SANGFOR

Praktik Terbaik Keamanan Endpoint untuk Skenario Panduan Implementasi Kebijakan Keamanan Endpoint Secure untuk Server

Versi 3.2.22

Catatan Perubahan

Tanggal	Deskripsi Perubahan
16 Mar 2021	Dokumen diterbikan
17 Mei 2021	Dokumen diperbaharui

DAFTAR ISI

Bagian 1 Skenario

Bagian 2 Gambaran

Dokument ini sesuai dengan Endpoint Secure sebagai panduan untuk implementasi Endpoint Secure security policy dengan tujuan untuk melindungi keamanan server. Dokumen ini terdiri dari dua bagian:
Mengidentifikasi resiko keamanan server dan mengimplementasikan security policy pada server. Mengidentifikasikan resiko keamanan server dapat memandu pengguna bagaimana cara mengidentifikasi resiko keamanan klien lebih awal, membuat pengguna mewaspadai resiko keamanan server dan dampaknya terhadap server, dan memandu pengguna untuk menangani resiko keamanan saat mengimplementasikan keamanan server. Security policy nya merujuk kepada policy mana yang seharusnya diatur oleh Endpoint Secure dan bagaimana untuk mengatur security untuk memastikan keamanan dari server.

Bagian 3 Mengidentifikasi Resiko Keamanan Server

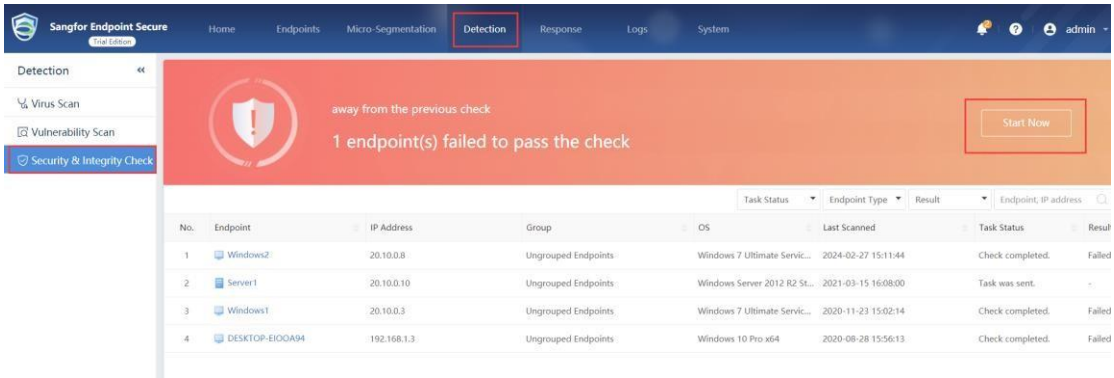
Mengidentifikasi resiko keamanan pada server merupakan cara untuk memandu pengguna untuk mengidentifikasikan resiko keamanan klien lebih awal, membuat pengguna menyadari resiko keamanan dan dampaknya terhadap server, dan memandu pengguna untuk menangani resiko keamanan. Bagian ini dapat memandu pengguna untuk mengidentifikasikan resiko keamanan lebih awal dan cara untuk menangani nya dengan tiga cara: pemeriksaan awal, pemeriksaan kerentanan, dan penghapusan virus. Ingat jika semakin banyak server, direkomendasikan untuk memilih 1 atau 2 server untuk memandu pengguna bagaimana cara mengidentifikasi resiko keamanan dan bagaimana cara untuk menangani mereka.

3.1 Pemeriksaan Keamanan & Integritas

Pemeriksaan keamanan & Integritas adalah proses pemeriksaan yang wajib untuk sistem windows dan linux sesuai dengan persyaratan keamanan yang diwajibkan, untuk membantu menemukan terminal yang tidak sesuai dan item yang tidak sesuai di intranet, dan memberikan saran perbaikan.

