

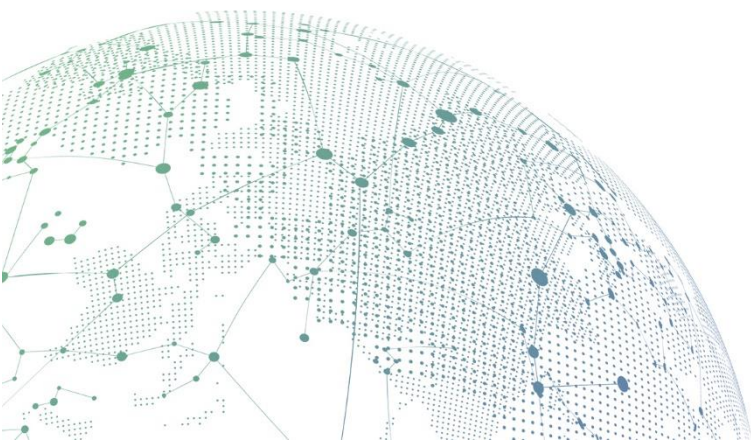


SANGFOR



Endpoint Security Praktik Terbaik untuk Skenario Panduan Implementasi Kebijakan Keamanan Endpoint Secure untuk Host

Versi 3.2.22



Catatan Perubahan

Tanggal	Deskripsi Perubahan
16 Maret 2021	Dokumen diterbitkan.
17 Mei 2021	Dokumen diperbaharui

DAFTAR ISI

Bagian1

Bagian1

Bagian1

1

1

2

3.2 Pemeriksaan Kerentanan Sistem3

3

3

4

4

Bagian5

5

5

6

8

8

9

Bagian 1 Skenario

Bagian 2 Gambaran

Dokumen ini sesuai untuk Endpoint Secure untuk memandu pada Endpoint Secure security policy dalam konteks in melindungi host security. Dokumen termasuk dua bagian: mengidentifikasi resiko resko host security dan mengimplementasikan policy dari host security. Pengindentifikasian resiko host security memandu pengguna untuk mengidentifikasi resiko client security lebih awal, membuat pengguna menyadari resiko keamanan dan dampaknya terhadap host, dan memandu pengguna untuk berurusan dengn resiko keamanan; mengimplementasikan policy keamanan host merujuk pada keamanan policy mana yang seharusnya dikonfigurasi oleh Endpoint Secure dan bagaimana mengkonfigurasi keamanan policy dalam rangka menjamin keamanan host.

Bagian 3 Mengidentifikasi Resiko Keamanan dari Host

Mengidentifikasi resiko keamanan host adalah untuk panduan pengguna untuk mengidentifikasi resiko keamanan client lebih awal, membuat pengguna lebih menyadari resiko keamanan dan dampaknya terhadap host, dan juga sebagai panduan pengguna untuk menangani resiko resiko keamanan. Bagian ini memandu pengguna untu mengidentifikasi resiko keamanan client lebih awal dan menanganinya dalam tiga bagian: pemeriksaan awal, pemeriksanan kerentanan sistem, dan membunuh virus.

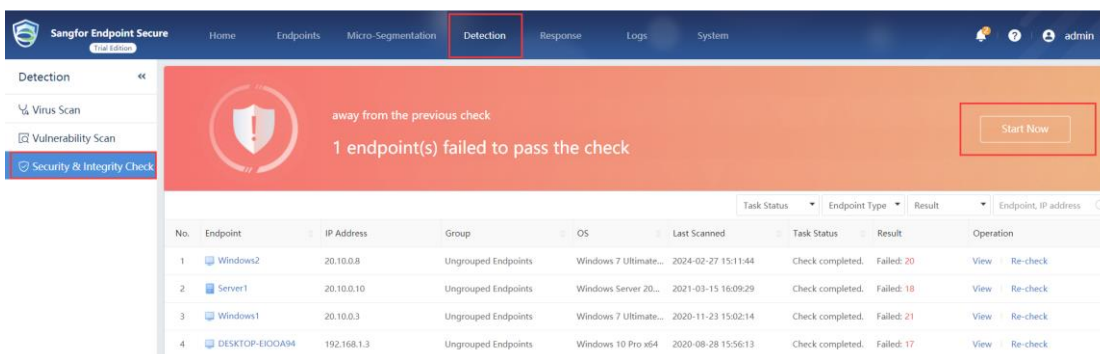
Mohon dicatat jika ada banyak host, disarankan untuk memilih 1 atau 2 host untuk memandu pengguna bagaimana untuk mengidentifikasi resiko keamanan host dan bagaimana untuk mengatasinya.

3.1 Pemeriksaan Keamanan dan Integritas

Pemeriksaan kamanan & integritas adalah sebuah pemeriksaan yang wajib bagi sistem windows dan linux menurut kebutuhan wajib keamanan, meolong pengguna menemukan hal yang tidak sesuai di endpoint, hal yang tidak sesuai di intranet, dan menyediakan saran perbaikan.

