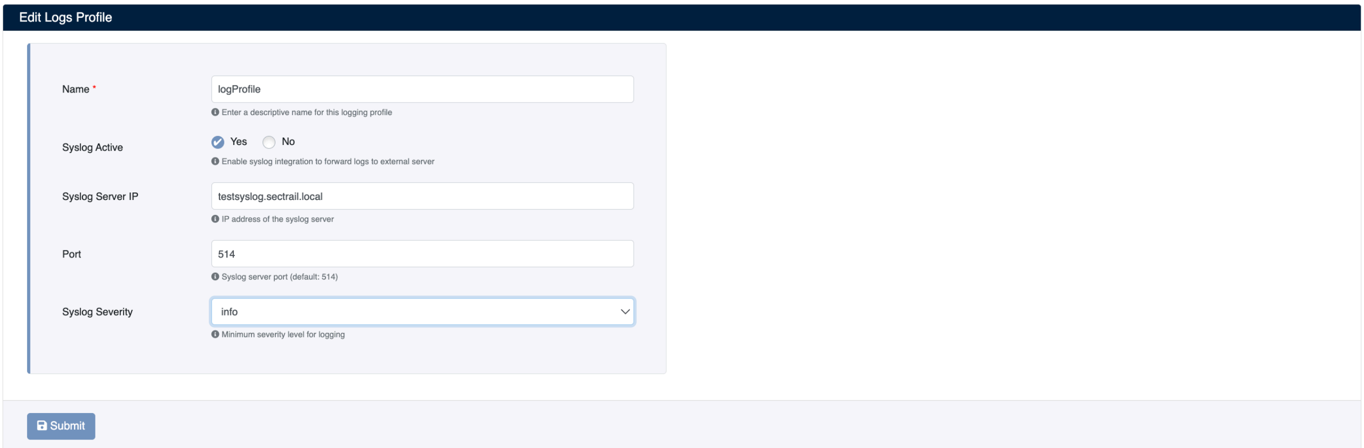
SecTrail CM, sistem üzerinde gerçekleşen tüm işlemleri farklı log kategorileri altında kaydeder. Bu loglar hem sistem içinden izlenebilir hem de harici bir Syslog sunucusuna iletilebilir.

Syslog Yapılandırması

Logları harici bir Syslog sunucusuna iletmek için **System > Log > Logging Profiles** bölümünden mevcut profili düzenleyin.



Profil üzerindeki kalem ikonuna tıklayarak aşağıdaki alanları doldurun:

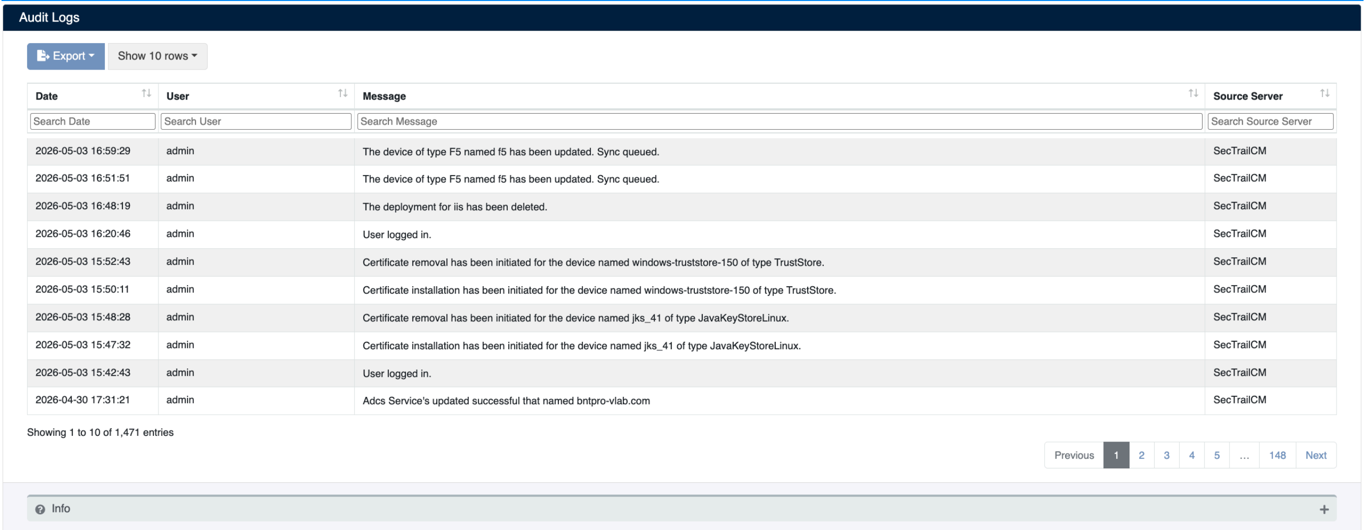


- **Name**: Log profili için tanımlayıcı bir isim
- **Syslog Active**: Syslog iletimini etkinleştirmek için `Yes` seçin
- **Syslog Server IP**: Syslog sunucusunun IP adresi veya hostname'i
- **Port**: Syslog sunucusunun portu (varsayılan: `514`)
- **Syslog Severity**: İletilecek minimum log seviyesi (örn. `info`, `warning`, `error`)

Log Kategorileri

Audit Logs

Kullanıcı işlemlerini ve sistem olaylarını kaydeder. Kimin, ne zaman hangi işlemi gerçekleştirdiğini takip etmek için kullanılır.



Audit Logs

Export | Show 10 rows

Date	User	Message	Source Server
2026-05-03 16:59:29	admin	The device of type F5 named f5 has been updated. Sync queued.	SecTrailCM
2026-05-03 16:51:51	admin	The device of type F5 named f5 has been updated. Sync queued.	SecTrailCM
2026-05-03 16:48:19	admin	The deployment for iis has been deleted.	SecTrailCM
2026-05-03 16:20:46	admin	User logged in.	SecTrailCM
2026-05-03 15:52:43	admin	Certificate removal has been initiated for the device named windows-truststore-150 of type TrustStore.	SecTrailCM
2026-05-03 15:50:11	admin	Certificate installation has been initiated for the device named windows-truststore-150 of type TrustStore.	SecTrailCM
2026-05-03 15:48:28	admin	Certificate removal has been initiated for the device named jks_41 of type JavaKeyStoreLinux.	SecTrailCM
2026-05-03 15:47:32	admin	Certificate installation has been initiated for the device named jks_41 of type JavaKeyStoreLinux.	SecTrailCM
2026-05-03 15:42:43	admin	User logged in.	SecTrailCM
2026-04-30 17:31:21	admin	Adcs Service's updated successful that named bntpro-vlab.com	SecTrailCM

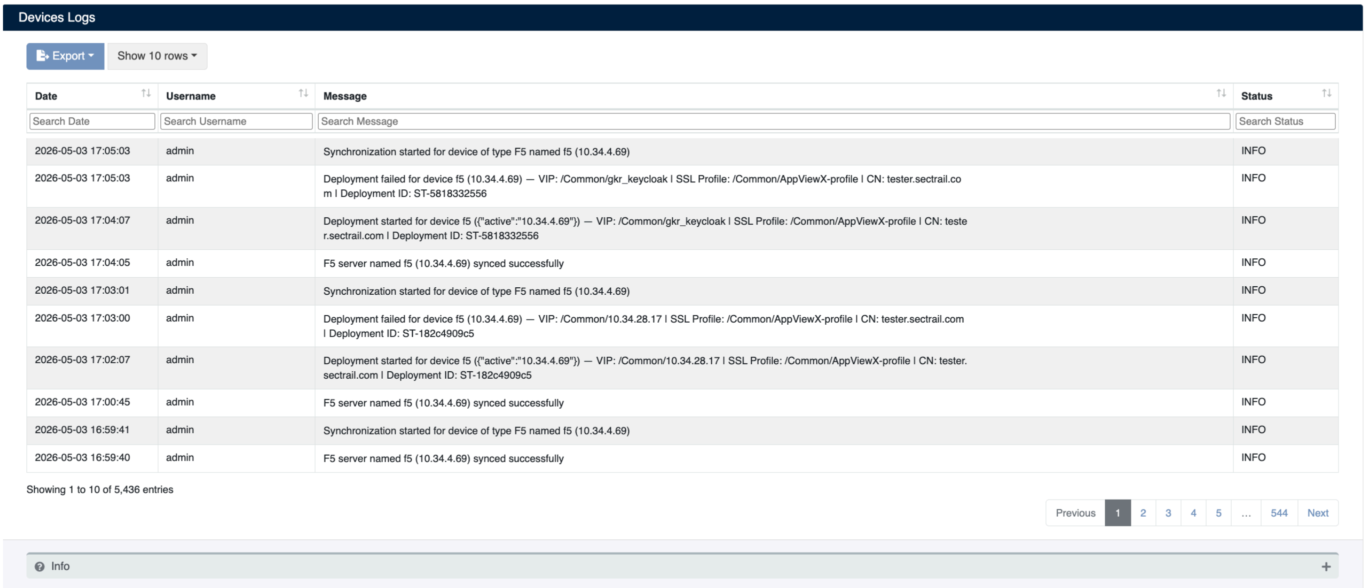
Showing 1 to 10 of 1,471 entries

Previous 1 2 3 4 5 … 148 Next

Info

Device Logs

Cihazlara yapılan sertifika dağıtım ve senkronizasyon işlemlerinin detaylı loglarını içerir.