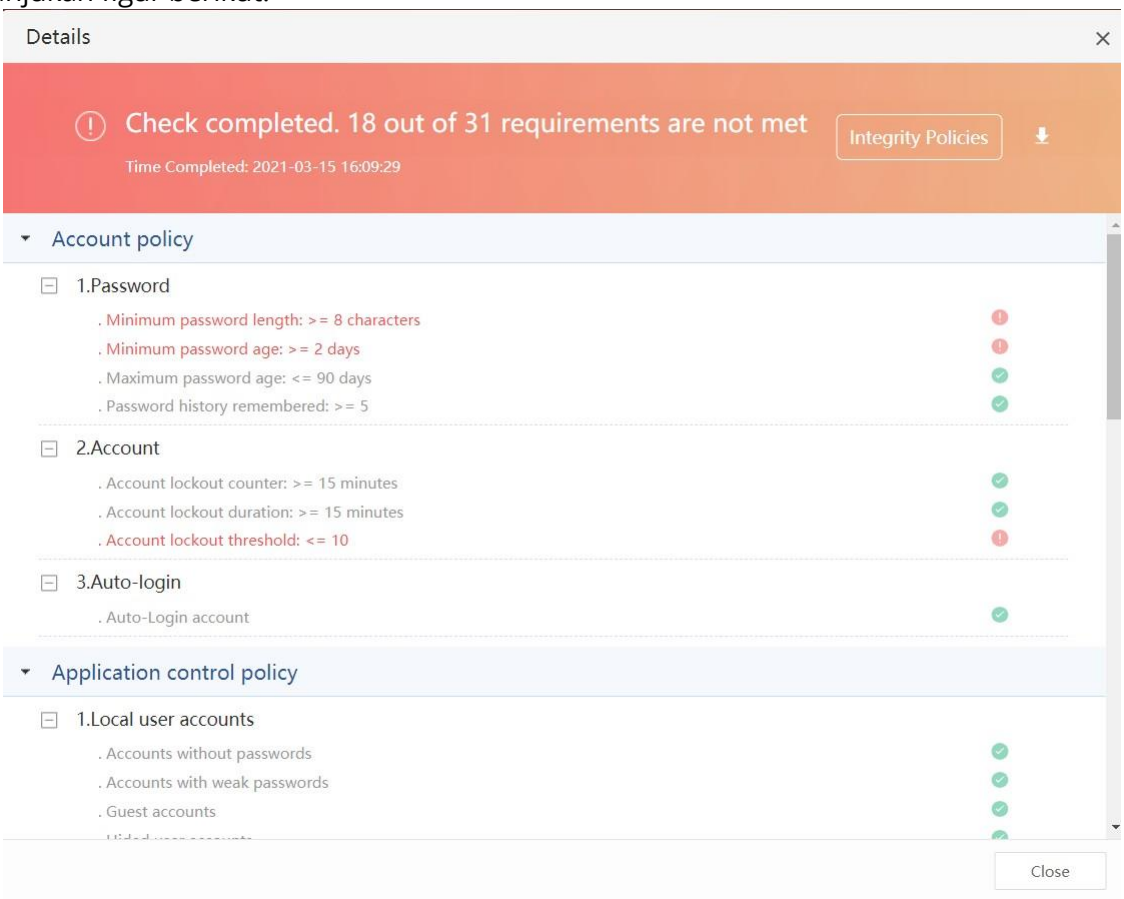
3.1.1 Pemeriksaan Keamanan & Integritas

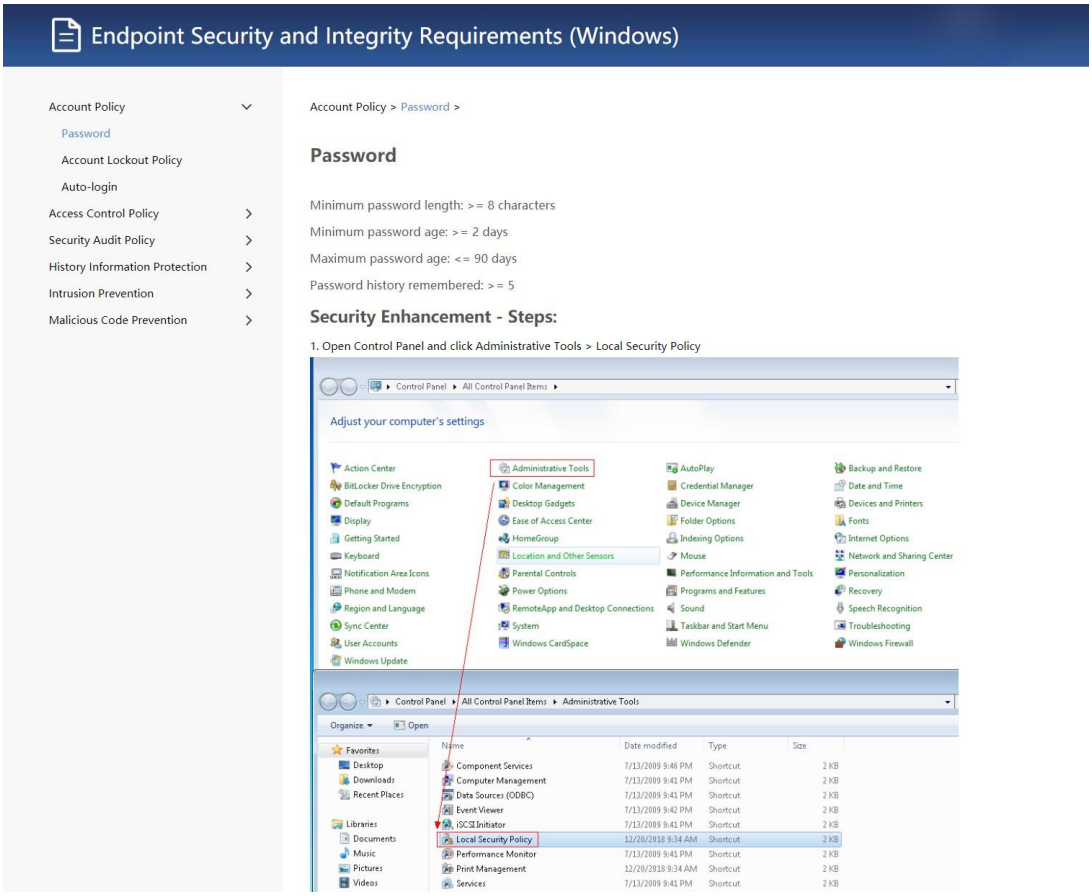
Pergilah ke Detection-> Security & Integrity Check, Lakukan pemeriksaan dasar pada server.



3.1.2 Menangani Ketidaksesuain

Memperkuat item yang tidak sesuai pada pemeriksaan keamanan sistem menghasilkan menurut dokumen pengaturan keamanan disediakan oleh Endpoint Secure, seperti ditunjukan figur berikut:



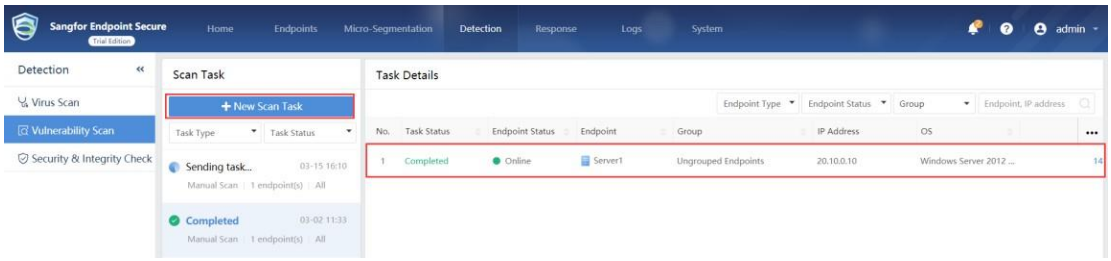


Pemeriksaan Kerentanan Sistem

Menolong pengguna mengidentifikasi kerentanan resiko tingi di server dan menyediakan saran perbaikan.

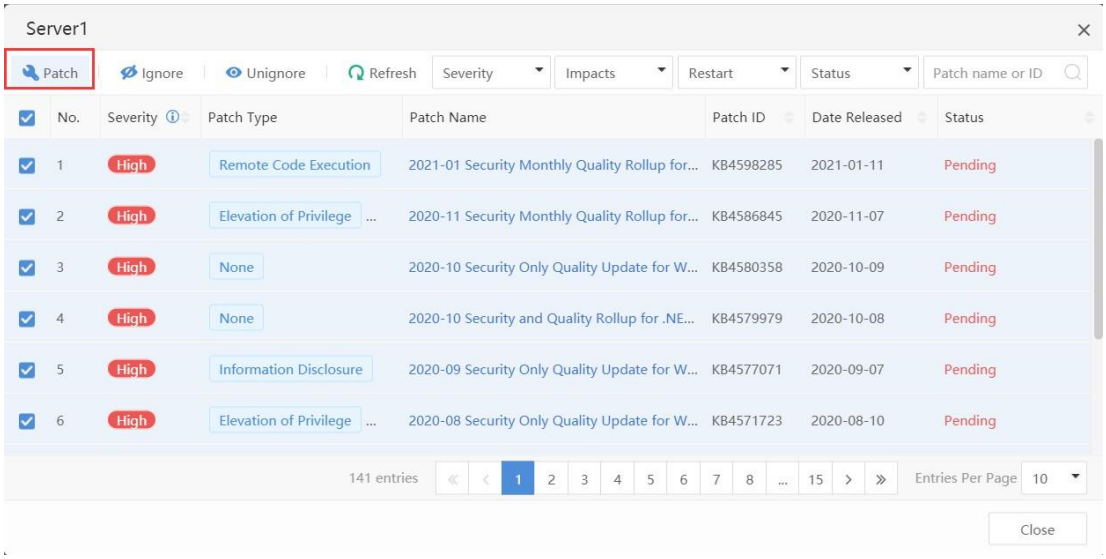
3.1.3Pemeriksaan Kerentanan

Pergilah ke Detection-> Vulnerability Scan path, Check servers for vulnerabilities.