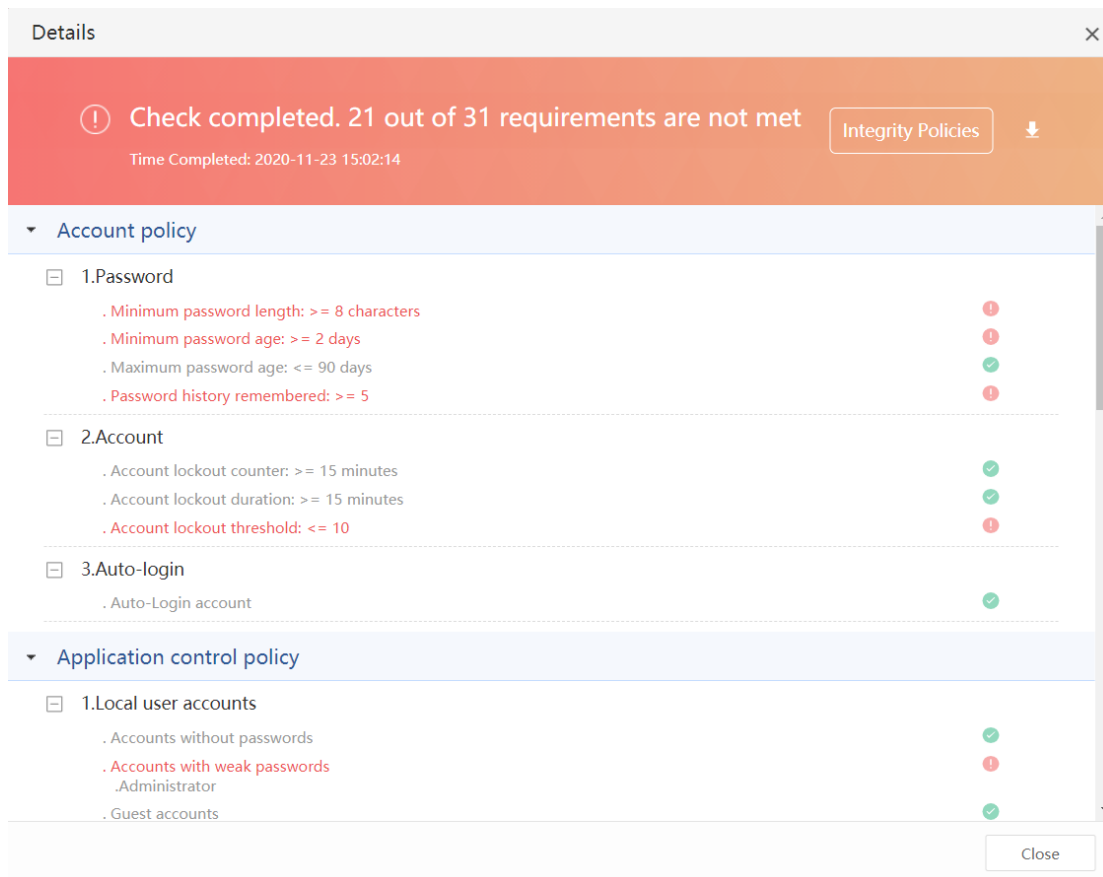
3.1.1 Pemeriksaan Keamanan & Integritas

Pergilah ke Detection-> Security & Integrity Check, Lakukan pemeriksaan basic security pada host.



3.1.2 Menhadapi Ketidaksesuaian

Memperkuat hal yang tidak sesuai pada pemeriksaan keamanan akan memberikan hasil sesuai dengan dokumen pengaturan wajin oleh Endpoint Secure, seperti tampilan pada figure berikut:



Endpoint Security and Integrity Requirements (Windows)

- Account Policy
 - Password
 - Account Lockout Policy
 - Auto-login
- Access Control Policy
- Security Audit Policy
- History Information Protection
- Intrusion Prevention
- Malicious Code Prevention

Account Policy > Password >

Password

Minimum password length: >= 8 characters
 Minimum password age: >= 2 days
 Maximum password age: <= 90 days
 Password history remembered: >= 5

Security Enhancement - Steps:

1. Open Control Panel and click Administrative Tools > Local Security Policy

The screenshot shows the Windows Control Panel with 'Administrative Tools' selected. A red box highlights 'Administrative Tools' in the top row. A second screenshot shows the 'Administrative Tools' window with 'Local Security Policy' selected in the list, also highlighted with a red box.

3.2 Pemeriksaan Kerentanan Sistem

Membantu pengguna untuk mengidentifikasi resiko tinggi kerentanan pada sistem dan menyediakan saran perbaikan.

3.2.1 Pemeriksaan Kerentanan

Pergilah ke bagian Detection-> Vulnerability Scan path, Periksa hosts untuk kerentanan.

