SANGFOR

IAG

Panduan Konfigurasi External Device Control

Versi 13.0.15

Catatan Perubahan

Tanggal	Deskripsi Perubahan
September 10, 2020	Rilis Dokumen Versi 13.0.15.

Daftar Isi

Bab 1 Latar Belakang Permintaan

Intranet endpoint secara sewenang-wenang terhubung ke perangkat peripheral yang tidak dapat dikontrol, seperti terhubung dengan USB flash drive untuk menyebarkan virus, dan terhubung ke wireless 4G network card untuk membuka internal dan eksternal networks, mengakibatkan kebocoran data.

Bab 2 Penjelasan Fitur

2.1 Penjelasan

- Mendukung penonaktifan perangkat storage, perangkat network, perangkat Bluetooth, camera dan printer.

- Mendukung refined control dari USB dan perangkat portabel (ponsel, tablet, etc.).

  - **Refined control dari USB:**

    1. Tolak - USB tidak diizinkan.

    2. Baca - USB diperbolehkan, tetapi konten tidak dapat ditulis ke USB (Anda dapat menyalin file dan membuka file di USB).

    3. Baca/tulis – Setara dengan tidak ada kontrol.

    4. Peringatan – Kirim alarm saat USB dimasukkan, fungsi alarm peristiwa dari perangkat perlu diaktifkan.

  - **Refined control dari perangkat portabel:**

    1. Izinkan – Setara dengan tidak mengontrol.

    2. Nonaktifkan – Melarang akses.

    3. Peringatan – Kirim alarm ketika dimasukkan, fungsi alarm peristiwa perangkat perlu diaktifkan.

2.2 Langkah Implementasi

1. Instal ingress client di endpoint (saat ini hanya mendukung Windows).

2. Ingress client terhubung ke perangkat IAG dan mendistribusikan policy ke lokal (pengguna diperlukan untuk online di IAG).

3. Dua metode kontrol:

   - Dengan menggunakan system group policy untuk melarang instalasi driver untuk peripheral, Jadi untuk mencapai tujuan pengendalian peripheral (Sistem Windows XP dan sistem versi home tidak memiliki group policy sehingga tidak mendukung external device control).

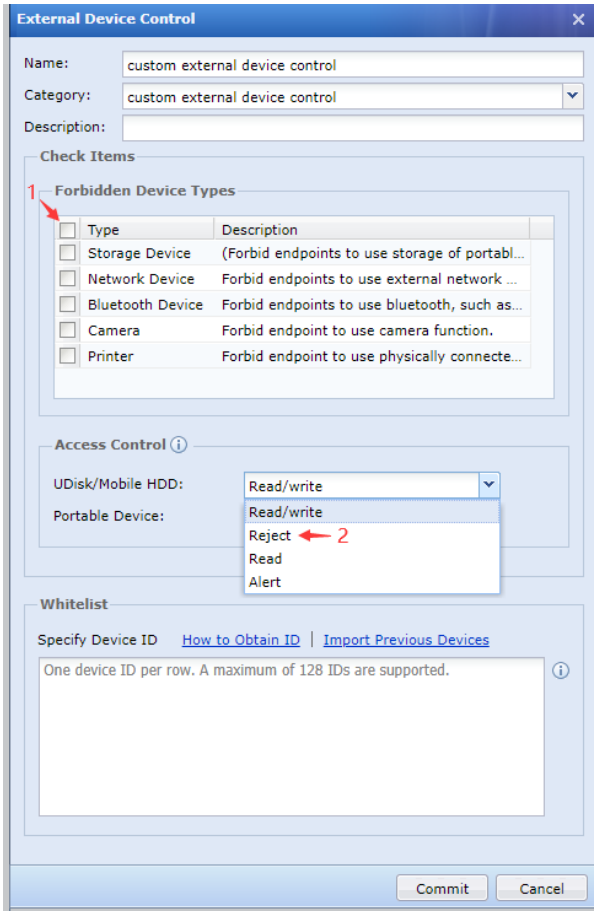
   - Refined control, gunakan fungsi system device manager dan proses metode injeksi untuk mencapai refined control dari USB dan perangkat portabel (hanya mendukung Win7 dan OS di atasnya, terlepas dari apakah itu adalah home versi).

4. Ketika ingress client dan IAG tidak dapat berkomunikasi dengan satu sama lain, metode kontrol group policy masih memiliki efek, dan fungsi kontrol dapat terus diimplementasikan (refined control tidak mengambil efek).

Dua cara untuk menonaktifkan:

1. Metode group policy : gunakan system group policy untuk implementasikan, kontrol pengaktifan dan menonaktifkan fungsi, dikendalikan oleh 1 pada gambar di bawah.

2. Implementasi dari refined management dan kontrol: gunakan fungsi system device manager dan menonaktifkannya, konfigurasi seperti yang ditunjukkan di 2 pada gambar di bawah ini.



Jika Anda memilih 1, dua metode penonaktifan akan berlaku pada saat yang sama, dan group policy akan digunakan pertama untuk menonaktifkan. Dalam menonaktifkan skenario kegagalan (skenario pengguna domain, home versi tidak memiliki skenario group policy), gunakan perangkat nonaktifkan metode untuk melarang; jika Anda memilih 2 untuk menolak, ini menggunakan perangkat manager untuk menonaktifkan metode.

