Cyber Command

Praktik Terbaik untuk Konfigurasi_Bagaimana untuk Berkorelasi dengan IAM untuk Operasi Sederhana

Versi 3.0.49

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Mei 7, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

Daftar Isi

Bab 1 Dasar

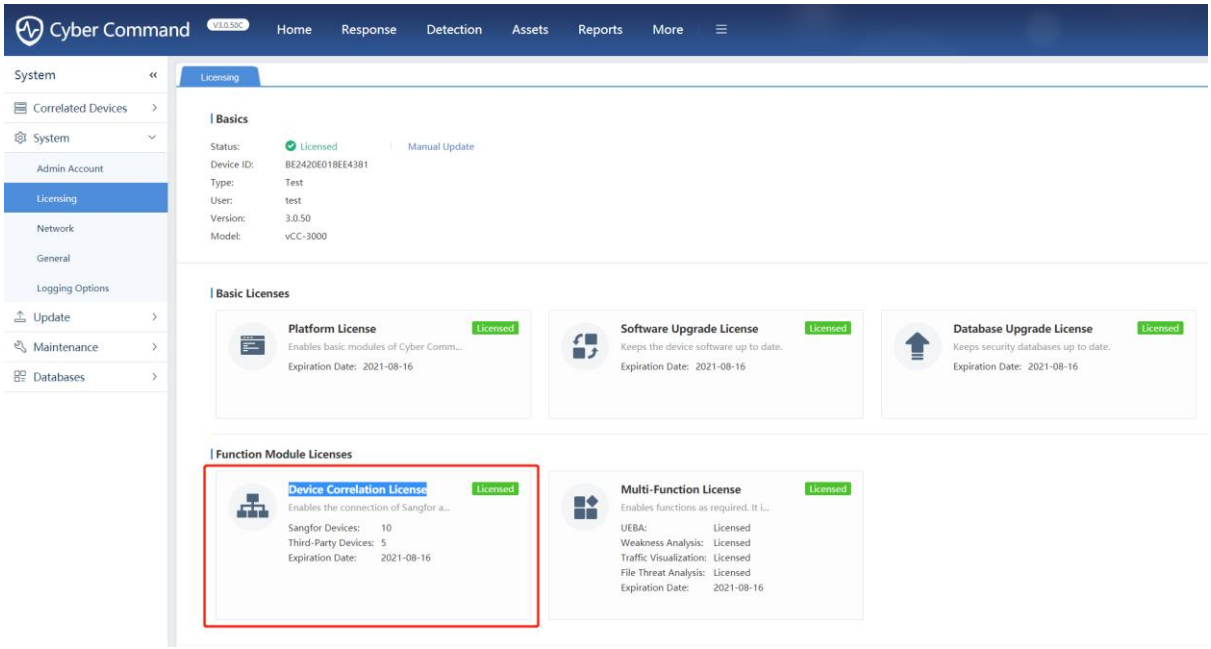
Dokumen terkait:

Praktik Terbaik untuk Konfigurasi termasuk pilihan mode deployment, ide konfigurasi, koleksi informasi, keterbatasan fungsi, perbedaan versi. Mengenai ***How to Correlate with IAM to Simply the Operation***, jika Anda ingin mempelajari tentang skenario POC umumnya dan langkah konfigurasi terperinci, silakan merujuk ke link berikut:

https://sangforltd.sharepoint.com/:w:/s/PMO/EUz4ij5rR99MiWk7fc6OSW8BlwV-ifkW9O5JCkX8khbndA?e=BPeTgf