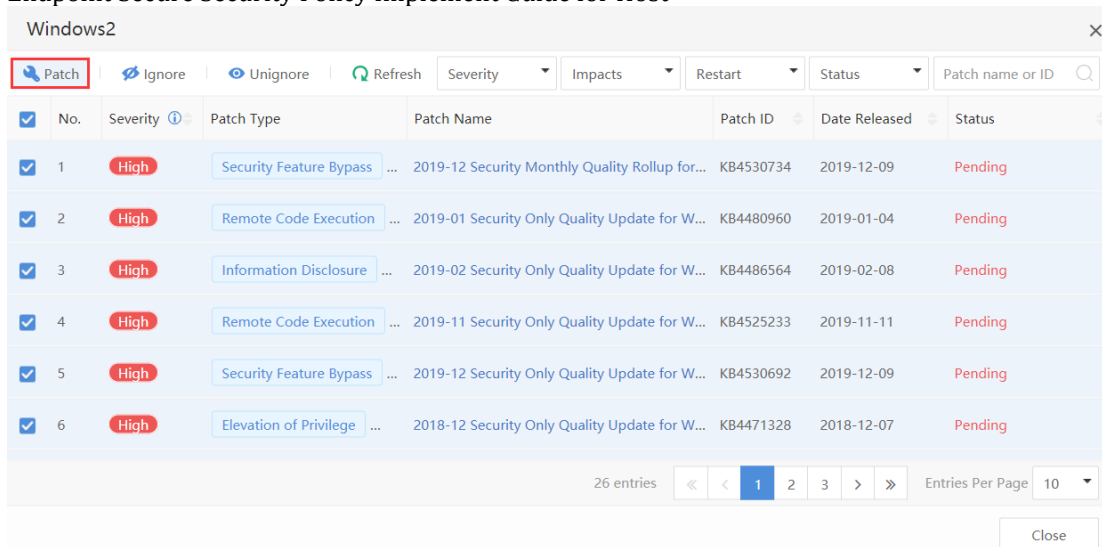
The screenshot shows the Sangfor Endpoint Secure interface. On the left, there is a navigation pane with 'Vulnerability Scan' selected. The main area shows a 'Task Details' table with the following data:

No.	Task Status	Endpoint Status	Endpoint	Group	IP Address	OS	Endpoint Type	Endpoint Status	Group	Endpoint, IP address
1	Completed	Online	Windows2	Ungrouped Endpoints	20.10.0.8	Windows 7 Ultimate S...	All	Unpatched Vulns	26	25 Patch Re-scan

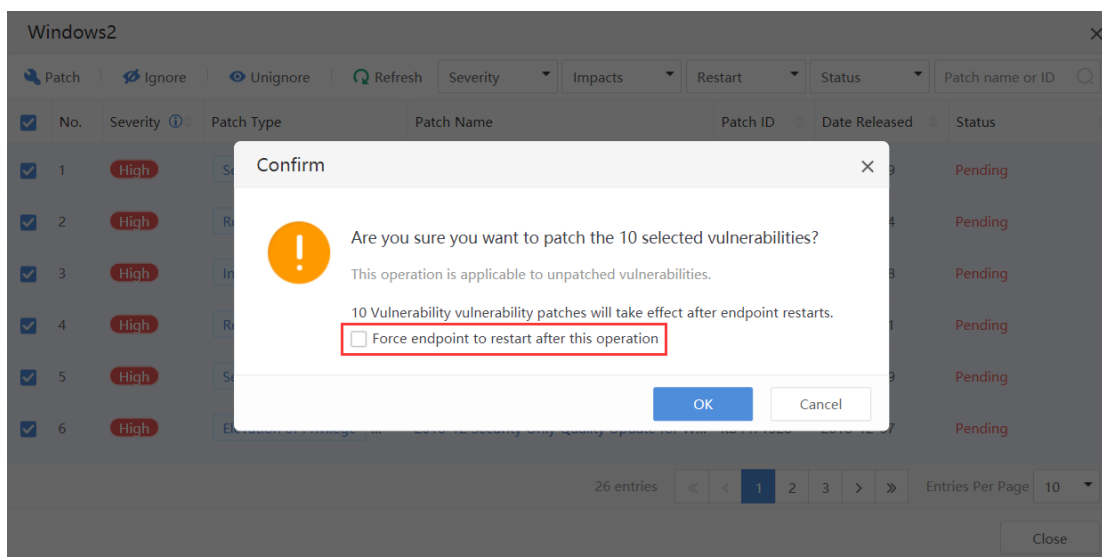
3.2.2 Menghadapi Kerentanan

Perbaiki kerentanan yang tidak selesai pada hasil pemeriksaan kerentanan, seperti ditampilkan figure dibawah:

Endpoint Secure Security Policy Implement Guide for Host



Ingat setelah mengklik "Patch", direkomendasikan untuk tidak mencentang "Force endpoint to restart after this operation" agar patches hanya dapat memberikan efek setelah komputer di restart, seperti figur dibawah:



3.3 Pemindaian Virus

Lakukan investigasi penuh dan matikan hosts, temukan dan hadapi ancaman lebih awal.

