

# Sangfor NGAF

## Best Practices for Scenarios\_NGAF Correlate with Cloud Endpoint Secure to Anti Proxy Tools

<b>Product Version</b>	8.0.39
<b>Document Version</b>	1.0
<b>Released on</b>	Sept. 08, 2021



Hak Cipta © Sangfor Technologies Inc. 2021. Semua hak dilindungi undang-undang. Kecuali yang dinyatakan lain atau yang disahkan, Sangfor Technologies Inc. (selanjutnya disebut sebagai "Sangfor") dan afiliasinya memiliki semua hak kekayaan intelektual, termasuk namun tidak terbatas pada hak cipta, merek dagang, paten dan rahasia dagang, dan hak terkait atas teks, gambar, lukisan, foto, audio, video, grafik, warna, dan tata letak sebagaimana disajikan dalam atau terkait dengan dokumen ini dan konten yang ada di dalamnya. Tanpa persetujuan tertulis sebelumnya dari Sangfor, dokumen dan konten yang ada di dalamnya tidak boleh direproduksi, ditransmisikan, diadaptasi, dimodifikasi atau ditampilkan atau didistribusikan dengan cara lain apa pun untuk tujuan apa pun.

## **Sangkalan**

Produk, layanan, atau fitur yang dijelaskan dalam dokumen ini, secara keseluruhan atau sebagian, mungkin tidak tercakup dalam lingkup pembelian anda atau lingkup penggunaannya. Produk, layanan, atau fitur yang anda beli harus tunduk pada kontrak komersial dan persyaratan yang disepakati oleh anda dan Sangfor. Kecuali ditentukan lain dalam kontrak, Sangfor menyangkal semua jaminan, tersurat maupun tersirat, untuk isi dokumen ini.

Karena peningkatan produk atau alasan lain, isi dokumen ini akan diperbarui dari waktu ke waktu. Kecuali jika disetujui lain, dokumen ini digunakan untuk referensi saja, dan semua pernyataan, informasi, dan rekomendasi di dalamnya bukan merupakan jaminan tersurat atau tersirat.

## Dukungan teknis

Untuk dukungan teknis, silakan kunjungi: <https://www.sangfor.com/en/about-us/contact-us/technical-support>

Kirim informasi tentang kesalahan atau masalah terkait produk ke [tech.support@sangfor.com](mailto:tech.support@sangfor.com).

## Log Perubahan

Tanggal	Deskripsi Perubahan
08 Sep 2021	Ini adalah rilis pertama dari dokumen ini.

## Daftar Isi

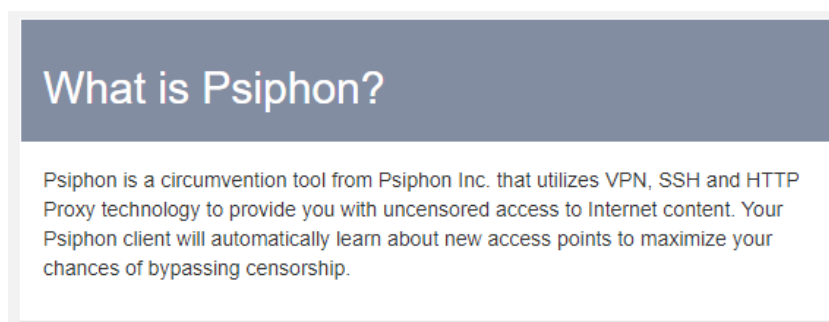
Change Log .....	2
1 Scenario .....	错误!未定义书签。
1.1 Scenario Introduction.....	错误!未定义书签。
1.2 Scenario Applicable Conditions .....	错误!未定义书签。
1.3 Topo .....	4
1.4 Testing Condition .....	错误!未定义书签。
2 Best Practice .....	错误!未定义书签。
2.1 Add Cloud Endpoint Secure License on Platform-X.....	错误!未定义书签。
2.2 Enable Device Integration Option in Cloud Endpoint Secure .....	错误!未定义书签。
2.3 Connect NGAF to Cloud Endpoint Secure .....	错误!未定义书签。
2.4 Configure App Control Policy in NGAF.....	错误!未定义书签。
2.5 Test Policy Effect .....	错误!未定义书签。
3 Precaution.....	错误!未定义书签。