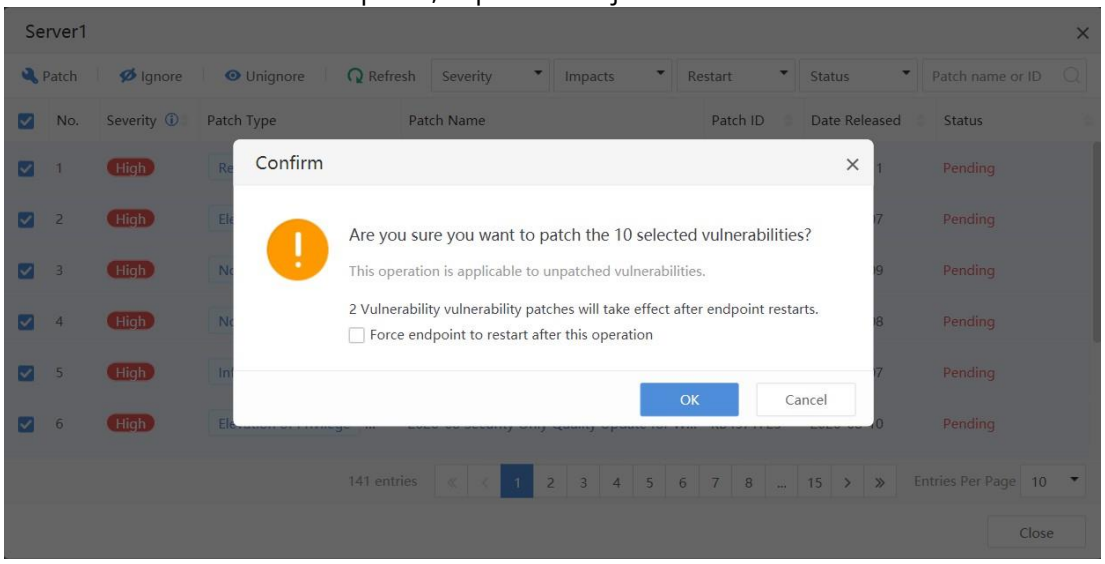
3.1.4 Menangani Ketidaksesuaian

Memperbaiki kerentanan yang belum diperbaiki pada hasil pemeriksaan, seperti ditunjukkan



dibawah:

Perlu diketahui setelah mengklik "Patch", direkomendasikan tidak mencentang "Force endpoint to restart after this operation" untuk pengingkatan hanya dapat mendapatkan efek setelah merestart komputer, seperti ditunjukkan dibawah:



3.2 Memindai Virus

Lakukan investigasi penuh pada server, temukan dan tangani file ancaman lebih awal.

3.2.1 Memindai Virus

Organisasi atau departemen dengan lingkungan bisnis yang sama akan mempromosikan implementasi menjadi beberapa ide berikut.

Temukan test komputer: Temukan komputer dalam lingkungan bisnis yang sama untuk diinstall Endpoint Secure client test untuk percobaan . Sebuah percoban Analisa dan hasilnya : Analisa file ancaman yang ditemukan oleh komputer test. Jika ditemuakan

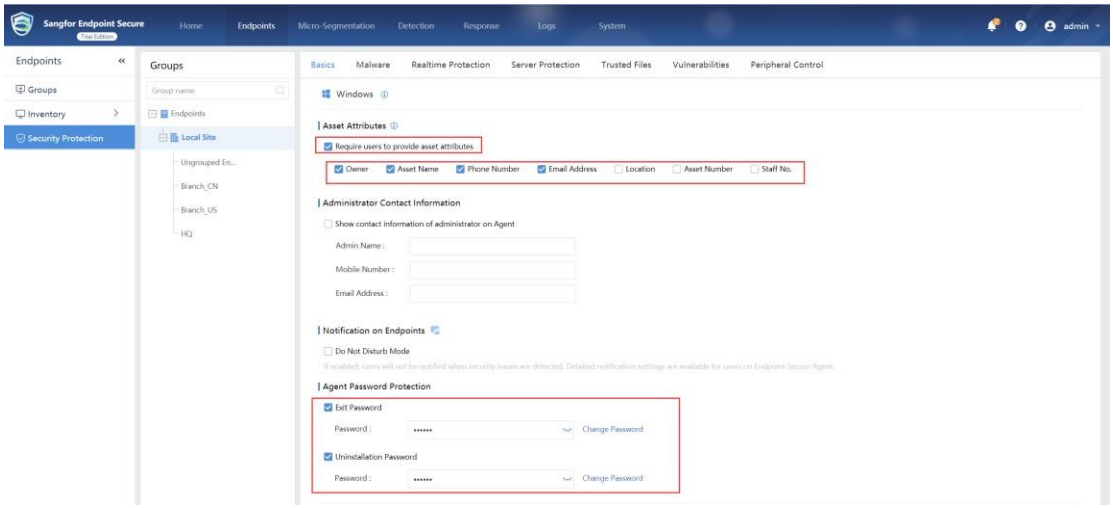
kesalahan penilaian, tambahkan ke witelist.
Jika yakin bahwa itu bukan salah penilaian, hubungi Sangfor Engineer untuk mengurusnya.
Memastikan kemampuan bisnis. Pastikan dan coba komputer bisnis untuk memastikan bisnis dapat digunakan secara normal.
Lakukan instalasi di komputer lainnya: komputer test dipastikan dan bisnis tidak terpengaruh, lalu itu akan dilakukan ke komputer lain di lingkungan yang sama untuk menginstall dan membuang ancaman.

Bagian 4 Panduan Implementasi Keamanan Server

Implementasi policy keamanan server merujuk kepada policy mana yang harus dikonfigurasi oleh Endpoint Secure dan bagaimana mengatur policy keamanan dalam rangka menjamin kelanjutan keamanan klien. Policy keamanan server dikonfigurasi dari basic policy, virus detection and killing policy, real-time protection policy, trust list, vulnerability detection dan repair detection, dan alarm policy untuk melindungi keamanan server.