3.3.1 Pemindaian Virus

Organisasi atau departemen dengan lingkungan bisnis yang sama akan mempromosikan implementasi sesuai ide-ide berikut.

Temukan komputer test: Cari komputer pada lingkungan bisnis yang sama untuk diinstall Endpoint Secure Client untuk percobaan skala penuh

Analisa dan hasil pembersihan: Analisa file ancaman yang ditemukan oleh komputer test.

Jika telah terkonfirmasi itu adalah sebuah keputusan yang salah, buatlah sebuah whitelist.

Konfirmasi bahwa itu bukan keputusan yang salah, hubungi engineer Sangfor untuk mengatasinya

Verifikasi kelanjutan bisnis: Verifikasi dan cobalah kemampuan bisnis komputer agar bisnis dapat berjalan normal.

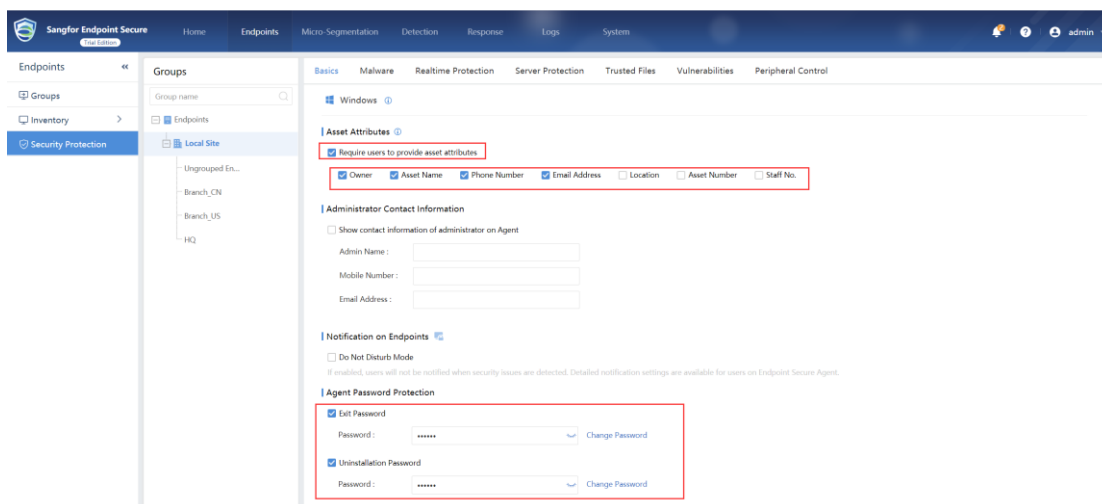
Lanjutkan instalasi pada komputer lainnya: komputer test telah terverifikasi dan bisnis tidak terpengaruh, Selanjutnya dilanjutkan di komputer lainnya pada lingkungan yang sama agar terinstall dan membunuh virus.

Bagian 4 Panduan Implementasi Host Security Policy

Implementasi dari host security policy merujuk pada security policy mana yang seharusnya dikonfigurasi oleh Endpoint Secure dan bagaimana untuk mengkonfigurasi security policy agar memastikan keamanan client setelahnya. Security policy host dikonfigurasi dari basic policy, virus detection and killing policy, real-time protection policy, trust list, vulnerability detection and repair detection, dan alarm policy untuk melindungi keamanan host.

4.1 Basic Policy

Pergilah ke Endpoints->Security Protection path, konfigurasi basic policy dari group dimana host berada, aktifkan asset information registration, dan tentukan password keluar terminal/ password untuk uninstall, seperti figur dibawah:



4.2 Anti-Virus

Pergilah ke Endpoints->Security Protection path, konfigurasi virus detection dan matikan policy di tempat host berada, seperti figur:

[Basics](#) [Malware](#) [Realtime Protection](#) [Server Protection](#) [Trusted Files](#) [Vulnerabilities](#) [Peripheral Control](#)

Windows ▾

| Scheduled Scan

Enable scheduled scanning

▾
 ▾
 ▾
 ▾
 ▾

Schedule	Task Type	CPU Usage	Status	Operation
No data available				

| Virus Scan

Scan Options: Skip files larger than MB

Scan compressed files up to layers deep

Action :

Standard
 Enhanced
 No Action - Report Only
Report malicious files to the Manager, but do not automatically fix or quarantine them. This option is suitable for scenarios in which an on-duty security professional is responsible for fixing threats.

Engine :

Enable more engines to improve virus detection (may impact system performance).