# 1 Skenario

## 1.1 Pengenalan Skenario

Banyak para pengguna menggunakan alat VPN untuk mengakses aplikasi yang tidak diotorisasi oleh administrator jaringan, seperti berbagai situs porno dan situs tidak jelas lainnya. Selain itu, penggunaan alat VPN dapat menyebabkan kebocoran informasi dan perilaku yang tidak dilakukan proses audit. Untuk administrator jaringan, alat VPN ini perlu dibuka blokirnya.

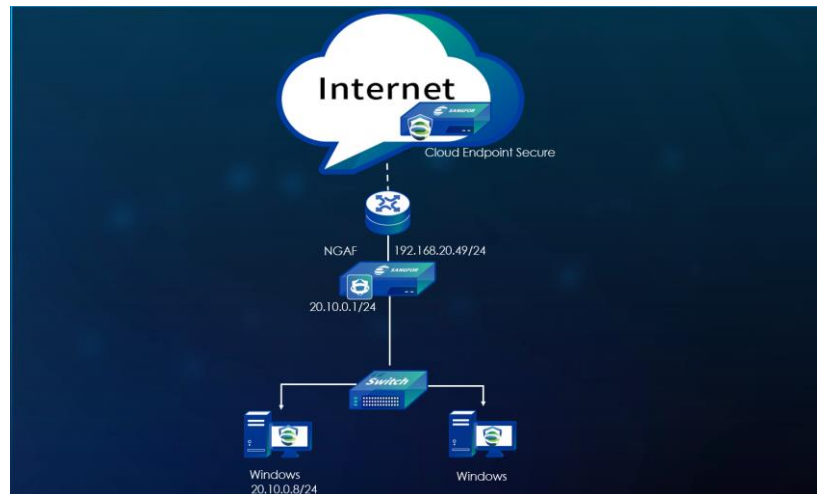
Secara tradisional, metode anti-proxy yang umum adalah membatasi nama domain dan IP yang terkait dengan alat proxy dalam dimensi lalu lintas jaringan, tetapi efeknya biasanya minimal. Seperti yang diklaim oleh beberapa alat perangkat lunak proxy, lalu lintas disamarkan sebagai SSH standar, Protokol HTTP, dan protokol DNS untuk melewati deteksi perangkat lunak keamanan, dan beberapa perangkat lunak proxy menempatkan server di cloud publik, membatasi IP-nya akan menyebabkan situs web normal dibatasi. Oleh karena itu, diperlukan cara yang lebih baik untuk mencegah alat proxy, yaitu melalui tautan NGAF dan ES, yang secara langsung membatasi pengoperasian alat proxy terkait proses.



## 1.2 Skenario Kondisi yang Berlaku

1. Pelanggan ingin menggunakan NGAF dan Endpoint Secure untuk membatasi Alat VPN
2. Pelanggan ingin menggunakan Endpoint Secure di cloud untuk mengurangi beban kerja pemeliharaan