Devices Logs

Export | Show 10 rows

Date	Username	Message	Status
2026-05-03 17:05:03	admin	Synchronization started for device of type F5 named f5 (10.34.4.69)	INFO
2026-05-03 17:05:03	admin	Deployment failed for device f5 (10.34.4.69) — VIP: /Common/gkr_keycloak | SSL Profile: /Common/AppViewX-profile | CN: tester.sectrail.com | Deployment ID: ST-5818332556	INFO
2026-05-03 17:04:07	admin	Deployment started for device f5 ({"active":"10.34.4.69"}) — VIP: /Common/gkr_keycloak | SSL Profile: /Common/AppViewX-profile | CN: tester.sectrail.com | Deployment ID: ST-5818332556	INFO
2026-05-03 17:04:05	admin	F5 server named f5 (10.34.4.69) synced successfully	INFO
2026-05-03 17:03:01	admin	Synchronization started for device of type F5 named f5 (10.34.4.69)	INFO
2026-05-03 17:03:00	admin	Deployment failed for device f5 (10.34.4.69) — VIP: /Common/10.34.28.17 | SSL Profile: /Common/AppViewX-profile | CN: tester.sectrail.com | Deployment ID: ST-182c4909c5	INFO
2026-05-03 17:02:07	admin	Deployment started for device f5 ({"active":"10.34.4.69"}) — VIP: /Common/10.34.28.17 | SSL Profile: /Common/AppViewX-profile | CN: tester.sectrail.com | Deployment ID: ST-182c4909c5	INFO
2026-05-03 17:00:45	admin	F5 server named f5 (10.34.4.69) synced successfully	INFO
2026-05-03 16:59:41	admin	Synchronization started for device of type F5 named f5 (10.34.4.69)	INFO
2026-05-03 16:59:40	admin	F5 server named f5 (10.34.4.69) synced successfully	INFO

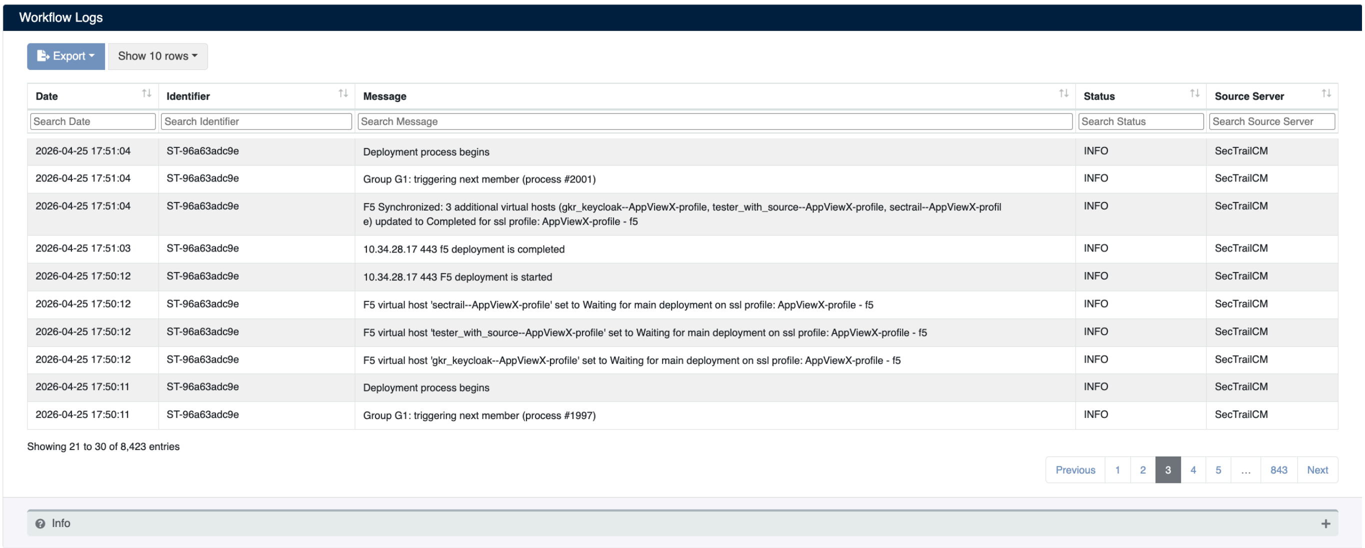
Showing 1 to 10 of 5,436 entries

Previous 1 2 3 4 5 … 544 Next

Info

Workflow Logs

Otomasyon iş akışları kapsamında tetiklenen dağıtım süreçlerinin adım adım loglarını içerir.