Sangfor Engine Zero
 Gene Analytic Engine
 Behavioral Analytic Engine
 Cloud-Based Engine

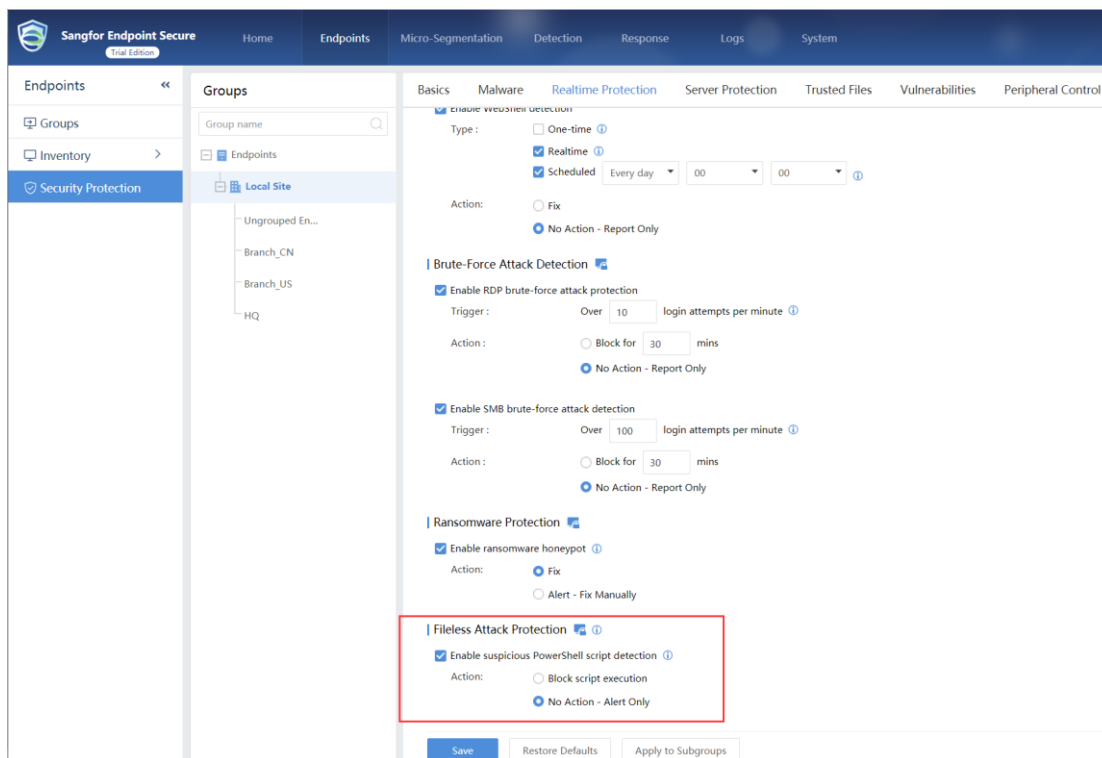
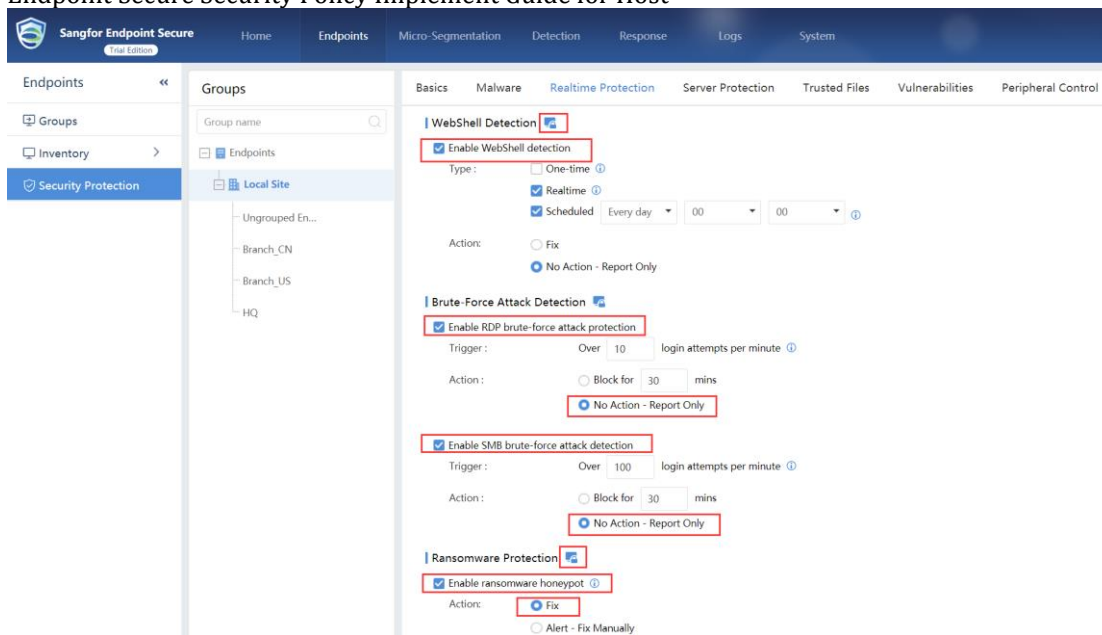
[Scheduled Scan] Hidupkan regular automatic scanning. Direkomendasikan melakukan pemeriksaan, setidaknya sekali sebulan, tipe pemindaian adalah quick scanning, dan mode pemindaian adalah balanced.