## 1.3 Topologi



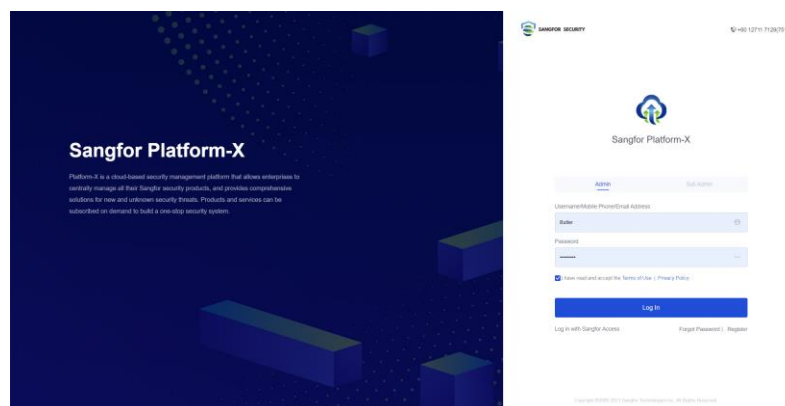
## 1.4 Kondisi Pengujian

1. Versi NGAF harus 8.0.39 dan yang lebih terbaru.

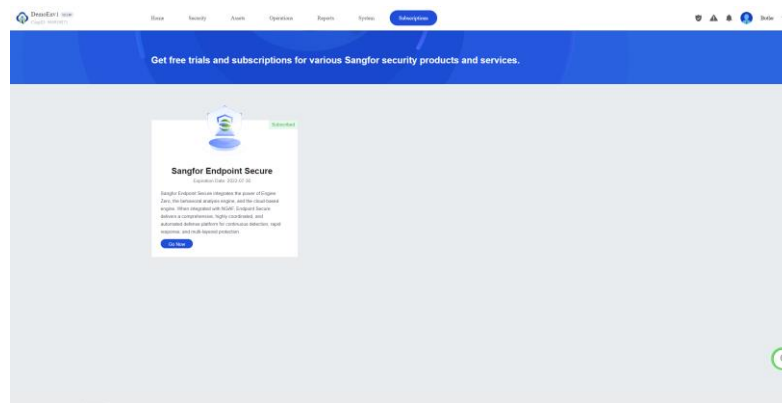
## 2 Praktik Terbaik

### 2.1 Tambahkan Lisensi Aman Cloud Endpoint di Platform-X

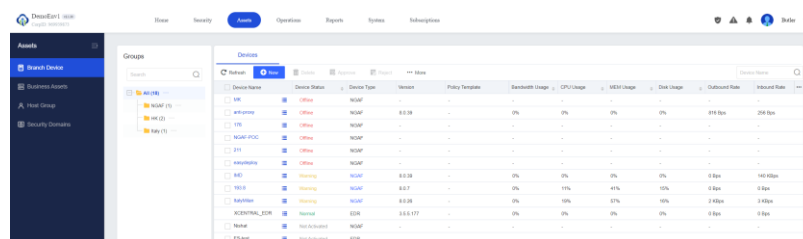
1. Hubungi penyedia layanan lokal anda untuk menambahkan lisensi Cloud Endpoint Secure ke Platform-X. Akses <https://x.sangfor.com/> dan masuk.



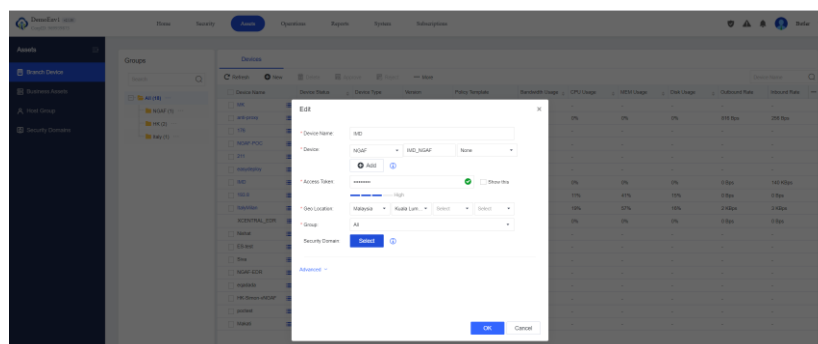
2. Jika lisensi Cloud Endpoint Secure telah berhasil ditambahkan ke Platform-X, itu akan menunjukkan bahwa modul Cloud Endpoint Secure telah menjadi langganan.