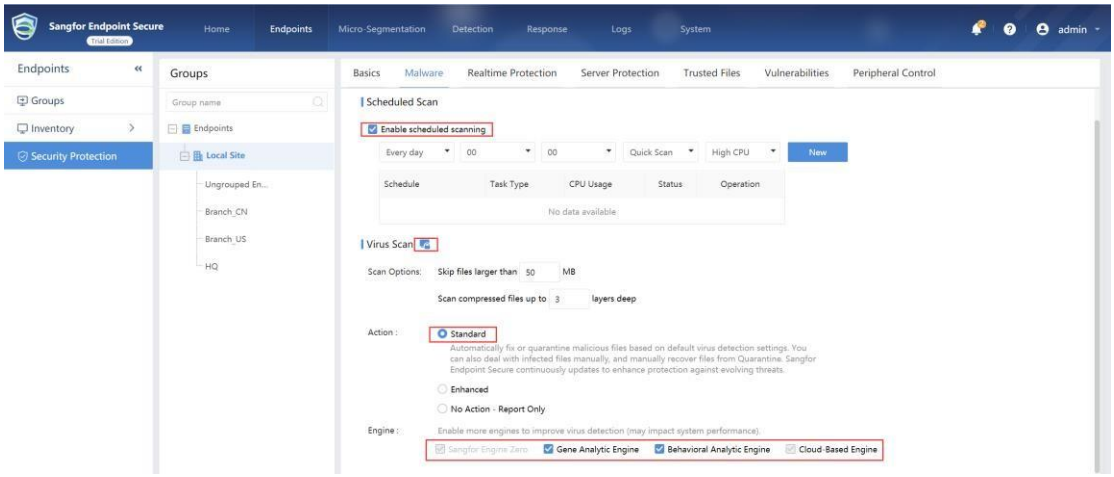
4.1 Basic Policy

Pergi ke Endpoints->Security Protection path, konfigurasi basic policy dari group dimana server berada, mengaktifkan asset information registration, dan set the terminal Exit Password/Uninstallation, seperti figur dibawah ini:



4.2 Anti-Virus

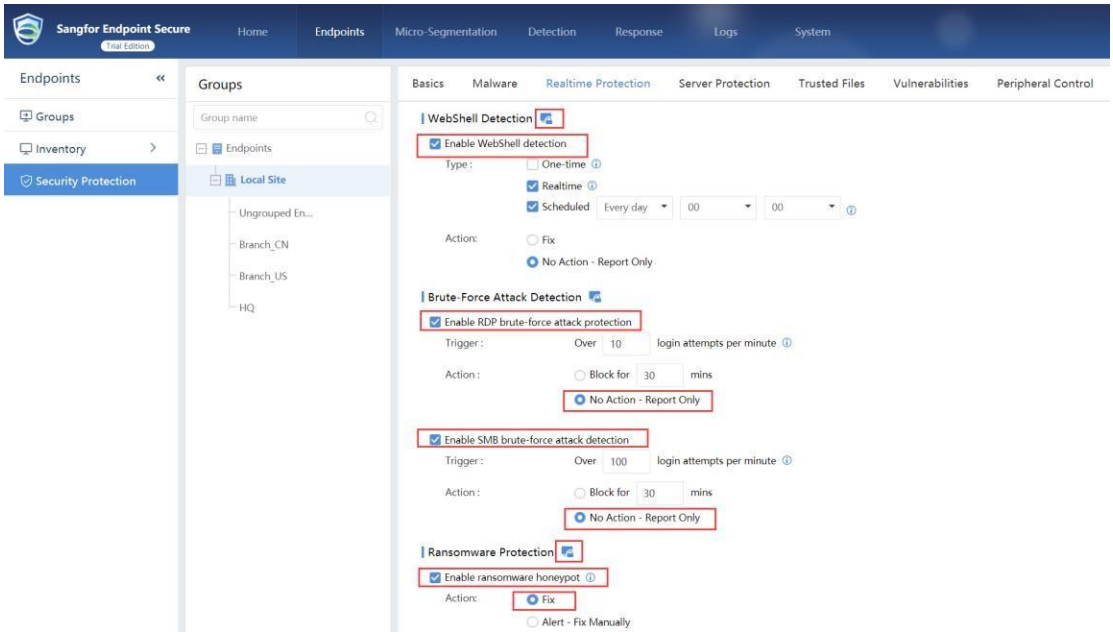
Pergi ke Endpoints->Security Protection path, konfigurasi virus detection dan killing policy pada group dimana server ditempatkan, seperti figur berikut:



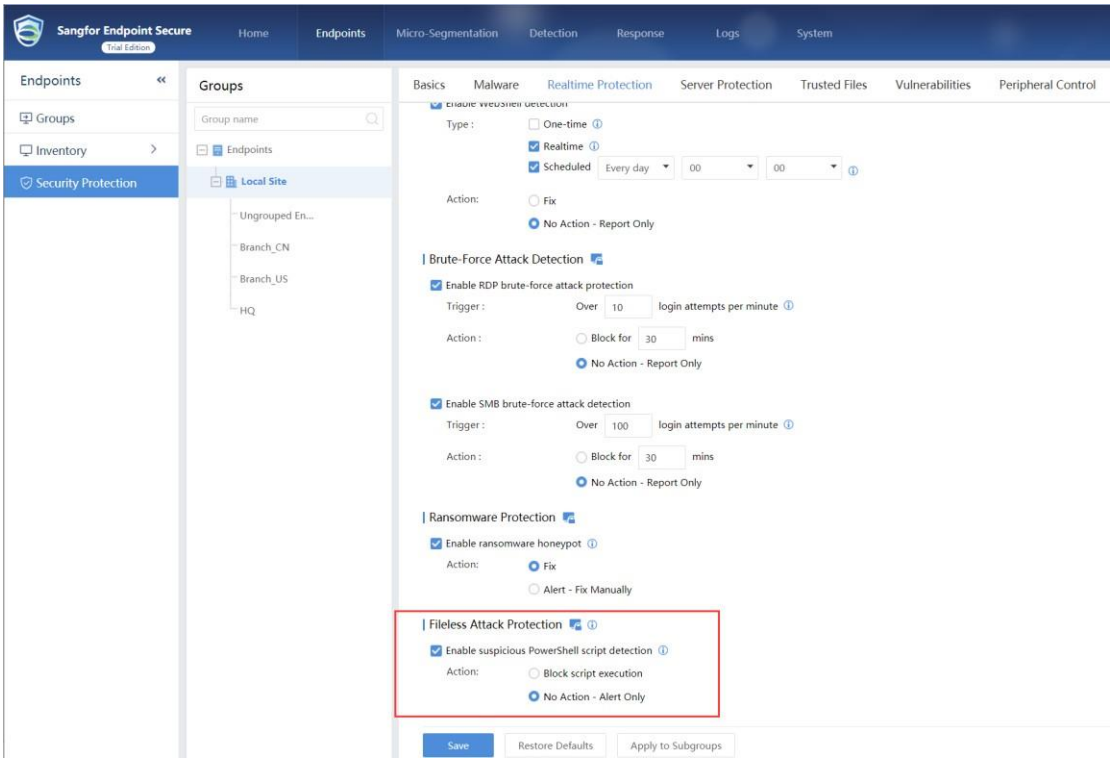
[Pemindaian Terjadwal] Aktifkan pemindaian umum otomatis. Direkomendasikan waktu untuk pemeriksaan sebulan sekali, tipe pemindaian adalah quick scanning, dan mode pemindaian adalah balanced.
[Aksi] Simpan konfigurasi defaut; aksi yang direkomendasikan setelah file ancaman ditemukan adalah "Standard"; Jika mesin pemindai dinyalakan sepenuhnya, itu akan menyerap sumber yang tinggi. Jika CPU dan Memori klien dikonfigurasi dengan 4 cores dan 8GB atau lebih, itu dapat dinyalakan sepenuhnya. Jika anda mengikuti konfigurasi disini, direkomendasian untuk membuka gene feature engine daripada behaviour analysis engine.