1.1 Konfirmasi Dasar Konfigurasi dan Deployment

1. Konfirmasi apakah CCOM telah mengaktifkan Device Correlation License.

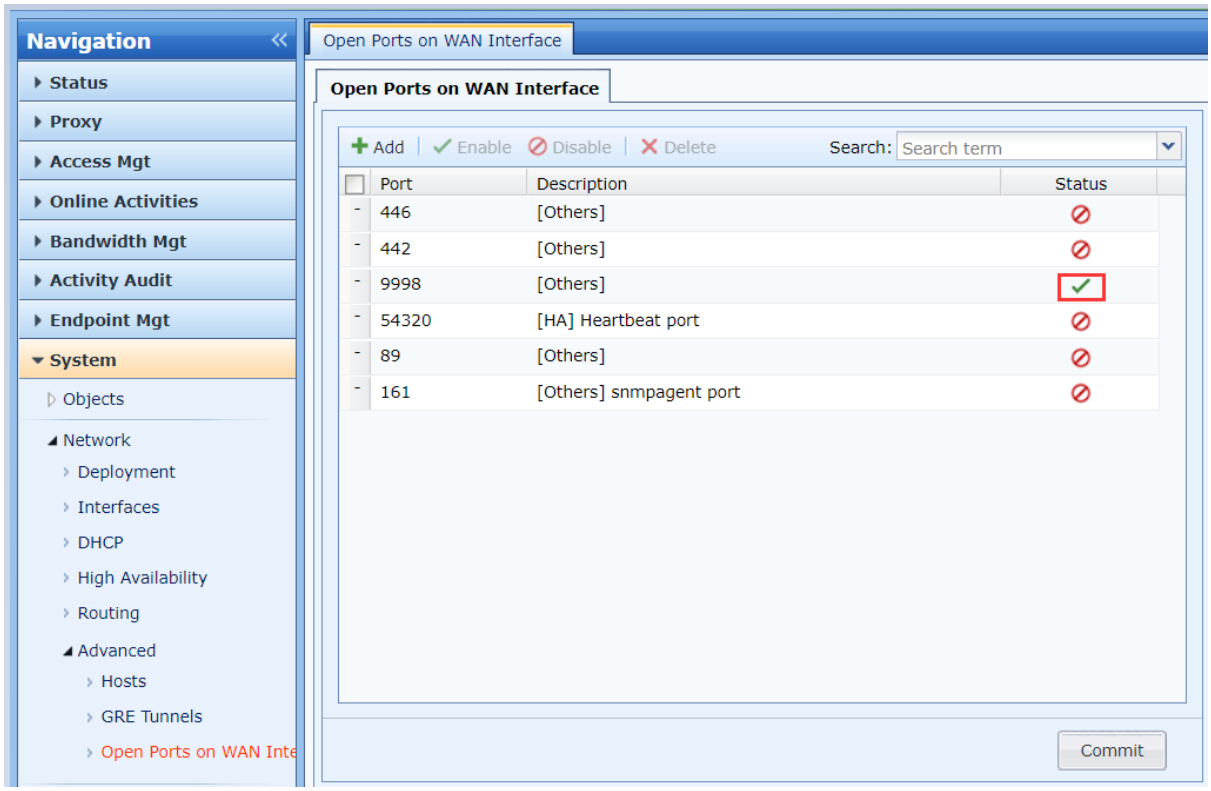


2. Konfirmasi topologi network, seperti apakah CC dan IAG dapat berkomunikasi, apakah route dapat dijangkau, dan apakah ada perangkat NAT di tengah.

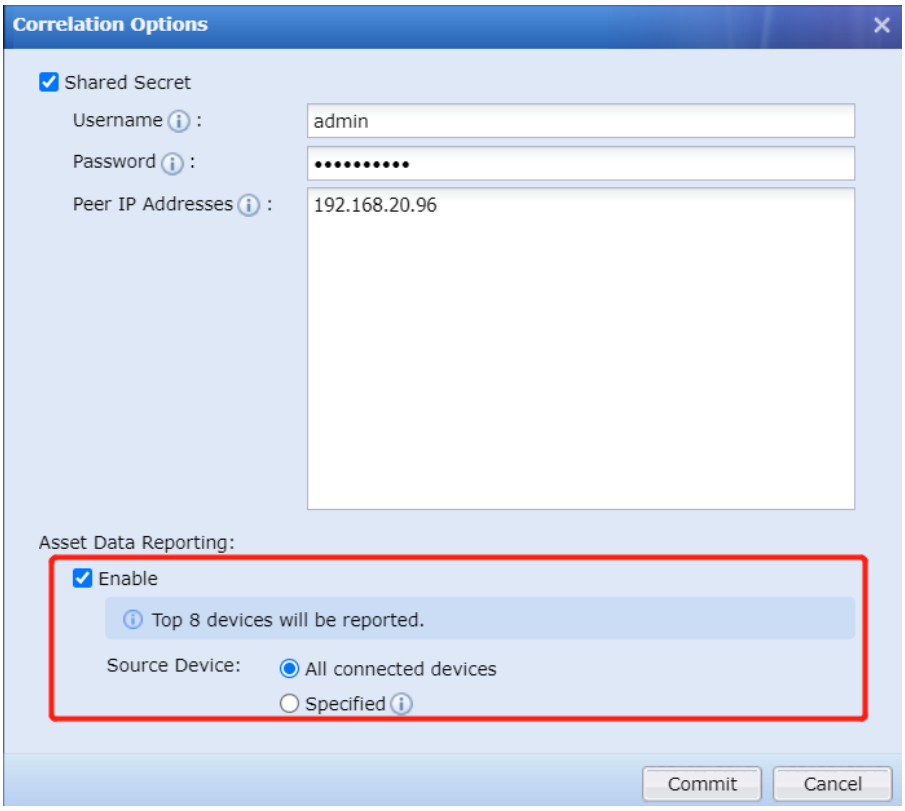
3. Ketika IAG berkorelasi dengan CC, itu perlu dikonfigurasi pada IAG dan CC secara bersamaan.