3. Membuat cabang perangkat untuk memungkinkan perangkat NGAF melakukan akses.



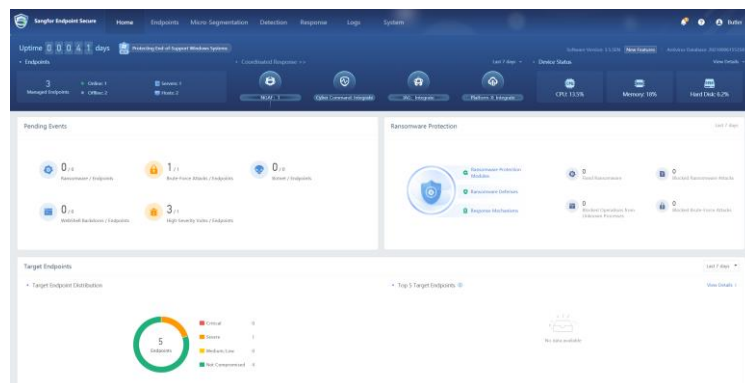
4. Mengisi nama perangkat akses sesuai dengan kebutuhannya, dan melakukan konfigurasi kata sandi akses dan area tempat perangkat berada.



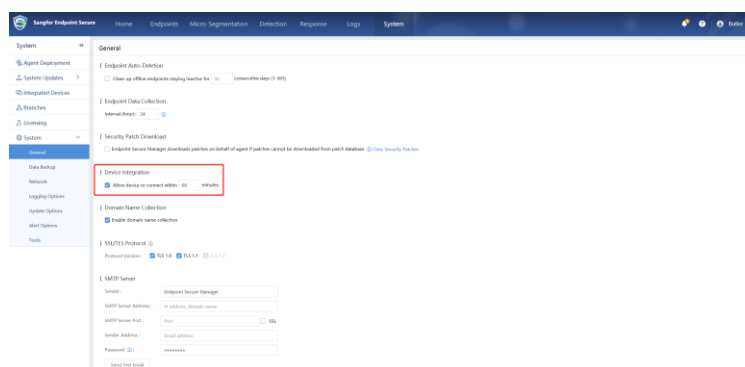
## 2.2 Mengaktifkan Opsi Integrasi Perangkat di Cloud Endpoint Secure

1. Untuk alasan keamanan, Endpoint Secure tidak mendukung akan akses perangkat otomatis secara default. Izin akses perangkat harus diaktifkan sebelum melakukan akses perangkat.