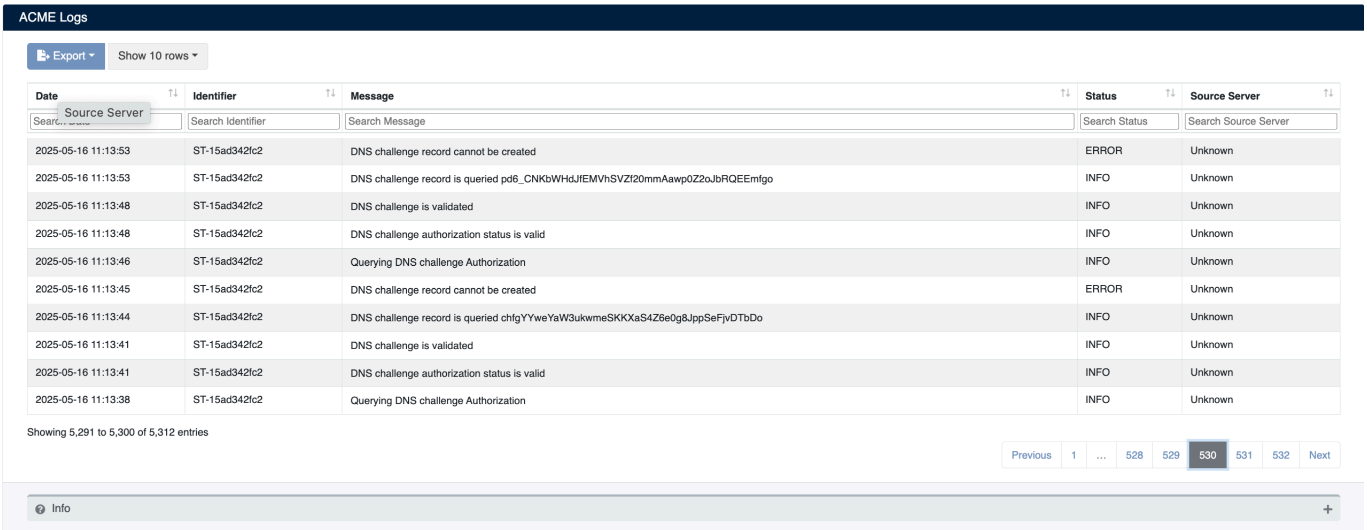


Date	Identifier	Message	Status	Source Server
2026-04-25 17:51:04	ST-96a63adc9e	Deployment process begins	INFO	SecTrailCM
2026-04-25 17:51:04	ST-96a63adc9e	Group G1: triggering next member (process #2001)	INFO	SecTrailCM
2026-04-25 17:51:04	ST-96a63adc9e	F5 Synchronized: 3 additional virtual hosts (gkr_keycloak--AppViewX-profile, tester_with_source--AppViewX-profile, sectrail--AppViewX-profile) updated to Completed for ssl profile: AppViewX-profile - f5	INFO	SecTrailCM
2026-04-25 17:51:03	ST-96a63adc9e	10.34.28.17 443 f5 deployment is completed	INFO	SecTrailCM
2026-04-25 17:50:12	ST-96a63adc9e	10.34.28.17 443 F5 deployment is started	INFO	SecTrailCM
2026-04-25 17:50:12	ST-96a63adc9e	F5 virtual host 'sectrail--AppViewX-profile' set to Waiting for main deployment on ssl profile: AppViewX-profile - f5	INFO	SecTrailCM
2026-04-25 17:50:12	ST-96a63adc9e	F5 virtual host 'tester_with_source--AppViewX-profile' set to Waiting for main deployment on ssl profile: AppViewX-profile - f5	INFO	SecTrailCM
2026-04-25 17:50:12	ST-96a63adc9e	F5 virtual host 'gkr_keycloak--AppViewX-profile' set to Waiting for main deployment on ssl profile: AppViewX-profile - f5	INFO	SecTrailCM
2026-04-25 17:50:11	ST-96a63adc9e	Deployment process begins	INFO	SecTrailCM
2026-04-25 17:50:11	ST-96a63adc9e	Group G1: triggering next member (process #1997)	INFO	SecTrailCM

Showing 21 to 30 of 8,423 entries

ACME Logs

ACME protokolü üzerinden gerçekleştirilen DNS challenge ve sertifika yenileme işlemlerinin loglarını içerir.

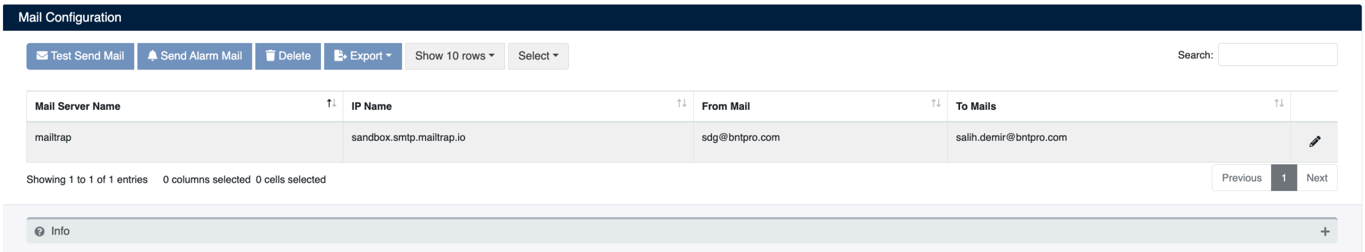


Date	Identifier	Message	Status	Source Server
2025-05-16 11:13:53	ST-15ad342fc2	DNS challenge record cannot be created	ERROR	Unknown
2025-05-16 11:13:53	ST-15ad342fc2	DNS challenge record is queried pd6_CNKbWHdJfEMVhSVZf20mmAawp0Z2oJbRQEEmfgo	INFO	Unknown
2025-05-16 11:13:48	ST-15ad342fc2	DNS challenge is validated	INFO	Unknown
2025-05-16 11:13:48	ST-15ad342fc2	DNS challenge authorization status is valid	INFO	Unknown
2025-05-16 11:13:46	ST-15ad342fc2	Querying DNS challenge Authorization	INFO	Unknown
2025-05-16 11:13:45	ST-15ad342fc2	DNS challenge record cannot be created	ERROR	Unknown
2025-05-16 11:13:44	ST-15ad342fc2	DNS challenge record is queried chfgYYweYaW3ukwmeSKKXaS4Z6e0g8JppSeFjvDTbDo	INFO	Unknown
2025-05-16 11:13:41	ST-15ad342fc2	DNS challenge is validated	INFO	Unknown
2025-05-16 11:13:41	ST-15ad342fc2	DNS challenge authorization status is valid	INFO	Unknown
2025-05-16 11:13:38	ST-15ad342fc2	Querying DNS challenge Authorization	INFO	Unknown

Showing 5,291 to 5,300 of 5,312 entries

Mail Yapılandırması

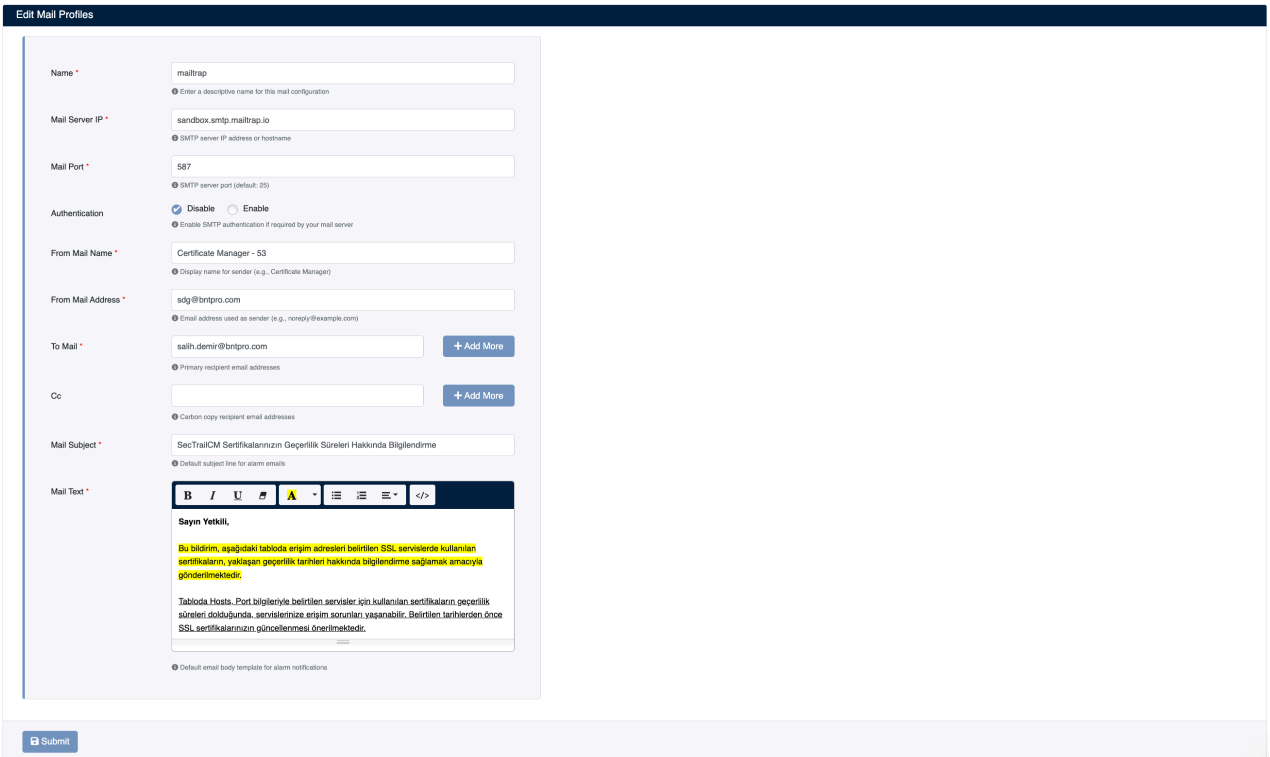
SecTrail CM, sertifika alarmları ve bildirimlerini e-posta üzerinden iletmek için SMTP tabanlı bir mail yapılandırması sunar. **System > Mail Configuration** bölümünden tanımlı profiller görüntülenebilir ve düzenlenebilir.



Listede **Mail Server Name**, **IP Name**, **From Mail** ve **To Mails** sütunları görüntülenir. **Test Send Mail** butonu ile yapılandırmanın doğruluğu test edilebilir, **Send Alarm Mail** butonu ile de anlık alarm maili gönderilebilir.