[Action] Simpan konfigurasi default; pada action setelah file ancaman akan dibuang direkomendasikan dikonfigurasi menjadi "Standard"; jika engine pemindaian telah sepenuhnya hidup, maka akan memakai sumber daya yang tinggi. Jika CPU dan memory klien telah dikonfigurasi dengan 4 core dan 8G atau lebih, maka dapat dinyalakan sepenuhnya. Jika anda mengkonfigurasi seperti hal disini, sangat direkomendasikan membuka mesin feature dibandingkanmesian behaviour analysis.

4.3 Realtime Protection

Pergilah ke Endpoints->Security Protection path, konfigurasi real-time protection policy dari group dimana host diletakkan, termasuk real-time file monitoring, ransomware protection and advanced threat protection, seperti terlihat pada figur dibawah, as shown in the figure below, atur windows real-time protection policy.

Endpoint Secure Security Policy Implement Guide for Host



[Realtime File System Protection] Aktifkan small lock icon pada bagian kanan, dan file real-time protection policy diterbikan dari MGR ke ES

[Protection Level] direkomendasikan untuk mengkonfigurasi protection level as "Medium";

[FileType] direkomendasikan mencentang semua tipe files;

[Scan Options] direkomendasikan untuk menyimpan konfigurasi default saat pemeriksaan file;

[Engine] Jika engine pemindai telah sepenuhnya nyala, itu akan menghabiskan sumber daya yang tinggi. Jika CPU dan memory host telah dikonfigurasi dengan 4 cores dan 8g atau lebih, maka sepenuhnya bisa dinyalakan. Jika konfigurasinya dibawahnya, direkomendasikan untuk menyalakan gene feature dibandingkan Sangfor Zero artificial intelligence engine. .

[Action] Aksi default yang dilakukan setelah file mencurigakan ditemukan direkomendasikan di atur menjadi "standard disposal"

Endpoint Secure Security Policy Implement Guide for Host

[Ransomware Protection] Aktifkan small lock icon pada bagian kanan, dan ransomware protection policy akan dikirimkan management terminal ke ES agent.

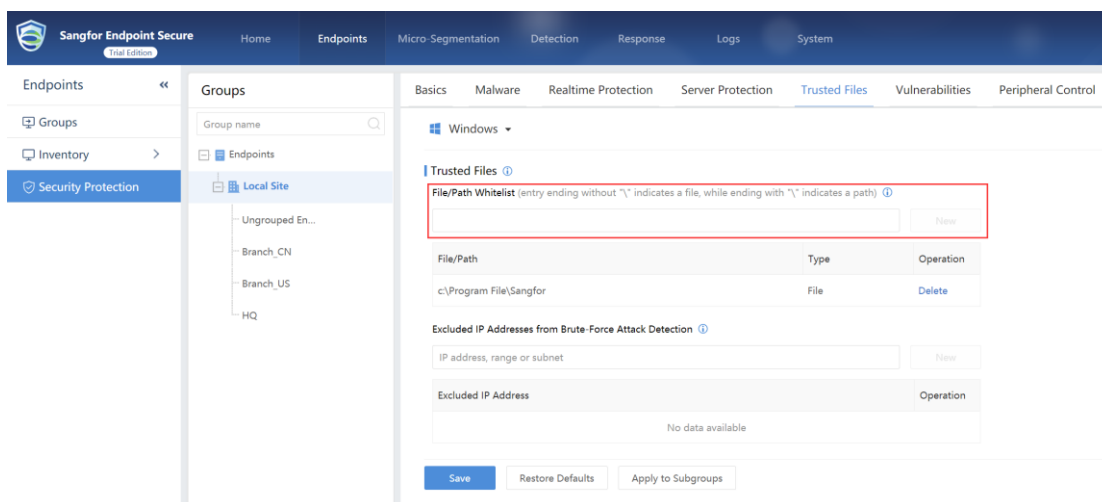
[Action] Ditemukan bahwa konfigurasi yang direkomendasikan untuk perilaku ransomware adalah "Fix".

[Fileless Attack Protection] Aktifkan small lock icon pada bagian kanan, dan advanced threat protection policy akan diterbitkan dari management end ke ES agent, dan centang "Enable suspicious PowerShell script detection".

[Action] Ketika sebuah skrip powershell ditemukan akan dieksekusi, direkomendasikan untuk mengatur itu ke "Block script execution".