4. IAG mengakses port 1775 (UDP, digunakan untuk sinkronisasi pengguna) dari CC, dan CC mengakses TCP port 7443 dan port 9998 dari IAG. Jika terkoneksi IP address perangkat diterjemahkan, enter IP address diterjemahkan.

5. Jika IAG deploy dalam mode routing, dan CC terkoneksi ke IP port WAN IAG untuk berkomunikasi dengan IAG, maka port perlu dibuka pada IAG.



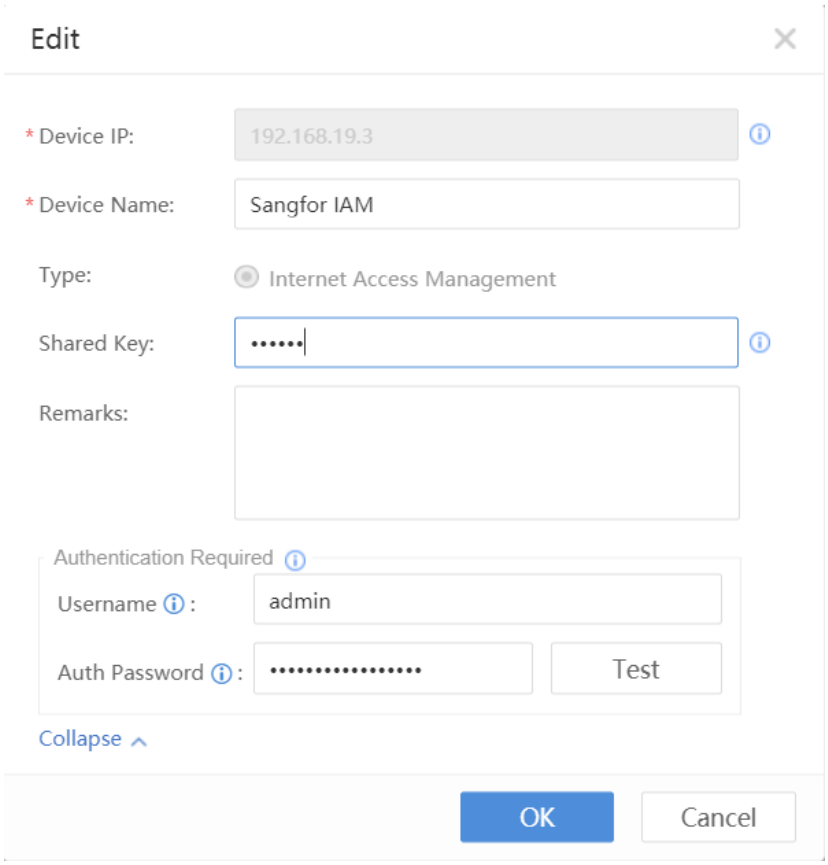
6. IAG mendukung laporan assets ke CC dimulai dari versi 13.0.15, yang perlu diaktifkan dalam pengaturan korelasi. Pengguna dan password di sini bukan akun dan password console CC atau IAG, Anda dapat kustom.