Pengaturan Whitelist:

1. Whitelist perlu mengisi hardware ID dari perangkat peripheral, Anda dapat merujuk ke perangkat ID memperoleh panduan.

2. Hardware ID terdiri dari hardware IDE dari tiap perangkat dan patriline komputer, oleh karena itu hardware ID dari setiap perangkat peripheral pada masing-masing komputer berbeda.

3. Fungsi quick import dari perangkat sebelumnya hanya efektif bagi USB dan hard disk portabel. Lainnya seperti perangkat network, perangkat Bluetooth, etc. tidak mendukung quick import dan perlu menggunakan alat.

4. Metode penggunaan alat dapat diperoleh dari perangkat ID mendapatkan panduan.

Bab 3 Skenario Aplikasi

Fungsi external device control sebagian besar digunakan ketika endpoint memiliki akses ilegal ke peripheral, seperti memasukkan USB untuk menyalin data, memasukkan wireless network card untuk mengakses external network, etc., yang dapat melarang endpoint dari sambungan pribadi ke peripheral.

Bab 4 Konfigurasi

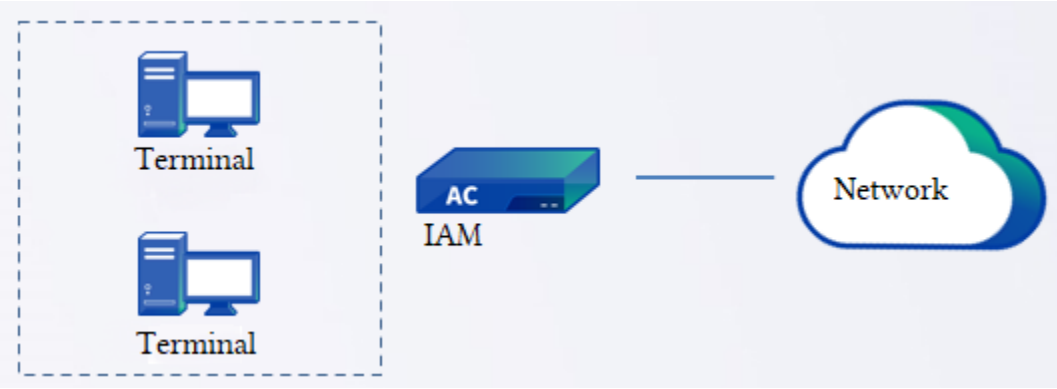
4.1 Langkah Konfigurasi:

1. Buat baru external device control policy dan konfigurasi secara spesifik periksa item atau kontrol item.

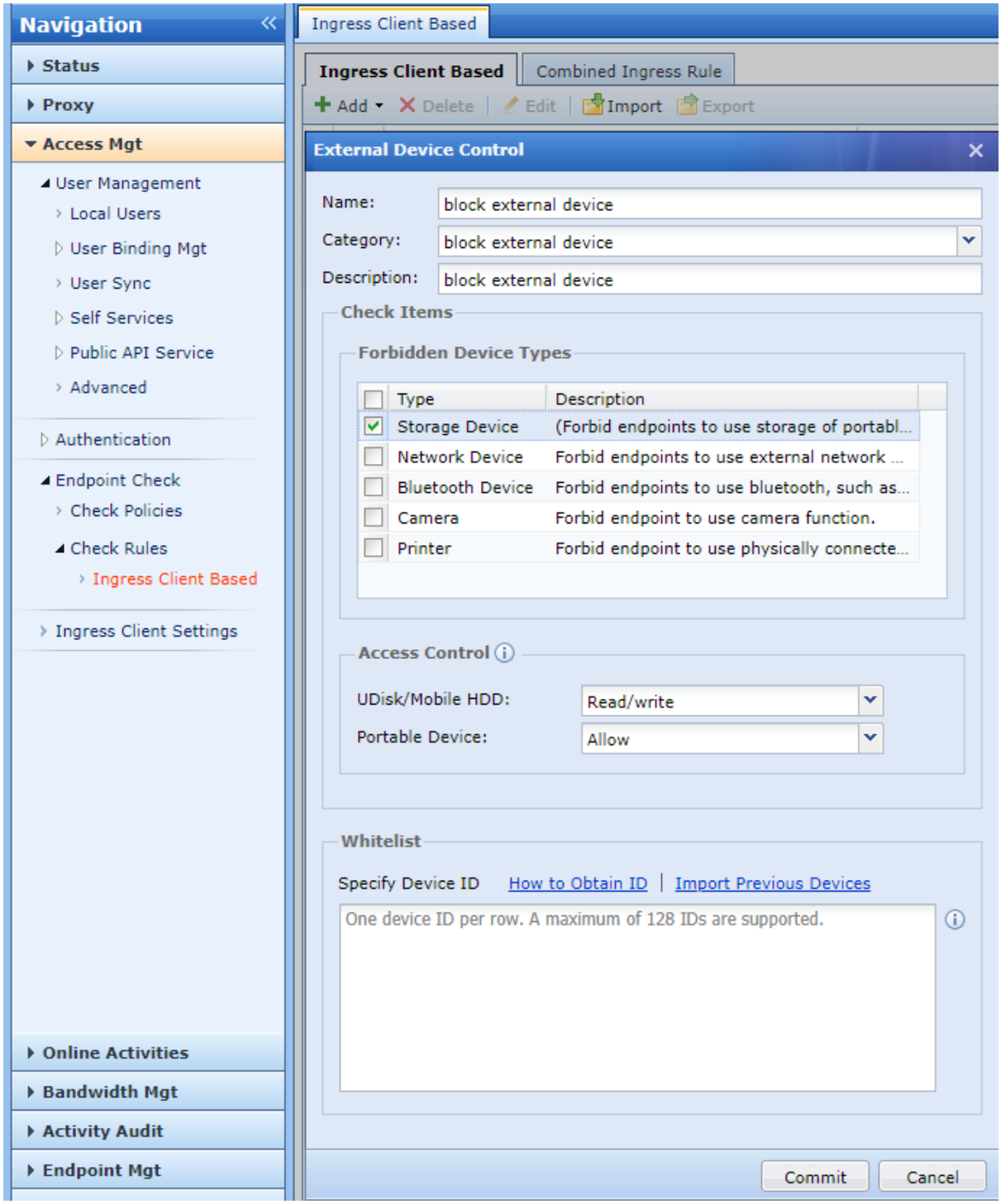
2. Konfigurasi endpoint periksa policy, mengasosiasikan dengan policy yang dikonfigurasi sebelumnya, dan pilih pengguna yang dapat diterapkan.