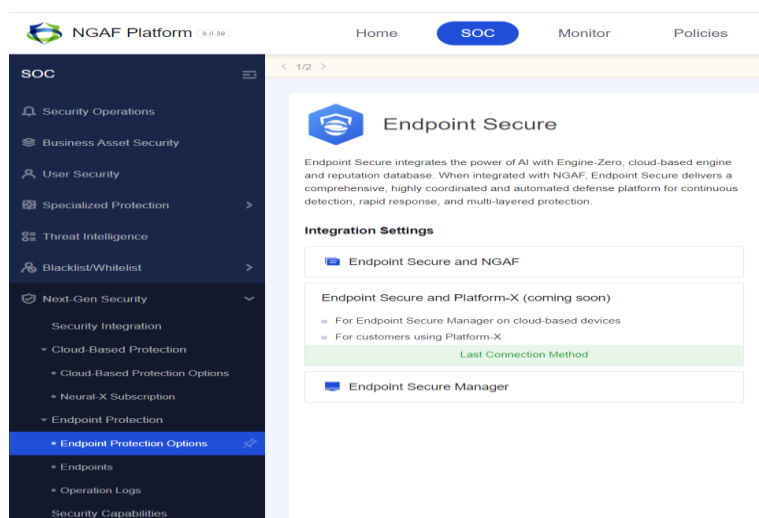


## 2. Mengaktifkan opsi Integrasi Perangkat.

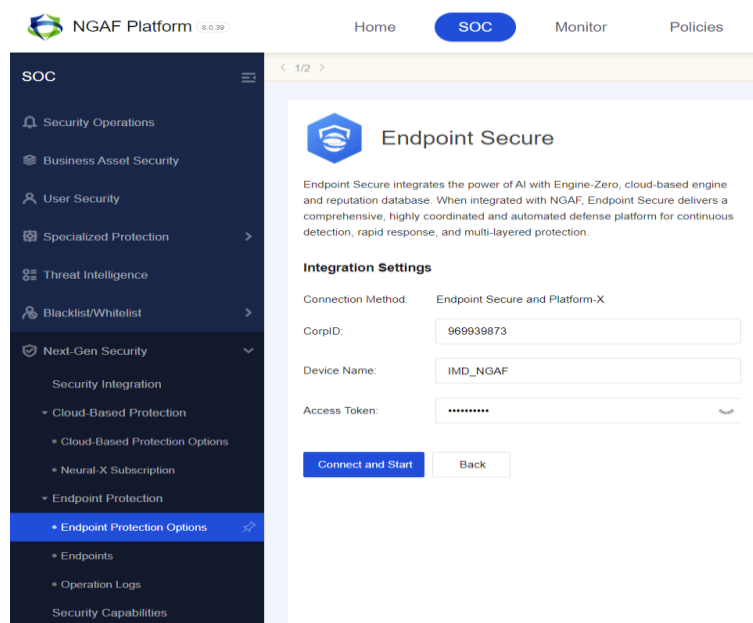


## 2.3 Menghubungkan NGAF ke Cloud Endpoint Secure

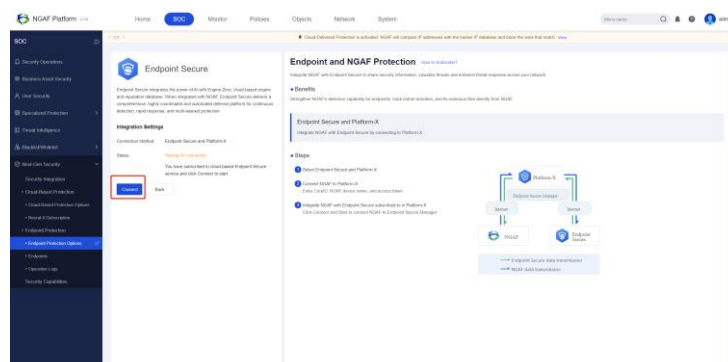
1. Masuk kedalam SOC Endpoint Secure Protection Path, dan memilih Endpoint Secure dan fungsi Platform-X, lalu mengisi password dan corporate ID yang telah kita konfigurasi sebelumnya.



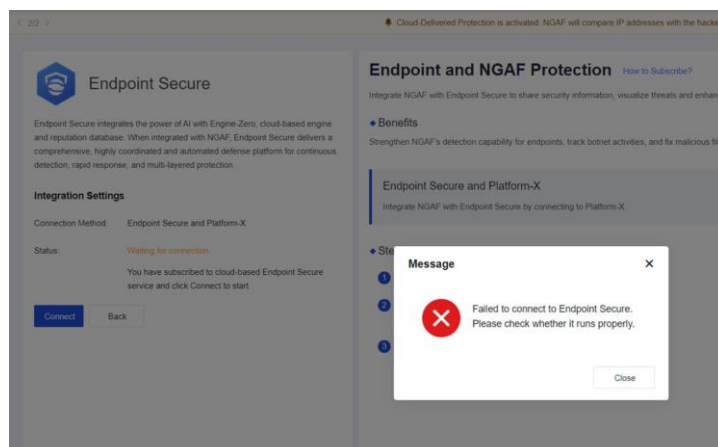
## 2. Mengisi nama perangkat dan mengisi informasi lainnya.