4.3 Realtime Protection

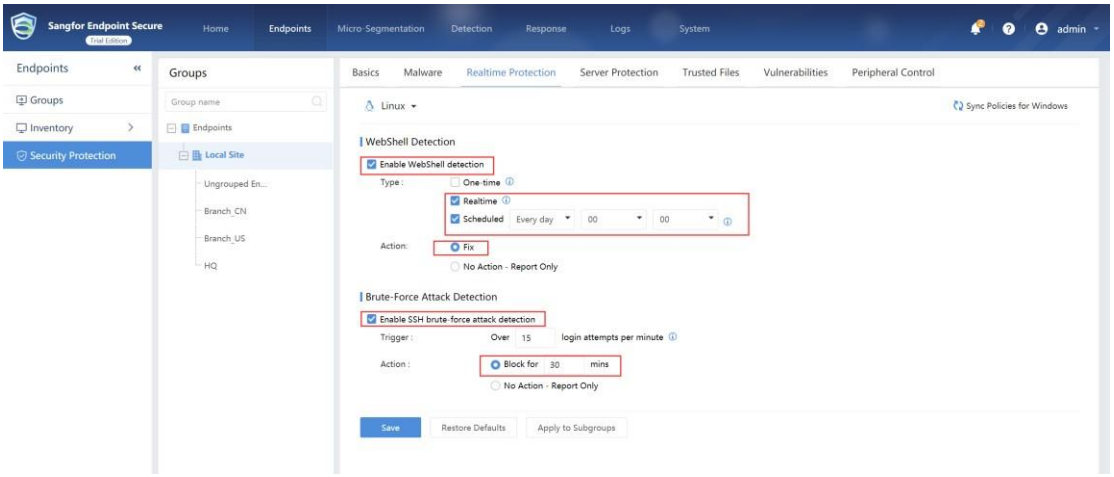
Pergi ke Endpoints->Security Protection path, konfigurasi real-time protection policy dari group dimana server berada, termasuk real-time file monitoring, ransomware protection and



advanced threat protection, seperti ditunjukkan oleh figur dibawah, atur real-time protection policy.

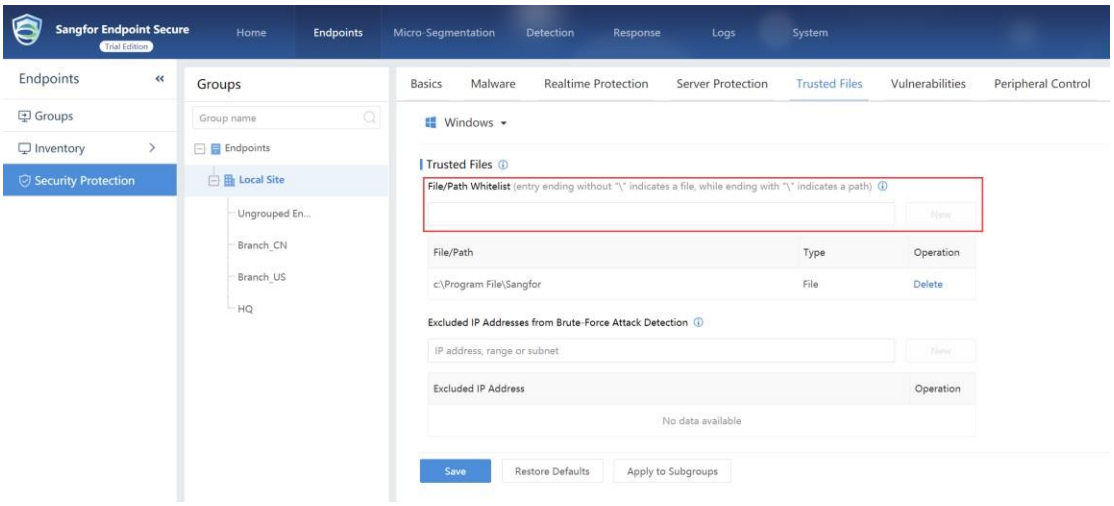


[Realtime File System Protection] Aktfikan small lock icon pada bagian kanan, dan file real-time protection policy akan diterbitkan oleh MGR ke ES agent.
[Protection Level] Direkomendasikan untuk melakukan konfigurasi pada protection level sebagai "Medium"; [File Type] Direkomendasikan untuk memilih semua tipe;
[Scan Options] Direkomendasikan untuk menyimpan konfgurasi defaut untuk pemindaian file;
[Engine] Jika engine pemindaian telah sepenuhnya menyala, itu akan menggunakan sumber tenaga yang besar. Jika CPU dan Memory server telah dikonfigurasi dengan 4 core dan 8GB atau lebih, itu dapat sepenuhnya dinyalakan. Jika konfigurasinya dibawah itu, direkomendasikan untuk menyalakan gene feature engine dibandingkan Sangfor Zero artificial intelligence engine. .
[Action] Aksi default setelah menemukan file yang mencurigakan adalah direkomendasikan untuk di set ke "standard disposal"
[Ransomware Protection] Aktifkan small lock icon pada bagian kanan, dan ransomware protection policy akan dikirimkan dari management terminal ke ES agent.
[Action] Telah ditemukan bahwa rekomendasi konfigurasi untuk ransomware behavior adalah "Fix".
[Fileless Attack Protection] Mengaktfikan small lock icon pada bagian kanan, dan advanced threat protection policy akan diterbirkan dari management end ke ES agent, dan centang "Enable suspicious PowerShell script detection".
[Action] Ketika powershell script yang mencurigakan ditemukan untuk dijalankan, direkomendasikan untuk di set menjadi "Block script execution".
Set Linux server real-time protection policy. Linux server real-time protection policy hanya memiliki webshell detection dan and brute force cracking detection, seperti ditunjukan figur dibawah.