Mail Profili Düzenleme

Profil üzerindeki kalem ikonuna tıklayarak aşağıdaki alanları doldurun:

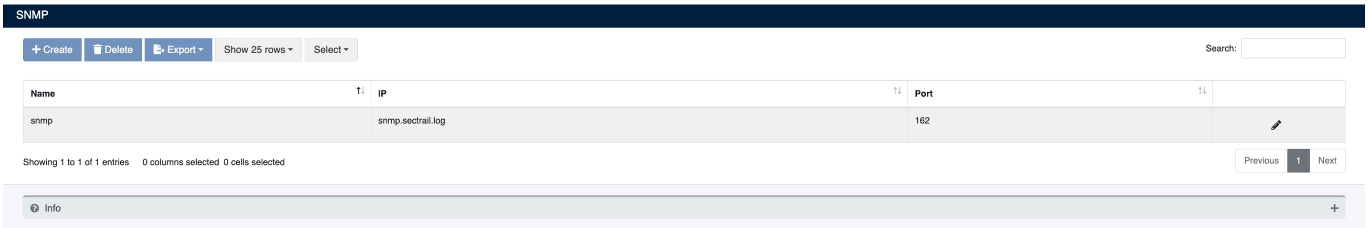


- **Name**: Mail profili için tanımlayıcı bir isim
- **Mail Server**: SMTP sunucusunun IP adresi veya hostname'i
- **Mail Port**: SMTP portu (varsayılan: `25`)
- **Authentication**: SMTP kimlik doğrulama gerekiyorsa `Enable` seçin
- **From Mail Name**: Gönderici adı (örn. `Certificate Manager - S5`)
- **From Mail Address**: Gönderici e-posta adresi
- **To Mail**: Bildirimlerin iletileceği birincil alıcı adresi; **+ Add More** ile birden fazla alıcı eklenebilir

- **Cc**: Kopyalanacak e-posta adresleri; **+ Add More** ile birden fazla eklenebilir
- **Mail Subject**: Alarm e-postalarının konu satırı
- **Mail Text**: Alarm e-postalarında kullanılacak varsayılan içerik şablonu (zengin metin editörü ile düzenlenebilir)

SNMP Yapılandırması

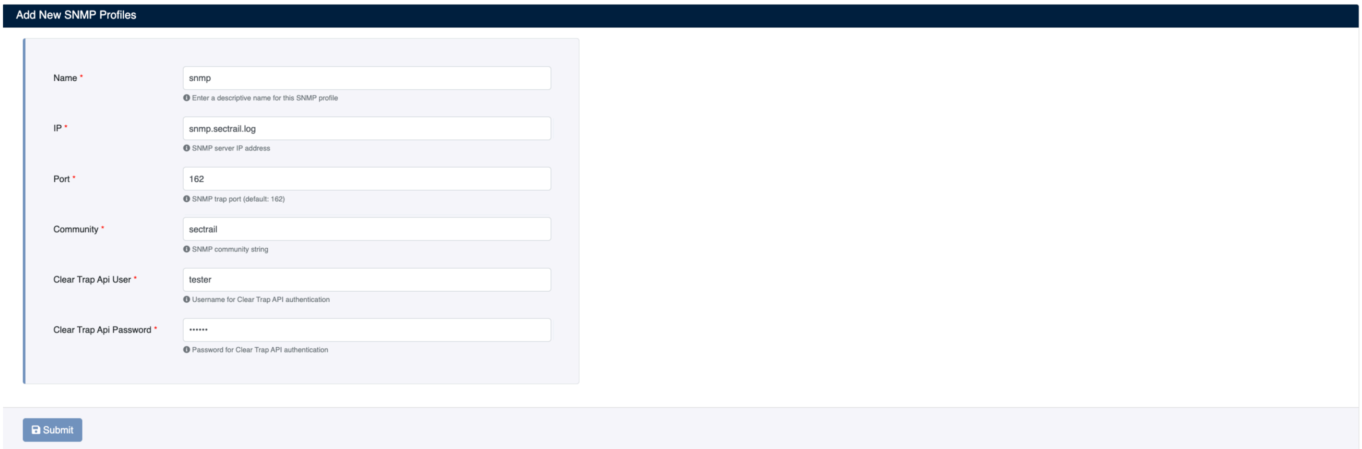
SecTrail CM, sertifika alarmlarını SNMP trap olarak harici bir SNMP sunucusuna iletebilir. **System > SNMP** bölümünden SNMP profilleri oluşturulabilir ve yönetilebilir.



Listede tanımlı profillerin **Name**, **IP** ve **Port** bilgileri görüntülenir.

Yeni SNMP Profili Oluşturma

+ Create butonuna tıklayarak yeni bir SNMP profili ekleyin:



- **Name**: SNMP profili için tanımlayıcı bir isim
- **IP**: SNMP trap alıcısının IP adresi veya hostname'i
- **Port**: SNMP trap portu (varsayılan: `162`)
- **Community**: SNMP community string (örn. `sectrail`)
- **Clear Trap Api User**: Clear trap işlemi için API kullanıcı adı
- **Clear Trap Api Password**: Clear trap işlemi için API şifresi

> **INFO**
>
> Profil oluşturulduktan sonra sertifika alarmları tetiklendiğinde, ilgili SNMP trap'leri yapılandırılan sunucuya otomatik olarak iletilir.

Kullanıcı Yönetimi

SecTrail CM, hem lokal kullanıcı yönetimi hem de LDAP/Active Directory entegrasyonu ile kurumsal kimlik yönetimi desteği sağlar. Bu sayede kullanıcılarınızı kolayca yönetebilir ve kurumsal dizin hizmetlerinizle entegre edebilirsiniz.

Kullanıcı Türleri

SecTrail CM iki farklı kullanıcı türünü destekler:

1. Lokal Kullanıcılar

Lokal kullanıcılar, SecTrail CM'in kendi veritabanında tanımlanan ve yönetilen kullanıcılardır.

Özellikler:

- SecTrail CM içerisinde oluşturulur ve yönetilir
- Kullanıcı adı, şifre ve e-posta adresi ile tanımlanır
- Rol bazlı yetkilendirme desteği
- API erişimi için özel kullanıcı oluşturma imkanı

2. LDAP/Active Directory Kullanıcıları

Kurumsal Active Directory veya LDAP sunucularınızla entegre edilerek merkezi kimlik yönetimi sağlar.

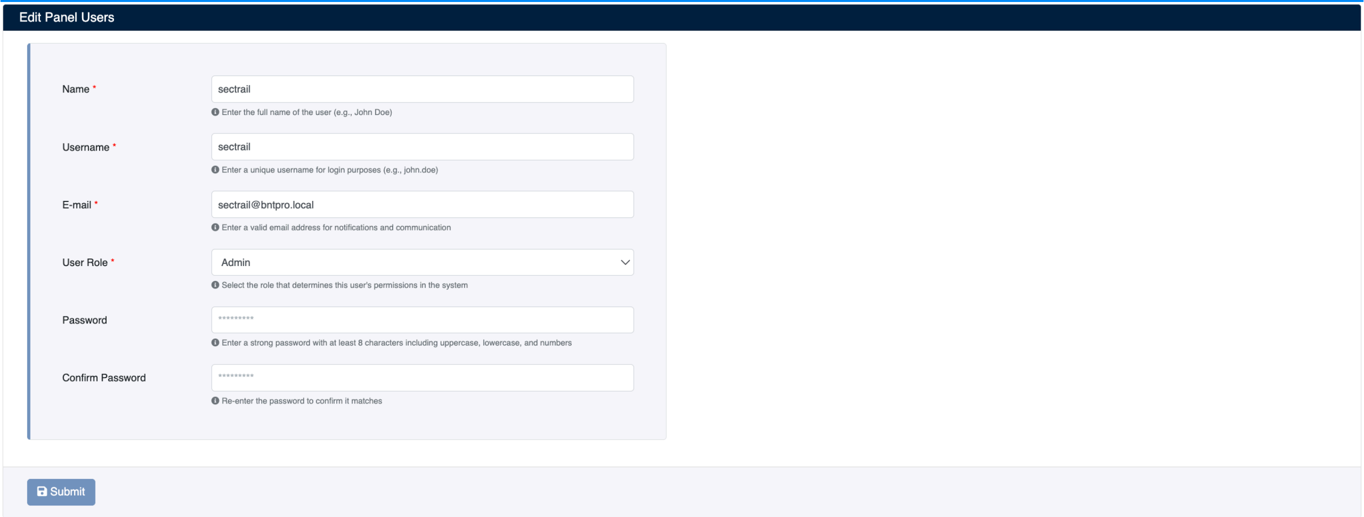
Özellikler:

- Merkezi kullanıcı yönetimi
- Mevcut kurumsal kimlik bilgileriyle giriş
- Grup bazlı yetkilendirme
- Kullanıcı bazlı yetkilendirme

Lokal Kullanıcı Yönetimi

Yeni Kullanıcı Oluşturma

1. **Users** menüsünden **Local Users** sekmesine gidin
2. **Create** butonuna tıklayın
3. **Add New Panel Users** formunda aşağıdaki bilgileri doldurun:



Form Alanları

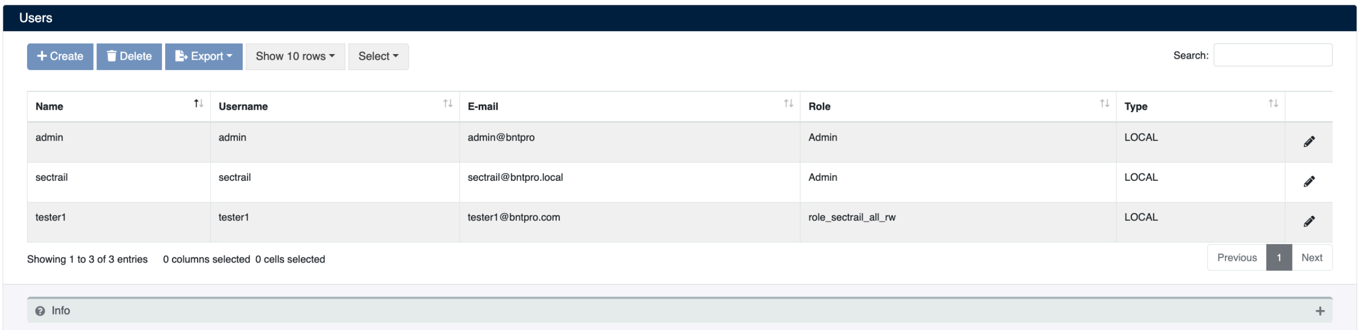
- **Name**: Kullanıcının adı ve soyadı
- **Username**: Sisteme giriş için kullanılacak kullanıcı adı (benzersiz olmalıdır)
- **E-mail**: Kullanıcının e-posta adresi (geçerli format: `name@mail.com`)
- **User Role**: Kullanıcıya atanacak rol
- **Password**: Kullanıcı şifresi
- **Confirm Password**: Şifre tekrarı

1. **Submit** butonuna tıklayarak kullanıcıyı oluşturun

> **TIP**
>
> API entegrasyonları için özel API rolüne sahip kullanıcılar oluşturun. Bu kullanıcılar sadece API erişimi için kullanılmalıdır.

Kullanıcı Listesi

Users ekranı, sistemdeki tüm kullanıcıları tablo formatında gösterir.



Bu ekranda:

Sütun Bilgileri:

- **Name**: Kullanıcının tam adı
- **Username**: Sisteme giriş için kullanılan kullanıcı adı
- **E-mail**: Kullanıcının e-posta adresi

- **Role**: Kullanıcıya atanmış rol

Kullanıcı İşlemleri

Her kullanıcı satırının sağ tarafında işlem butonları bulunur:

- **Edit ()**: Kullanıcı bilgilerini düzenleme
- **Delete ()**: Kullanıcıyı sistemden silme

> **WARNING**
>
> Aktif oturumu olan kullanıcıları silerken dikkatli olun. Kullanıcı silme işlemi geri alınamaz.

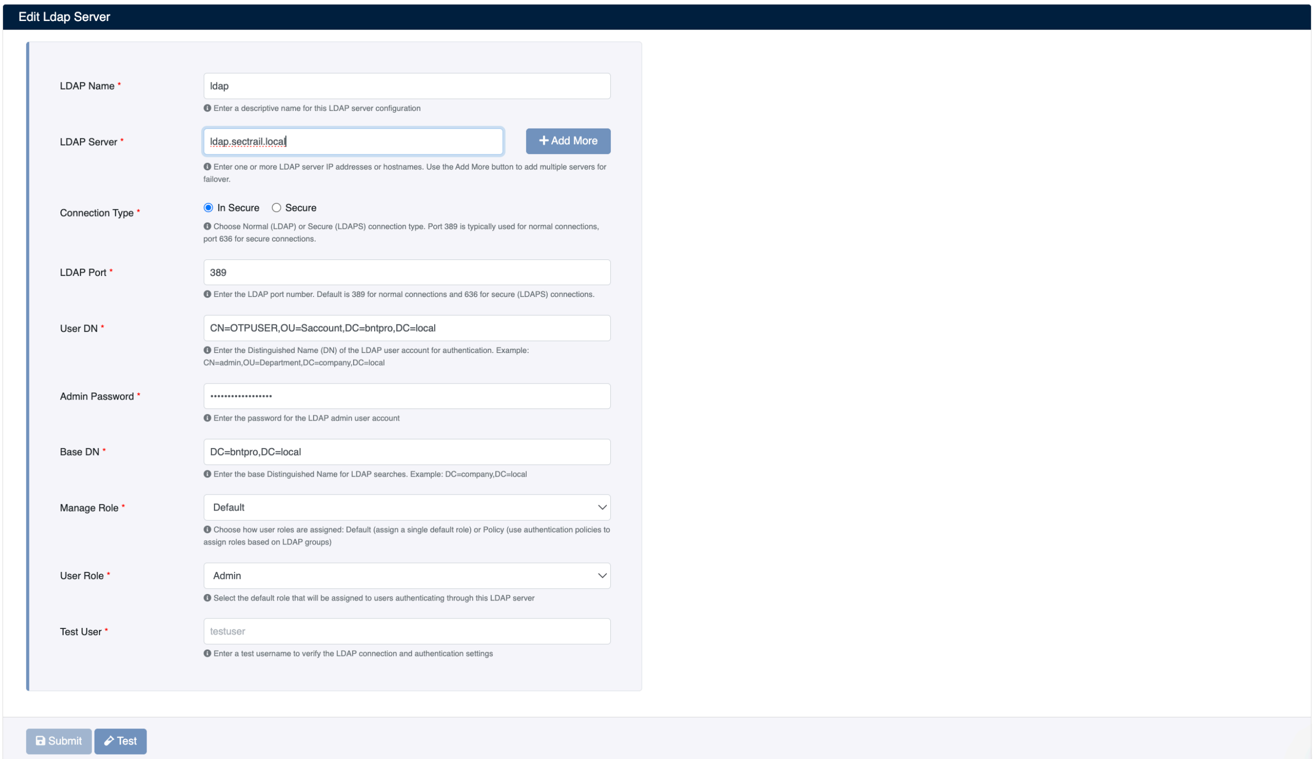
LDAP/Active Directory Entegrasyonu

SecTrail CM, Active Directory veya LDAP sunucularınızla entegre edilerek kurumsal kimlik yönetimi sağlar.

LDAP Sunucu Yapılandırması

Yeni LDAP Profili Oluşturma

Add New Ldap Server formu ile yeni bir LDAP/AD profili oluşturabilirsiniz.