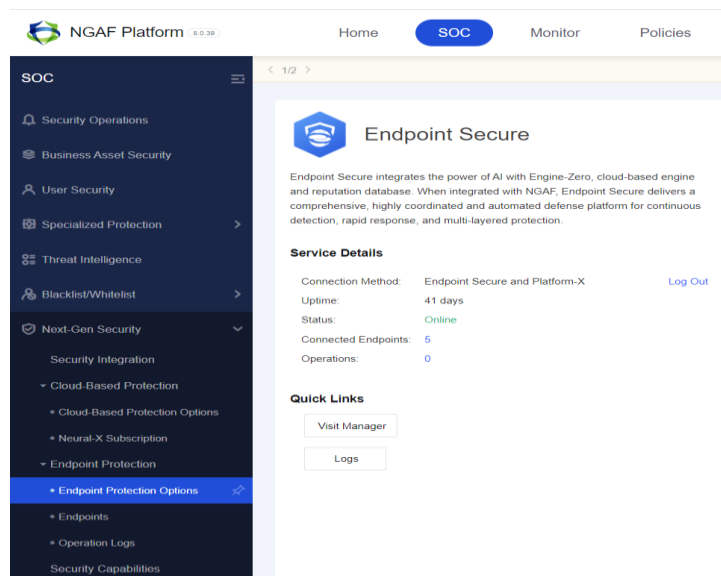
## 3. Melakukan Klik Menhubungkan.



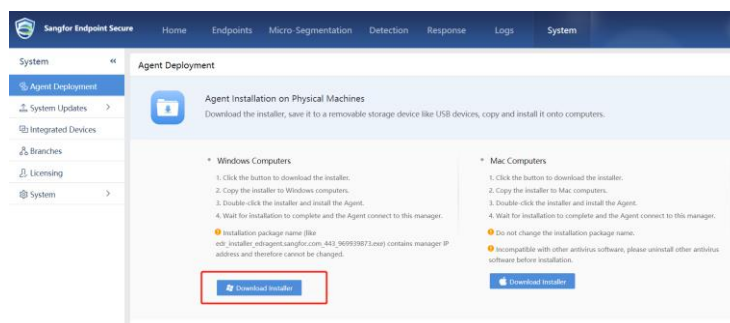
Catatan: Jika anda tidak melakukan pengaktifan Opsi Integrasi Perangkat, saat anda melakukan akses Cloud Endpoint Secure di NGAF, anda akan mendapatkan pesan kesalahan berikut.



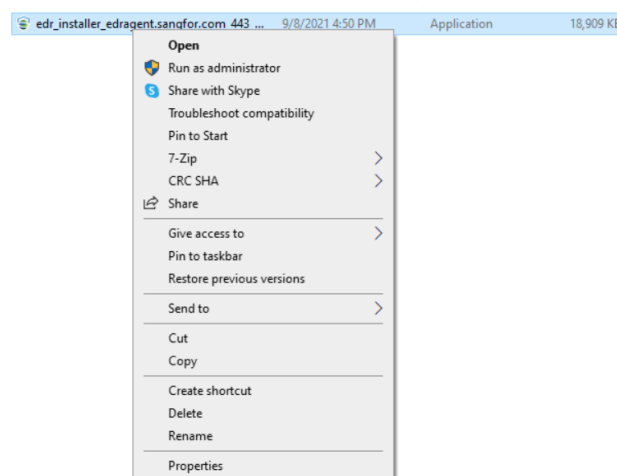
4. Setelah NGAF berhasil terhubung ke Cloud Endpoint Secure, anda dapat melihat status koneksi dan titik akhir daring.