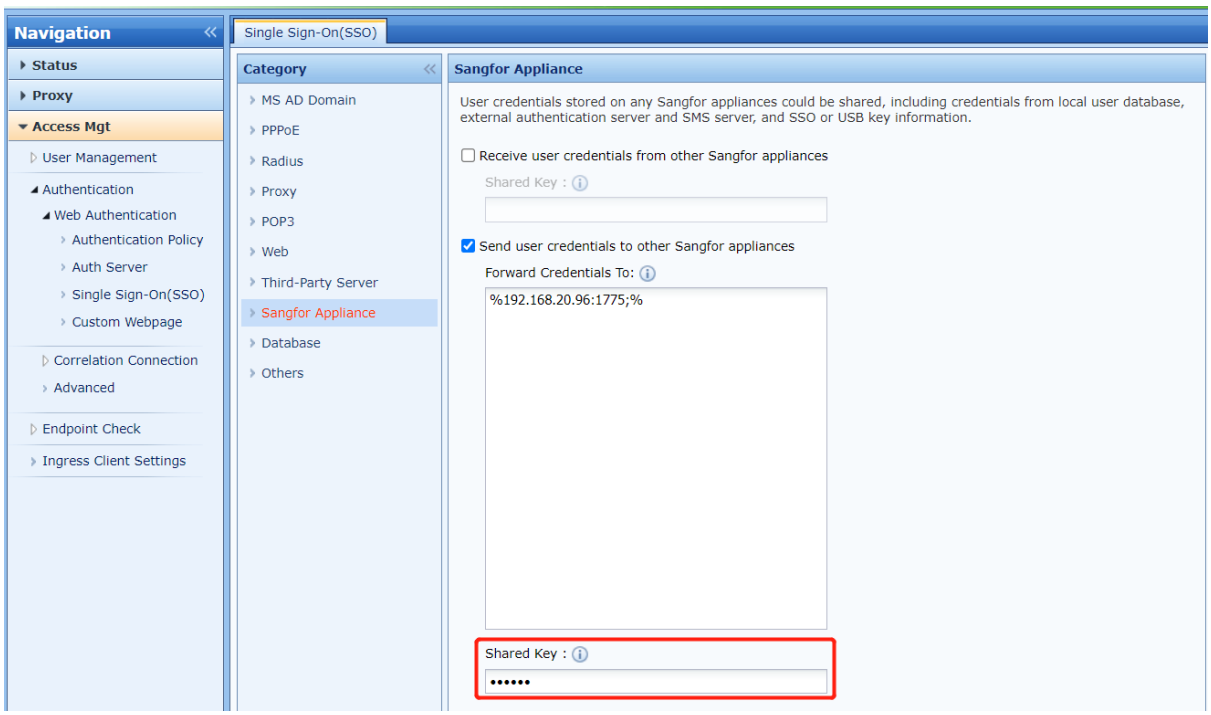
7. Jika Anda perlu sinkronisasi pengguna online di IAG ke CC, Anda harus konfigurasi Sangfor Appliance di IAG, dan shared secret key harus konsisten dengan shared secret key dalam konfigurasi linkage di CC.

Sangfor IAG forwarding authentication adalah untuk foward informasi authentication dari lokal password authentication, external password authentication, SMS authentication, single sign-on, dan pengguna dkey authentication. Itu tidak akan forward informasi dari Open Pengguna Authentication ke CC.

CC Side:



IAG Side:



1.2 Fungsi Korelasi

1. Setelah IAG terkoneksi ke CC, CC dikaitkan dengan IAG untuk Browsing Rik Pemberitahuan, yang dapat mengingatkan pengguna dari insiden security ditemukan oleh terminal melalui redireksi web, dan kemudian freeze pengguna yang telah menemukan masalah security untuk mengurangi dampak permukaan ancaman.

2. IAG dapat mendeteksi botnet, tetapi IAG tidak upload security log ke CC. Oleh karena itu, IAG dan CC biasanya tidak digunakan sendiri, tetapi ES digunakan untuk memeriksa lebih lanjut security terminal.

3. Jika Anda ingin dapat secara otomatis berkoordinasi dengan IAG untuk menangani ancaman setelah CC menemukannya, jangan lupa untuk konfigurasi automatic response policy pada CC.

4. CC berkorelasi dengan IAG terutama digunakan untuk mendeteksi high-risk host, dan kemudian mengeluarkan policy untuk freeze pengguna. Jadi harap pastikan bahwa pengguna yang di frozen berada di daftar pengguna online IAG. Jika pengguna tidak termasuk pengguna online, freezing policy akan tidak valid.