Form Alanları

- **LDAP Name**: LDAP profilinin benzersiz adı
- **LDAP Server**: LDAP/AD sunucusunun IP adresi veya hostname. **Add More** butonu ile birden fazla sunucu eklenebilir
- **Connection Type**: Bağlantı türü seçimi
- **In Secure**: Şifrelenmemiş bağlantı (Port 389, test/geliştirme için)
- **Secure**: SSL/TLS şifreli bağlantı (Port 636, üretim için)

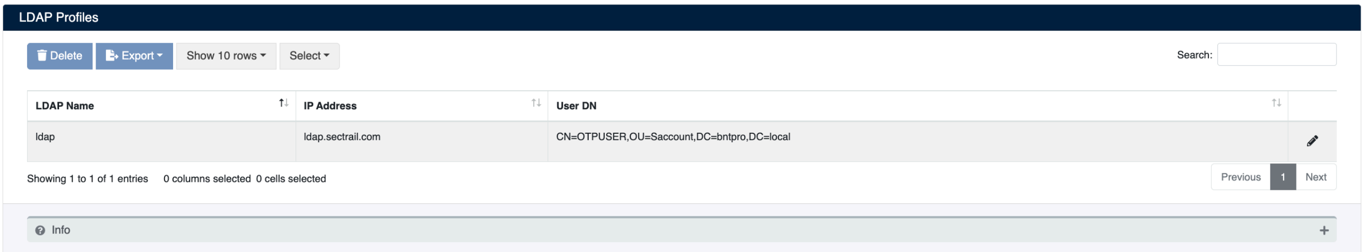
- **LDAP Port**: Bağlantı portu numarası (varsayılan: `389` veya `636`)
- **User DN**: LDAP bağlantısı için yönetici DN
- **Admin Password**: User DN'de belirtilen yöneticinin şifresi
- **Base DN**: Kullanıcı aramalarının başlayacağı temel DN
- **Manage Role**: LDAP yöneticileri için varsayılan rol
- **User Role**: LDAP kullanıcıları için varsayılan rol
- **Test User**: Bağlantıyı test etmek için kullanıcı adı

> **WARNING**
>
> LDAP bağlantılarınızı mutlaka test edin. Yanlış yapılandırma kullanıcı girişlerini engelleyebilir ve sisteme erişimi imkansız hale getirebilir.

> **TIP**
>
> İlk LDAP yapılandırmanızı yapmadan önce, sisteme giriş yapabileceğiniz bir lokal admin hesabınızın olduğundan emin olun. Böylece LDAP sorununda sisteme erişebilirsiniz.

LDAP Profil Yönetimi

LDAP Profiles tablosu, tanımlı tüm LDAP sunucularını gösterir.



Tablo Sütunları:

- **LDAP Name**: Profil adı
- **IP Address**: LDAP sunucu IP adresi
- **User DN**: Bağlantı için kullanılan yönetici DN

Profil İşlemleri:

Her profil satırının sağında iki işlem butonu bulunur:

- **Edit ()**: LDAP profil ayarlarını düzenleme
- Tüm yapılandırma alanlarını güncelleyebilirsiniz
- Sunucu adresi, port, DN bilgileri değiştirilebilir
- Şifreyi yeniden girmeniz gerekebilir
- **Delete ()**: LDAP profilini silme
- Silme işlemi geri alınamaz
- Bu profille ilişkili Remote Authentication Policy'ler etkilenebilir

> **CAUTION**

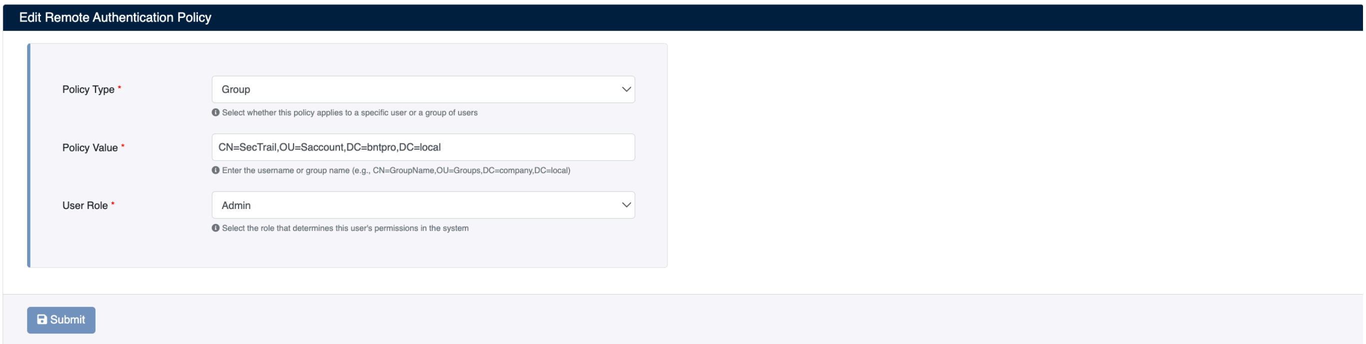
> Aktif olarak kullanılan bir LDAP profilini silmeden önce, o profil ile giriş yapan kullanıcıların başka bir yöntemle sisteme erişebildiğinden emin olun.

Uzak Kimlik Doğrulama Politikaları

Remote Authentication Policy, LDAP/AD kullanıcılarına grup veya kullanıcı bazında özel rol ataması yapmanızı sağlar. Bu sayede AD grup üyeliklerine göre farklı roller atayabilirsiniz.

Yeni Politika Oluşturma

Add New Remote Authentication Policy formu ile yeni bir politika oluşturabilirsiniz.

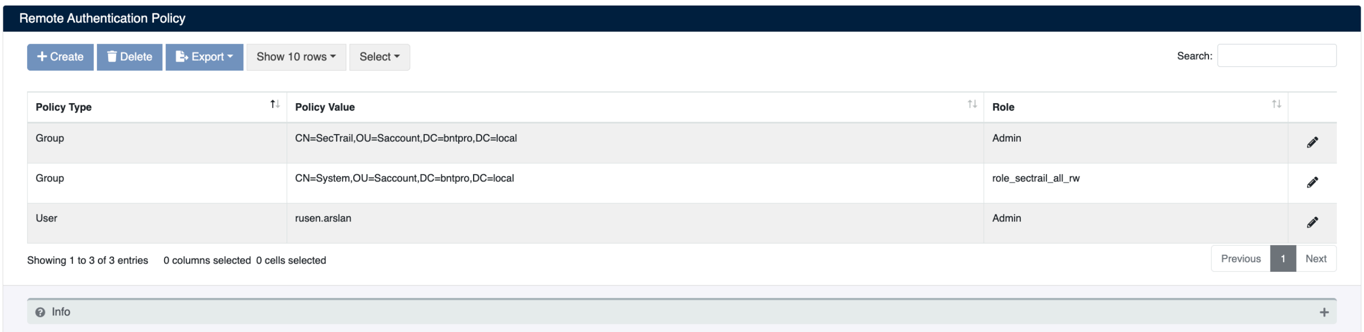


Form Alanları

- **Policy Type**: Politika türü
- **Group**: AD grup bazlı politika
- **User**: Bireysel kullanıcı bazlı politika
- **Policy Value**: Politika değeri (Policy Type'a göre değişir)
- **Group seçiliyse**: AD grup DN girilir
- **User seçiliyse**: Sadece kullanıcı adı girilir
- **User Role**: Bu politikaya uyan kullanıcılara atanacak rol

Politika Listesi

Remote Authentication Policy tablosu, tanımlı tüm politikaları gösterir.



Tablo Sütunları:

- **Policy Type**: Politika türü (`Group` veya `User`)
- **Policy Value**: Grup DN'i veya kullanıcı adı
- **Role**: Atanan rol

Politika İşlemleri:

Her politika satırının sağında iki işlem butonu bulunur:

- **Edit ()**: Politika ayarlarını düzenleme
- Policy type, value veya role değiştirilebilir
- Aktif kullanıcılar için dikkatli düzenleme yapın
- **Delete ()**: Politikayı silme
- Politika silindiğinde kullanıcılar LDAP profilindeki varsayılan role döner
- Aktif oturumlar etkilenmez, yeni girişlerde geçerli olur

Politika Öncelik Sırası

Bir kullanıcı için birden fazla politika geçerliyse, öncelik sırası şu şekildedir:

1. **User (Kullanıcı) Politikaları**: En yüksek öncelik
2. **Group (Grup) Politikaları**: İkinci öncelik

> **TIP**
>
> Mümkün olduğunca grup bazlı politikalar kullanın. Bu, yönetimi kolaylaştırır ve AD yapınızla uyumlu çalışır.

> **WARNING**
>
> Politika değişiklikleri yeni oturumlarda geçerli olur. Aktif kullanıcıların yeniden giriş yapması gerekebilir.

Kullanıcı Rolleri

SecTrail CM'de kullanıcılar rol tabanlı yetkilendirme ile yönetilir. Her kullanıcıya bir veya daha fazla rol atanabilir.

Varsayılan Roller

- **Admin**: Tam yönetici yetkisi
- **API**: API erişimi için özel rol

Roller ve izinleri hakkında detaylı bilgi için Rol ve İzinler bölümüne bakınız.

Rol ve İzinler

SecTrail CM, rol tabanlı erişim kontrolü (RBAC - Role-Based Access Control) kullanarak kullanıcı yetkilerini yönetir. Bu sistem sayesinde kullanıcılara iş tanımlarına uygun yetkiler atayabilir ve güvenli bir erişim yönetimi sağlayabilirsiniz.

Rol Tabanlı Erişim Kontrolü

Rol tabanlı erişim kontrolü, kullanıcılara doğrudan izin atamak yerine, roller aracılığıyla izin vermeyi sağlayan bir güvenlik modelidir.

Temel Kavramlar

- **Role**: Belirli izinlerin toplandığı mantıksal bir grup
- **İzin**: Sistemde gerçekleştirilebilecek belirli bir işlem yetkisi
- **Kullanıcı**: Bir veya daha fazla role atanmış sistem kullanıcısı

Avantajlar

- **Merkezi Yönetim**: İzinler rol seviyesinde yönetilir
- **Kolay Bakım**: Kullanıcı yetkileri rol değişiklikleriyle toplu olarak güncellenir
- **Güvenlik**: Minimum yetki ilkesinin uygulanmasını kolaylaştırır
- **Esneklik**: Organizasyonel yapıya uygun rol tanımları
- **Denetlenebilirlik**: Rol bazlı yetki kontrolü ve raporlama

Varsayılan Roller

SecTrail CM ile birlikte aşağıdaki varsayılan roller gelir:

Admin

Tam yönetici yetkisine sahip roldür. Sistem üzerinde tüm işlemleri gerçekleştirebilir.

Kullanım Alanları:

- Sistem yöneticileri
- Tam yetkili süper kullanıcılar
- İlk kurulum ve yapılandırma

API

API erişimi için özel olarak tasarlanmış roldür. REST API üzerinden işlem yapmak için kullanılır.

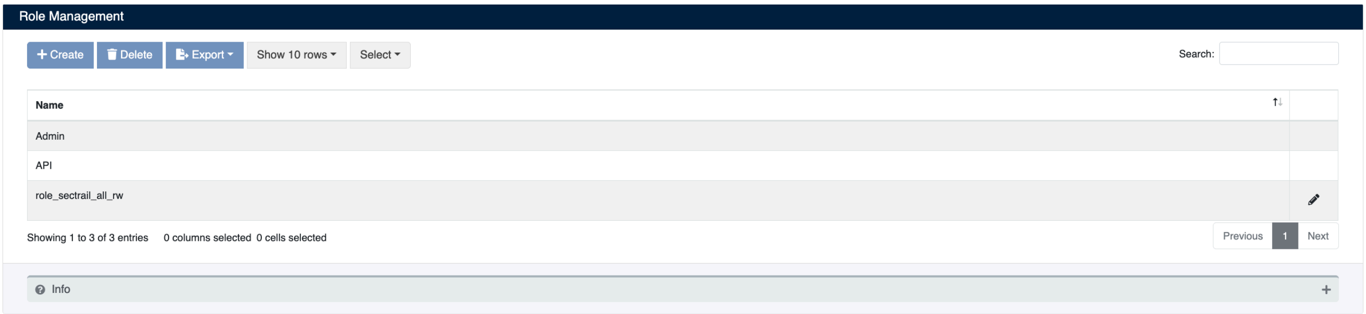
Kullanım Alanları:

- Sistem entegrasyonları
- Otomasyon scriptleri
- Üçüncü taraf uygulamalar

Rol Yönetimi

Rol Listesi Görüntüleme

Role Management ekranı, sistemdeki tüm rolleri basit bir tablo formatında gösterir.

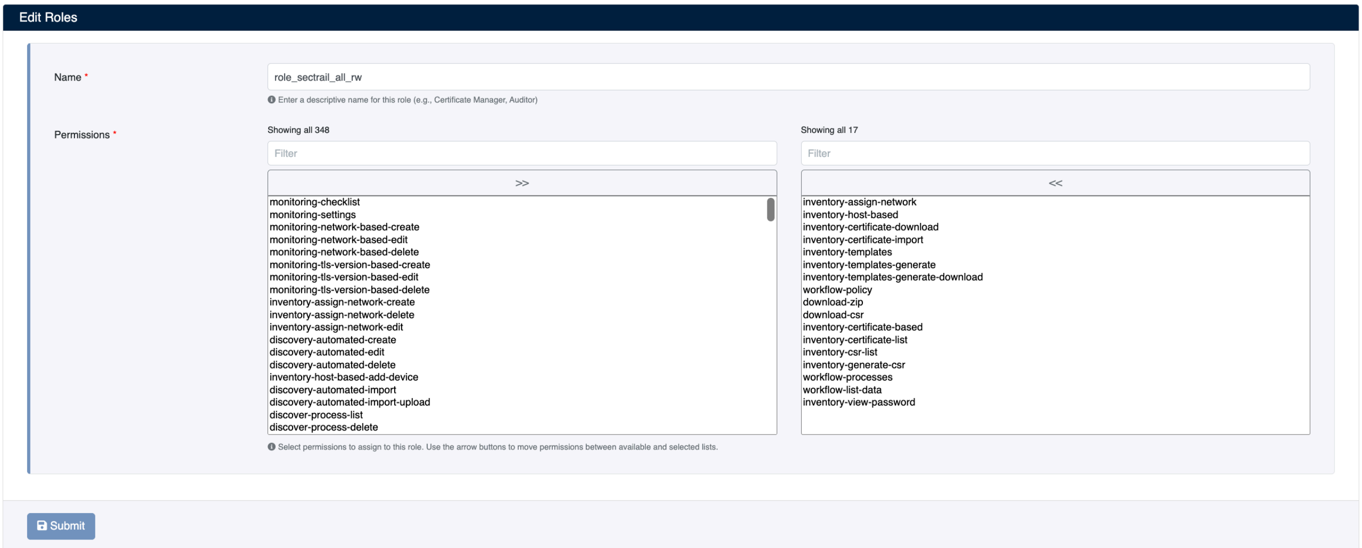


Tablo Sütunları:

- **Name**: Rol adı
- **Actions**: İşlem butonları

Yeni Rol Oluşturma

Add New Roles formu ile yeni bir rol oluşturabilir ve bu role izinler atayabilirsiniz.



Form Alanları

- **Name**: Rolün benzersiz adı (küçük harf ve tire karakteri önerilir, örn: `sign`, `certificate-viewer`, `deployment-operator`)
- **Permissions**: İki panelli transfer kutusu ile izin seçimi yapılır

İzin Seçim Arayüzü:

Form, sol ve sağ olmak üzere iki panel içerir:

- **Sol Panel **: Sistemde mevcut tüm izinleri gösterir. Filter kutusu ile izinleri hızlıca arayabilirsiniz.
- **Transfer Butonları**: `>>` butonu ile sol panelden sağ panele, `<<` butonu ile sağ panelden sol panele izin taşıyabilirsiniz

- **Sağ Panel (Selected Permissions)**: Role atanacak izinlerin listesini gösterir

> **FİLTRELEME KULLANIMI**
>
> - `sign` -> İmzalama işlemleri
> - `delete` -> Silme yetkilerini bul
> - `create` -> Oluşturma yetkilerini bul
> - `edit` -> Düzenleme yetkilerini bul
> - `download` -> İndirme yetkilerini bul

Rol Düzenleme

1. Rol listesinde düzenlemek istediğiniz rolün yanındaki **Edit ()** butonuna tıklayın
2. Rol adını ve izinleri güncelleyin
3. **Submit** butonuna tıklayarak değişiklikleri kaydedin

Rol Silme

1. Rol listesinde silmek istediğiniz rolün yanındaki **Delete ()** butonuna tıklayın
2. Silme işlemini onaylayın

> **WARNING**
>
> Aktif kullanıcılara atanmış rolleri silmeden önce, bu kullanıcılara başka roller atadığınızdan emin olun. Aksi takdirde kullanıcılar sisteme erişemeyebilir.

Kullanıcılara Rol Atama

Rolleri oluşturduktan sonra, kullanıcılara bu rolleri atamanız gerekir.

Lokal Kullanıcılar

1. **Users** > **Local Users** bölümüne gidin
2. Kullanıcı oluştururken veya düzenlerken **User Role** alanından ilgili rolü seçin
3. Değişiklikleri kaydedin

LDAP/AD Kullanıcıları

LDAP veya Active Directory kullanıcıları için roller, Remote Authentication Policy üzerinden atanır:

1. **Remote Authentication Policy** bölümüne gidin
2. Grup veya kullanıcı bazlı politika oluşturun
3. **User Role** alanında atamak istediğiniz rolü seçin

Detaylı bilgi için Kullanıcı Yönetimi bölümüne bakınız.

API Dokümantasyonu

SecTrail Certificate Manager, sertifika yönetimi işlemlerinizi otomatikleştirmenize olanak tanıyan güçlü bir RESTful API sunar.

Genel Bakış

SecTrail CM API'si, sertifika yaşam döngüsü yönetimi için kapsamlı endpoint'ler sağlar. API'yi kullanarak:

- Sertifika imzalama işlemleri gerçekleştirebilir
- Sertifika yükleme ve yönetimi yapabilir
- Keşif listelerini toplu olarak yönetebilir
- Sertifika envanterini sorgulayabilirsiniz

API Dokümantasyon Arayüzü

SecTrail CM, tüm API uç noktalarını keşfetmeniz ve test etmeniz için etkileşimli bir Swagger/OpenAPI dokümantasyon arayüzü sunar:

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

Bu arayüz üzerinden:

- Tüm mevcut uç noktaları görüntüleyebilir
- İstek/Yanıt şemalarını inceleyebilir
- API çağrılarını doğrudan test edebilirsiniz

Kimlik Doğrulama

API'yi kullanmaya başlamadan önce kimlik doğrulama belirteci (Bearer token) ile kimlik doğrulaması yapmanız gerekmektedir. Detaylı bilgi için Kimlik Doğrulama bölümüne bakınız.

Başlarken

1. API rolüne sahip bir kullanıcı oluşturun
2. Kimlik doğrulama belirteci alın
3. API uç noktalarını kullanmaya başlayın

Tüm uç noktalar ve kullanım örnekleri için Uç Noktalar sayfasını inceleyebilirsiniz.

Kimlik Doğrulama

SecTrail CM API'si, kimlik doğrulama belirteci (Bearer token) tabanlı kimlik doğrulama kullanır. API uç noktalarını kullanabilmek için öncelikle bir erişim belirteci almanız gerekmektedir.

API Kullanıcısı Oluşturma

API'yi kullanmaya başlamadan önce, API rolüne sahip bir kullanıcı oluşturmalısınız:

Adımlar

1. SecTrail CM arayüzünde **Users** > **Local Users** bölümüne gidin
2. Yeni bir kullanıcı oluşturun
3. Kullanıcıya **API** rolünü atayın
4. Kullanıcı adı ve şifreyi kaydedin

> **TIP**
>
> API kullanıcıları için güçlü şifreler kullanın ve bu kimlik bilgilerini güvenli bir şekilde saklayın.

Kimlik Doğrulama Belirteci Alma

API kullanıcınızı oluşturduktan sonra, bir kimlik doğrulama belirteci almanız gerekmektedir.

Uç Nokta

```
POST /api/login
```

İstek Gövdesi

```
{
 "username": "api-user",
 "password": "your-secure-password"
}
```

Yanıt

```
{
 "user": "apiuser",
 "access_token": "eyJ0eXAiOiJKV1QiLCJhbGci..."
}
```

Örnek cURL Komutu

```
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"
```


Belirteç Kullanımı

Aldığınız kimlik doğrulama belirtecini, tüm API isteklerinizde `Authorization` başlığında kullanmalısınız:

```
curl -X GET https://your-sectrailcm-server/api/endpoint \
 -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."
```

Belirteç Süresi

- Kimlik doğrulama belirteçleri belirli bir süre sonra geçerliliğini kaybeder
- Belirteç süreniz dolduğunda, yeni bir belirteç almanız gerekir
- Yanıtta kullanıcı adı (`user`) ve erişim belirteci (`access_token`) bilgilerini alırsınız

Güvenlik Önerileri

- Belirteçlerinizi asla kaynak kodunuzda saklamayın
- Ortam değişkenleri veya güvenli bir kasa (vault) kullanın
- HTTPS kullanarak tüm API isteklerini güvenli hale getirin
- Belirteçleri düzenli olarak yenileyin
- API kullanıcılarına sadece gerekli yetkileri verin

API Uç Noktaları

SecTrail CM API'si, sertifika yönetimi işlemlerinizi otomatikleştirmek için çeşitli uç noktalar sunar. Tüm uç noktaların detaylı dokümantasyonu için Swagger arayüzünü kullanabilirsiniz:

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

Temel Kullanım Alanları

1. Sertifika İmzalama

API üzerinden çeşitli formatlarda sertifika imzalama işlemleri gerçekleştirebilirsiniz:

Desteklenen İmzalama Türleri:

- CSR (Certificate Signing Request) imzalama
- Self-Signed sertifika oluşturma
- Template tabanlı sertifika üretimi
- JKS (Java KeyStore) formatında sertifika oluşturma

Uç Nokta:

```
POST /api/generate
```

> **INFO**
>
> Sertifika imzalama işlemleri için `requestType` parametresi kullanılarak işlem türü belirlenir. Detaylı parametre listesi için Swagger dokümantasyonunu inceleyiniz.

2. Sertifika Yükleme ve Dağıtım

API üzerinden sertifikalarınızı hedef sunuculara ve cihazlara otomatik olarak dağıtabilirsiniz:

Özellikler:

- Çoklu hedef cihaza dağıtım (F5, Apache, Nginx, IIS, vb.)
- Virtual host bazlı dağıtım
- Zamanlı dağıtım desteği
- Başarısız dağıtımlar için retry mekanizması
- Dağıtım durumu sorgulama ve izleme

Uç Nokta:

```
POST /api/deployment
```

3. Keşif Listesi Yönetimi

Keşif listelerinizi API üzerinden toplu olarak yönetebilirsiniz:

Özellikler:

- Keşif listesi oluşturma
- Toplu domain/IP ekleme
- Keşif sonuçlarını sorgulama
- Keşif planlarını zamanlama

Uç Nokta:

```
POST /api/discoverList
```

4. Sertifika Envanteri

Envanterdeki sertifikaları sorgulayabilir ve bilgilerini alabilirsiniz:

Özellikler:

- Toplu sertifika listesi alma
- Sertifika detaylarını görüntüleme
- Sertifika durumu sorgulama

Uç Nokta:

```
POST /api/getCertificates
```

API Kullanım Örnekleri

Kimlik Doğrulama

Tüm API isteklerinde kimlik doğrulama belirteci kullanmanız gerekmektedir:

```
curl -X POST https://your-sectrailcm-server/api/endpoint \
 -H "Authorization: Bearer YOUR_TOKEN" \
 -H "Content-Type: application/json" \
 -d '{"key": "value"}'
```

Hata Yönetimi

API, standart HTTP durum kodları kullanır:

- `200 OK` - İstek başarılı
- `201 Created` - Kaynak oluşturuldu
- `400 Bad Request` - Geçersiz istek
- `401 Unauthorized` - Kimlik doğrulama hatası
- `403 Forbidden` - Yetki hatası
- `404 Not Found` - Kaynak bulunamadı
- `500 Internal Server Error` - Sunucu hatası

Swagger Dokümantasyonu

Tüm uç noktaların detaylı açıklamaları, parametre tanımları ve örnek istek/yanıt yapıları için Swagger arayüzünü kullanın:

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

Swagger arayüzü üzerinden:

- Tüm uç noktaları keşfedebilir
- İstek/Yanıt şemalarını görüntüleyebilir
- API çağrılarını etkileşimli olarak test edebilirsiniz

> **TIP**
>
> Swagger dokümantasyonunda "Try it out" özelliğini kullanarak API çağrılarınızı doğrudan test edebilir ve sonuçları görebilirsiniz.