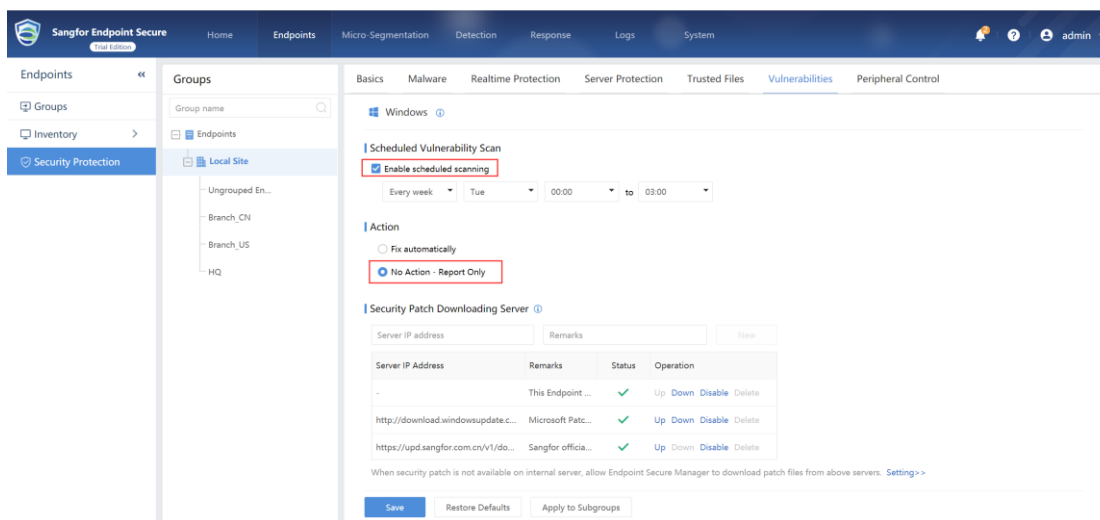
4.4 File Terpercaya

Pergilah ke Endpoints->Security Protection path, konfigurasi the whitelist policy pada group dimana host diletakkan, dan tambahkan file atau direktori yang tidak membutuhkan antivirus dan real-time protection untuk trust list (semacam file sistem bisnis), seperti terlihat di figur berikut:



4.5 Penyelesaian Kerentanan

Pergilah ke Endpoints->Security Protection path, Konfigurasi vulnerability repair policy pada group dimana host diletakkan, seperti figur berikut:



[Scheduled Vulnerability Scan] Aktifkan regular automatic scanning.

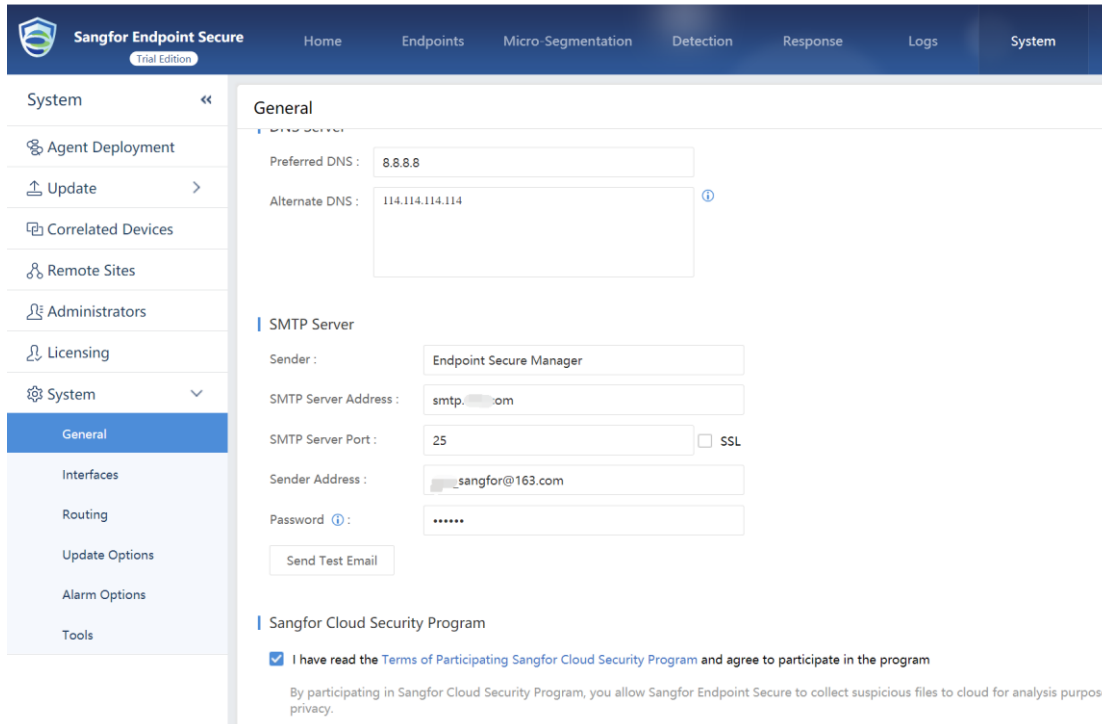
W.: www.sangfor.com | W.: community.sangfor.com | E.: tech.support@sangfor.com

[Action] Direkomendasikan untuk mengatur hasil pemindaian kerentanan menjadi "No Action-Report Only", network administrator akan memperbaiki itu sesuai kondisi yang sebenarnya.