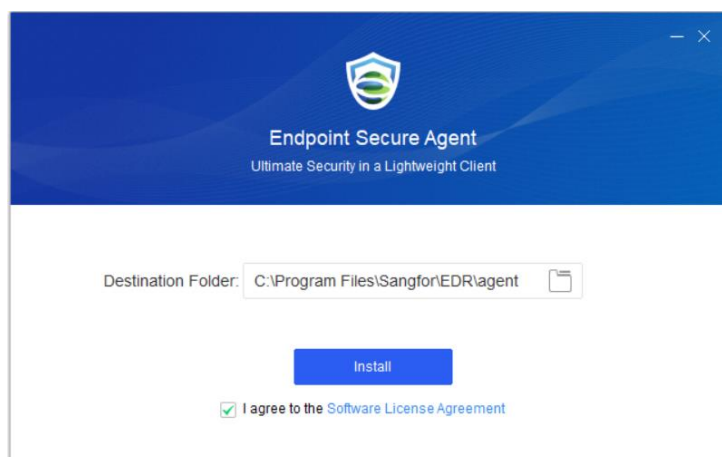
5. Masuk Cloud Endpoint Secure dan mengunduh Endpoint Secure Agent.



6. Instal Endpoint Secure Agent dengan izin akses administrator.

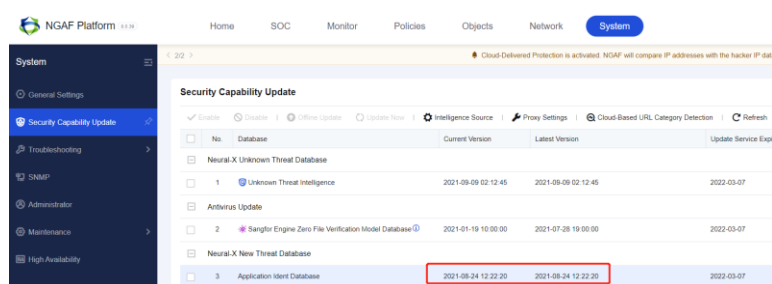


7. Klik instal untuk mengunduh sumber daya dan menunggu proses pemasangannya.

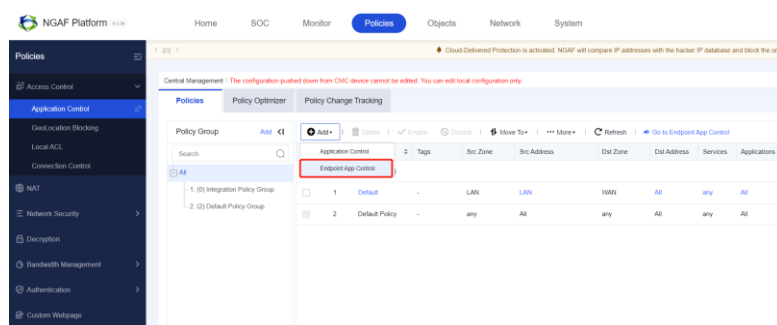


## 2.4 Melakukan Konfigurasi Kebijakan Kontrol Aplikasi di NGAF

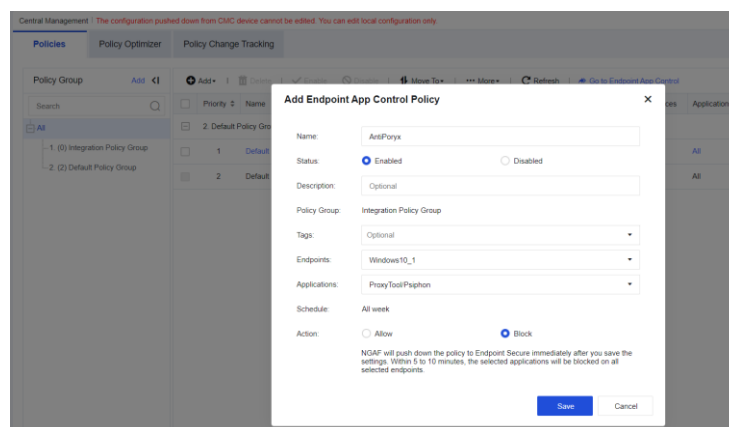
1. Periksa apakah aturan basis data adalah versi terbaru.