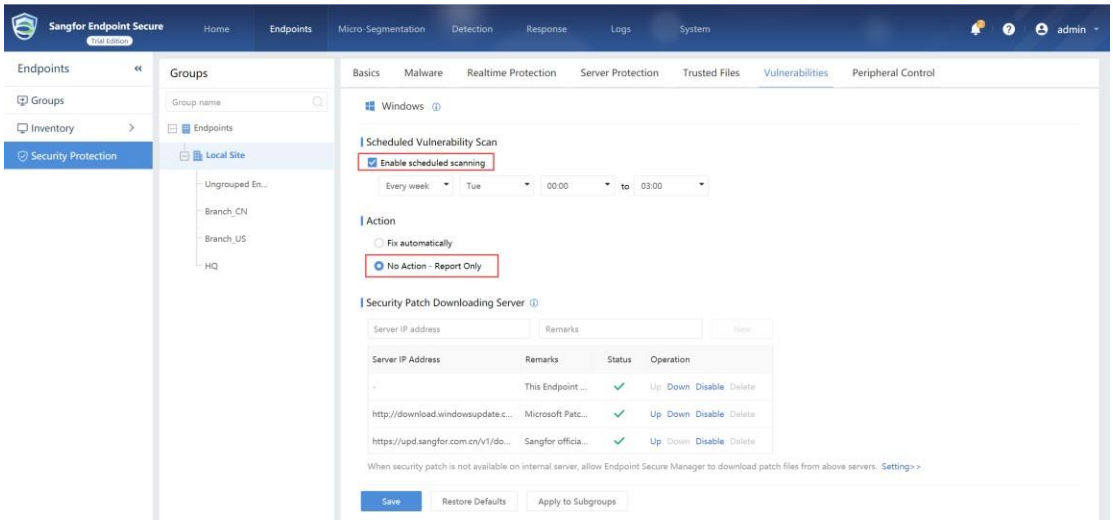
4.4Trust Files

Pergilah ke Endpoints->Security Protection path, Konfigurasikan whitelist policy pada group dimana server berada, dan tambahkan file dan direktori dimana tidak membutuhkan antivirus dan real-time protection untuk trust list (semacam file business system), seperti ditunjukkan figur berikut:



4.5Vulnerability Fix

Pergilah ke Endpoints->Security Protection path, konfigurasikan vulnerability repair policy pada group dimana server berada, seperti ditunjukkan figur berikut:



[Scheduled Vulnerability Scan] Mengaktifkan regular automatic scanning.

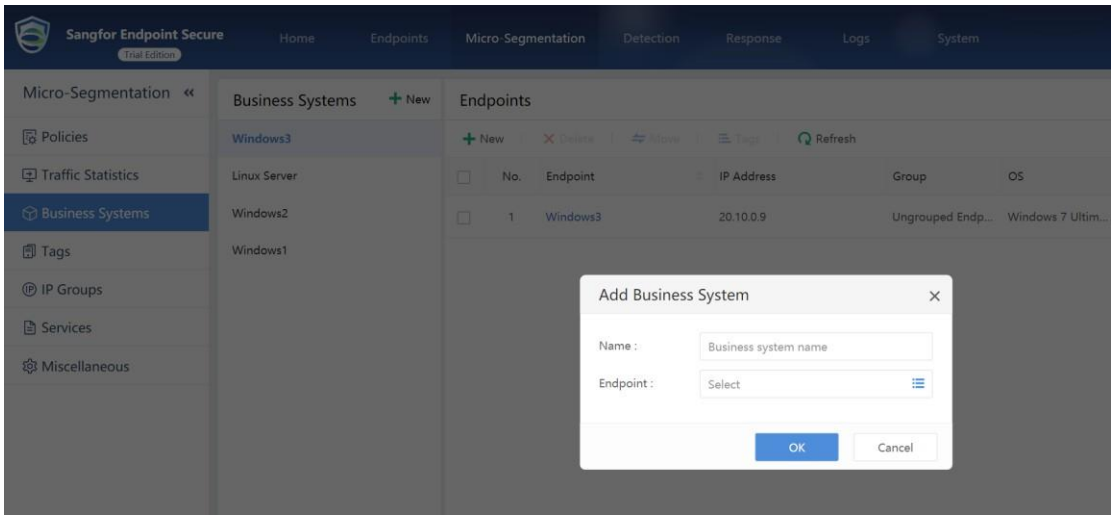
[Action] Direkomendasikan untuk mengatur vulnerability scan result menjadi "No Action-Report Only ", network administrator akan memperbaiki itu berdasarkan situasi yang sebenarnya.