4.2 Kasus Konfigurasi:

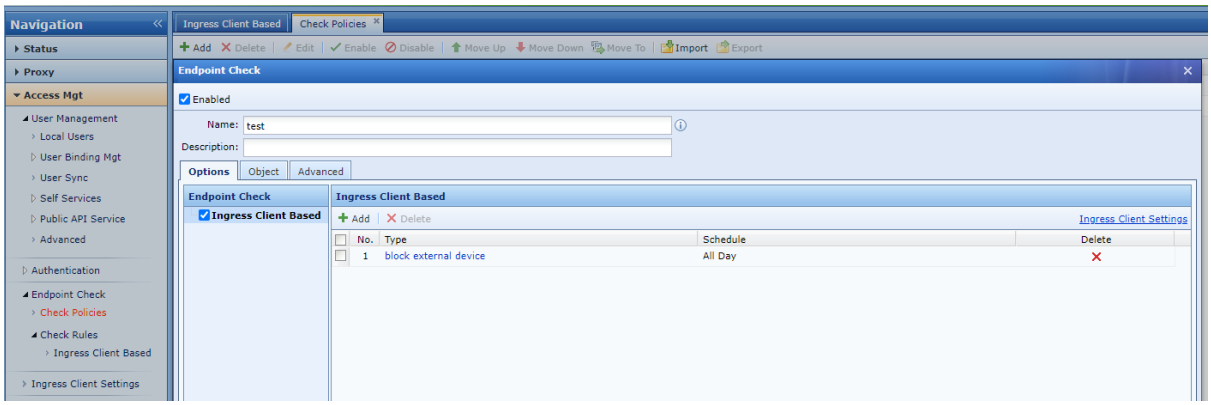
Network pribadi pelanggan menyebarkan IAG, endpoints dilarang mengakses perangkat seperti USB dan hard drive portabel.



Buat baru external device control policy, definisi name, category dan description, dan kemudian centang storage device.



Buat baru endpoint periksa policy dan mengasosiasikan dengan policy yang dikonfigurasi sebelumnya dan pilih pengguna yang dapat diterapkan.



Bab 5 Tindakan Pencegahan

1. Terminal hanya dapat memperoleh policy setelah melewati autentikasi, dan ingress client harus diinstal untuk fungsi kontrol perangkat eksternal.

2. Tidak boleh ada NAT di jalur dari terminal ke perangkat IAG. Jika ada NAT, fungsi periksa endpoint tidak akan berpengaruh.

3. Sistem Windows XP dan semua keluarga versi sistem tidak memiliki group policies, dan tidak mendukung metode group policy control.

4. Refined control hanya mendukung Win7 dan di atasnya, terlepas dari apakah itu home versi.

5. Gunakan group policy untuk menonaktifkan storage device. Jika komputer memiliki hard disk internal non-USB kedua selain disk sistem, itu juga akan dinonaktifkan. Perlu menambahkan whitelist untuk mengizinkannya.

6. Group policy saat ini tidak kompatibel dengan 360 Tianqing. Jangan gunakan group policy untuk kontrol lingkungan peripheral dengan Tianqing.

7. Refined management dan control hanya untuk storage devices dengan antarmuka USB : USB portabel perangkat hard disk portabel.

8. Gabungan aturan ingress tidak berlaku untuk aturan external device control (gabungan aturan ingress untuk yang lama aturan ingress seperti proses dan aturan berbasis file).

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