2. Membuka jalur Access Control Application Control, dan menambahkan Endpoint App Control Policy.

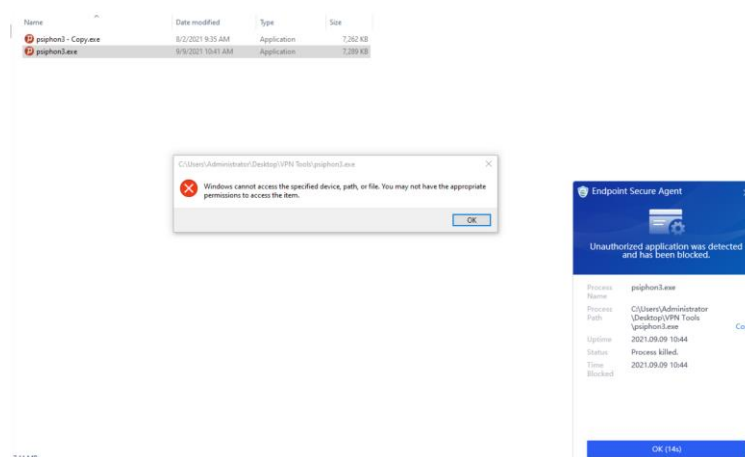


3. Pilih host sumber yang ingin anda batasi dengan menggunakan alat proxy, pastikan untuk mengatur tindakan sebagai pembatasan.

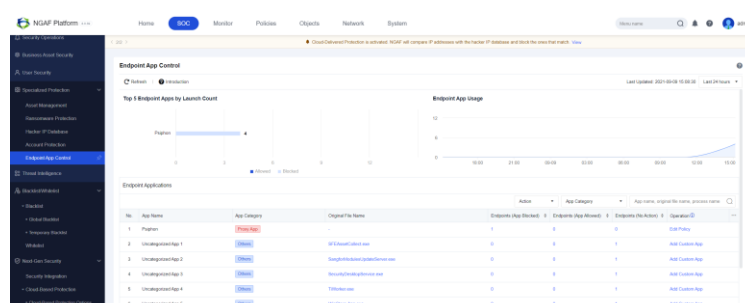


## 2.5 Menguji Efek Kebijakan

1. Setelah kebijakan dikeluarkan, anda dapat memastikan bahwa ketika anda menjalankan alat VPN secara manual, alat VPN tidak dapat berjalan, dan Endpoint Secure Agent meminta kotak peringatan.



2. Membuka halaman SOC Endpoint App Control, anda dapat melihat statistik informasi blok terbaru.



## 3 Tindakan pencegahan

1. Jumlah maksimum endpoint yang didukung oleh perangkat NGAF dengan

memori 4G adalah 1000. Jumlah maksimum endpoint yang didukung oleh perangkat NGAF dengan memori lebih dari 4G adalah 2000. Jika jumlah sebenarnya dari endpoint melebihi 2000, NGAF hanya akan mengeluarkan kebijakan hingga 2000 dari mereka. Ini akan menyebabkan beberapa endpoint gagal mengeluarkan kebijakan.

2. Saat NGAF mengeluarkan kebijakan, harap pastikan bahwa komunikasi antara NGAF dan Endpoint Secure Manager adalah normal, jika tidak, kebijakan tidak dapat diterbitkan.

3. Data di Endpoint App Control di SOC diperbarui setiap 5-10 menit, bukan real-time.

4. NGAF dan Endpoint Secure Manager akan mempertahankan detak jantung untuk menentukan bahwa komunikasi antara kedua pihak adalah normal, tetapi mungkin ada beberapa situasi ekstrem, seperti kebijakan penerbitan NGAF untuk Endpoint Secure Manager, Endpoint Secure Manager, dan komunikasi Endpoint Secure Agent yang tidak normal, yang mengakibatkan jika kebijakan Send to Endpoint Secure Agent gagal, maka Endpoint Secure Manager akan menggunakan kebijakan yang disembunyikan secara lokal untuk mengontrol alat VPN.



**SANGFOR**