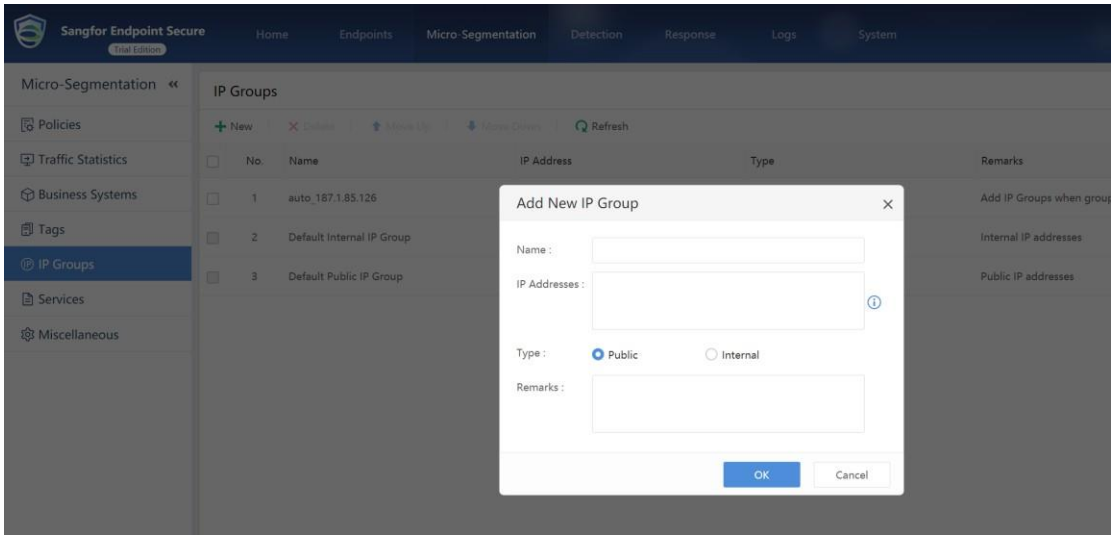
4.6 Micro-Segmentation Policy

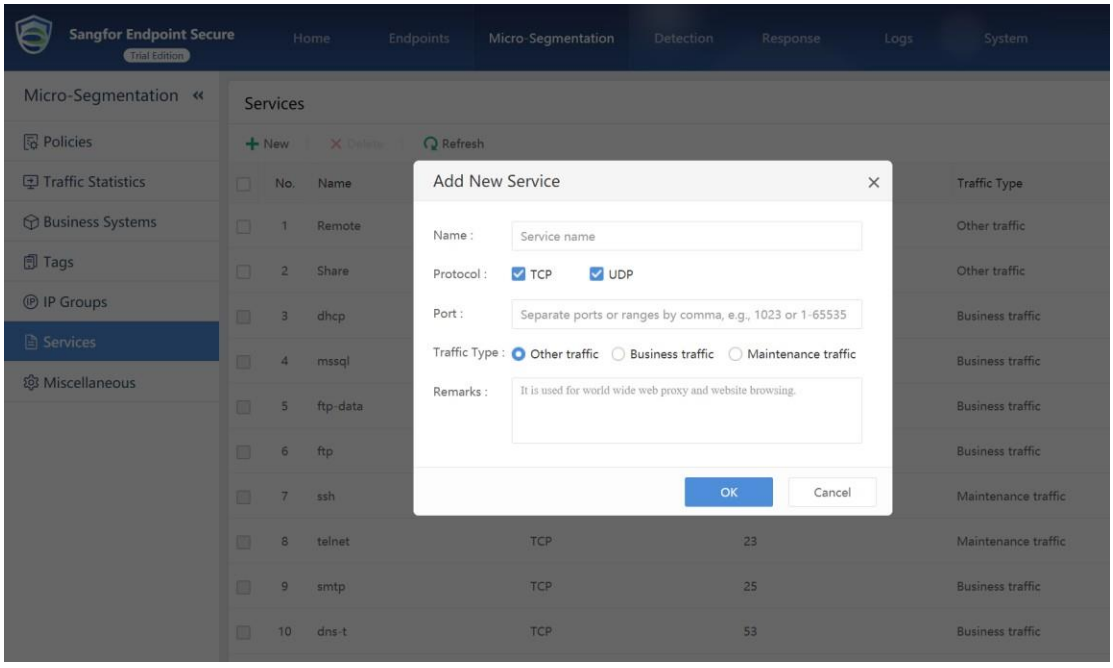
1. Micro-isolation adalah dasar dari five-tuples untuk mengontrol inbound dan outbound trafik dari server untuk mencapai tujuan dari melindungi keamanan server. Direkomendasikan bahwa port yang diperlukan dapat dilepaskan dari micro-isolation policy, dan non-essential high-risk ports dapat dilarang untuk meningkatkan keamanan. Konfigurasi sebagai berikut berdasarkan kebutuhan pelanggan, berikut urutan hubungan akses antar pelanggan bisnis, system/IP/role/service dan setiap objek dan persiapan and setiap objek, Dan persiapan dari mengikuti micro-isolation policy, seperti ditunjukkan tabel berikut ini;

Objects	Business System	**Business System Name**	**Endpoint Group**	**Included Endpoints**	
		OA Server	Server Group	OA_WEB	
		Database Server	Server Group	Database Server	
	IP Group	**IP Group**	**IP Range**	**IP Group Type**	
		Office Endpoint	172.16.200.1-172.16.200.254	LAN	
	Services	**Services Name**	**Services Type**	**Port**	**Traffic Type**
		http	TCP	80	Business
		mysql	tcp	3306	Business
Access Relationshi p	Access Relationship	**Source**	**Destination**	**Services**	**Action**
		IP Group: Office Endpoint	Business System: OA Server	http	Allow
		Business System: OA Server	Business System: Database Server	mysql	Allow

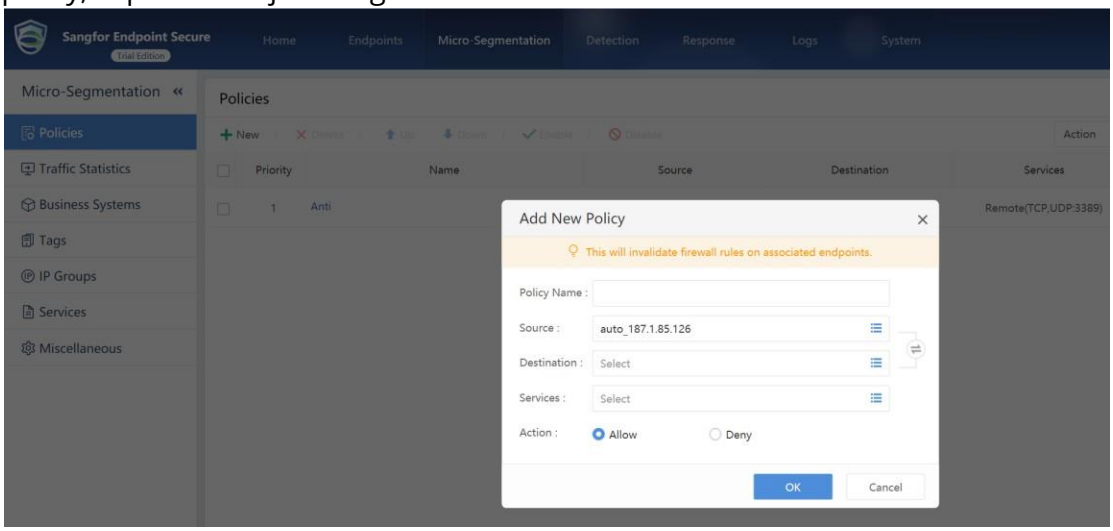
2. Berdasarkan isi dari tahap pertama, Isikan business system/IP group/service, dan hubungkan itu ke micro-isolation policy, seperti ditunjukkan pada figur dibawah.



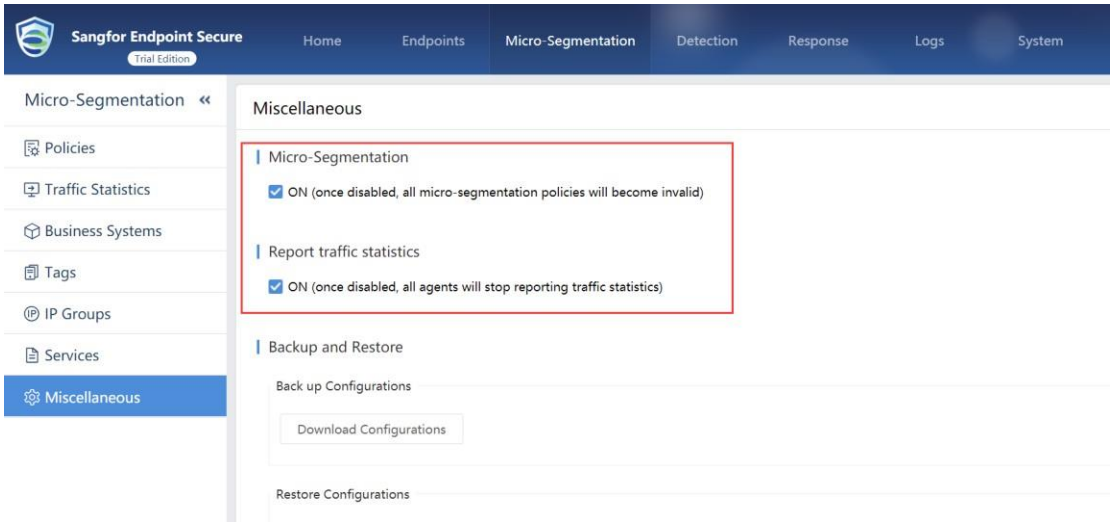




3. Tetapkan micro-isolation policy. Menurut hubungan akses diurutkan di langkah 1 dan business system/IP group/service ditetapkan pada langkah 2, tetapkan micro-isolation policy, seperti ditunjukan figur dibawah



4. Aktifkan micro-isolation policy switch dan traffic report, seperti ditunjukan figur dibawah:

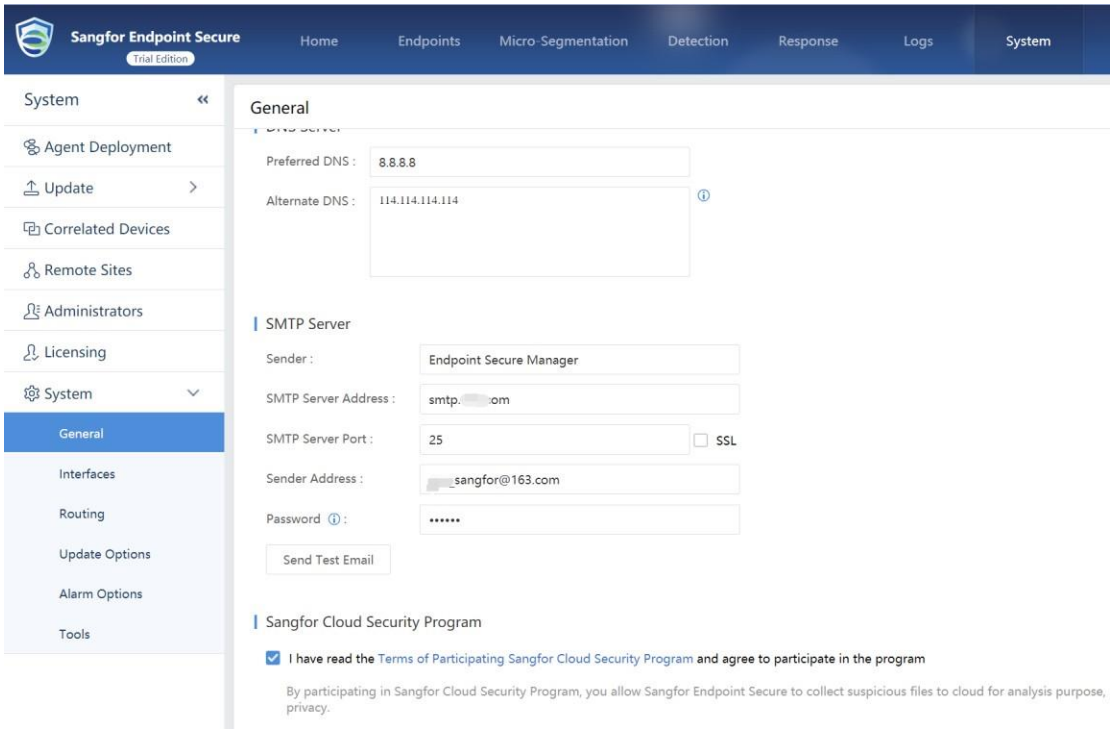


5. Periksa efek micro-isolation dan coba konektifitas port server.

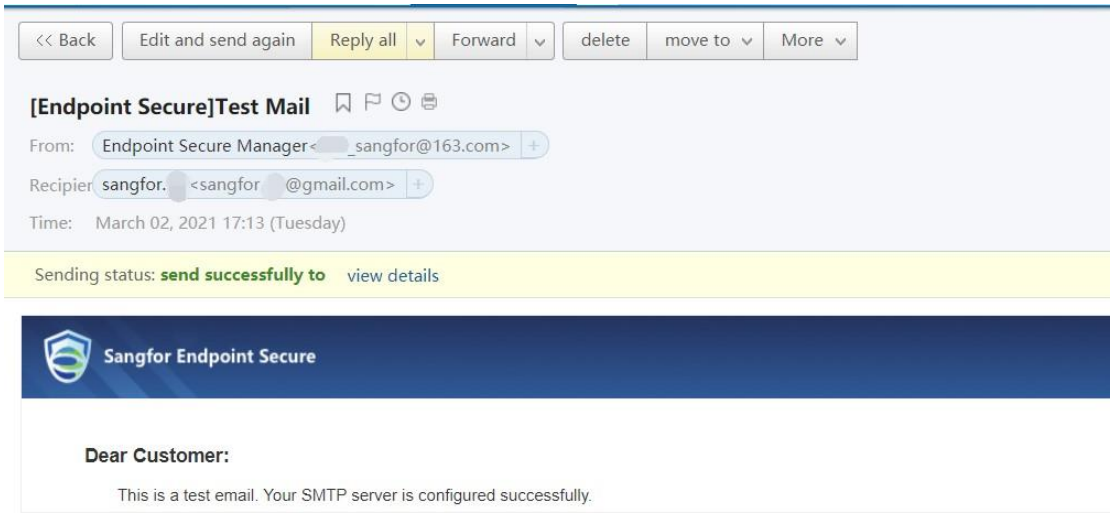
4.7 Alarm Policy

Konfigurasi alarm policy untuk memberitahukan kepada administrator tepat waktu ketika ada ancaman terjadi di intranet. Langkah konfigurasinya seperti berikut:

1. Konfigurasi SMTP Server.



Klik Send "Send Test Email", jika anda dapat menerima test email seperti ditunjukan figur dibawah, artinya mailbox server telah sukses dikonfigurasi.



SANGFOR