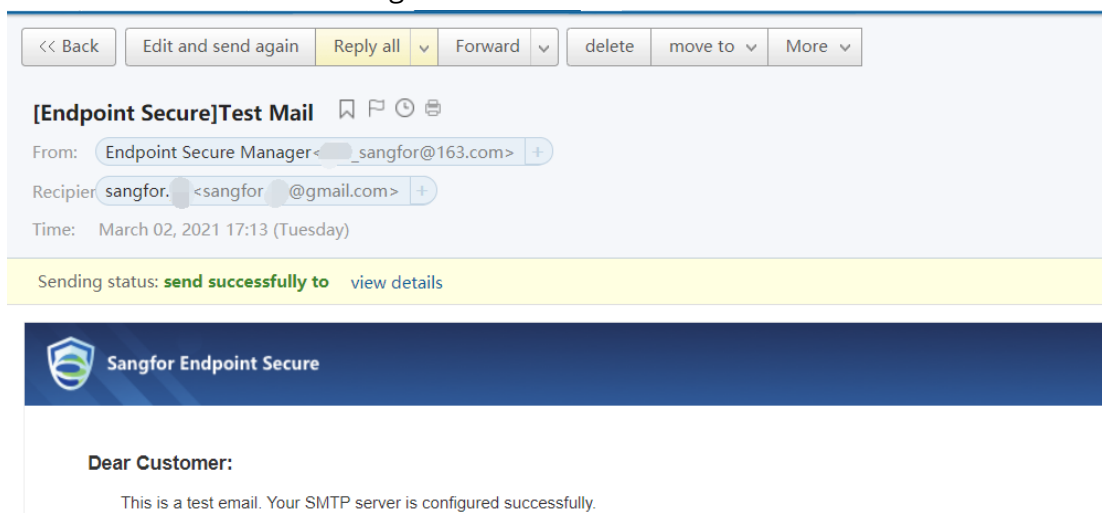
4.6 Alarm Policy

Konfigurasi alarm policies untuk memberikan notifikasi kepada administrator tepat waktu saat ancaman sedang terjadi di intranet, Langkah konfigurasinya adalah sbb:

1. Konfigurasi SMTP Server.



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



2. Konfigurasi alarm policy.

Endpoint Secure Security Policy Implement Guide for Host

Alarm-triggering Event

- Enabled
 - CPU usage is above 10 % , for 5 mins
 - Memory usage is above 10 % , for 5 mins
 - Disk usage is above 5 %
 - Within 24 hours, over 1 % endpoints infected by viruses
 - Within 24 hours, over 1 % endpoints undergo brute-force attacks
 - Within 24 hours, 1 high-threat virus intrusions detected
 - Within 24 hours, 1 high-threat WebShell backdoors detected
 - Ransomware attack occurs
 - Over 3 endpoints fail to perform virus scan task

3. Konfigurasi alamat penerima, sebaiknya sama dengan mailbox dari network administrator.

Alarm Delivery




- Restrict email alarms
 - Within 1 hours, a maximum of 50 emails will be sent, and excessive ones will be sent next time

Name	Email address	Operation
sangfor	sangfor.yzj@sangfor.com	Delete

Ketika alarm terpicu, network administrator akan menerima email seperti ini.


Endpoint Secure Security Policy Implement Guide for Host

<< Back Edit and send again Reply all Forward delete move to More

[Endpoint Secure]Endpoint Status Alarm   

From: Endpoint Secure Manager <[redacted]@sangfor.com>
Recipient: sangfor <[redacted]@sangfor.com>
Time: March 02, 2021 17:37 (Tuesday)

Sending status: **send successfully to** [view details](#)

 Sangfor Endpoint Secure

Dear Customer:

Sangfor Endpoint Secure has detected the following alarm-triggering events at 2021-03-02 17:37:05. Please log in to Endpoint Secure Manager and fix them.

Type: Manager Resource Usage Alarm
Description: CPU usage of Endpoint Secure Manager exceeds **10%** ,last for 6 minutes

[Fix Now >>](#)

Note: Click Fix Now to be redirected to Endpoint Secure Manager. If you cannot be redirected, please check network connection or Endpoint Secure Manager address. If Endpoint Secure Manager address is an internal IP, please try to log in to the Manager and fix it.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc