



IAM

Proxy SSO Panduan Konfigurasi

Version 12.0.18



Perubahan Catatan

Tanggal	Deskripsi Perubahan
12 Desember 2019	Dokumen rilis Versi 12.0.18.

Daftar Isi

Bab 1 Pengenalan Fungsi.....	1
1.1 Skenario Aplikasi.....	1
1.2 Deskripsi yang diperlukan.....	1
1.3 Panduan Konfigurasi.....	1
1.4 Konfigurasi and Gambar.....	1
1.4.1 Proxy Server di zona Wan.....	1
1.4.1.1 Proses Aliran Data.....	1
1.4.1.2 Panduan Konfigurasi.....	2
1.4.2 Proxy Server di zona LAN.....	2
1.4.2.1 Proses Aliran Data.....	3
1.4.3.1 Proses Aliran Data.....	4
1.4.3.2 Panduan Konfigurasi.....	4
Bab 2 Perhatian.....	6
2.1 Proxy Server di zona WAN.....	6
2.2 Proxy Server di zona LAN.....	6
2.3 Menggunakan Metode Kontrol ISA.....	6

Bab 1 Pengenalan Fungsi

Secara umum berlaku untuk lingkungan dimana pengguna menggunakan proxy untuk menjelajahi internet, dan setiap pengguna diberi akun dari proxy server. Saat menggunakan metode autentikasi single sign-on proxy, ketika pengguna melewati autentikasi proxy server, perangkat juga melewati autentikasi.

1.1 Skenario Aplikasi

Secara umum berlaku untuk lingkungan dimana pengguna menggunakan proxy untuk menjelajahi internet, dan setiap pengguna diberi akun dari proxy server. Saat menggunakan metode autentikasi single sign-on proxy, ketika pengguna melewati autentikasi proxy server, perangkat juga melewati autentikasi.

1.2 Deskripsi yang diperlukan

1. Perangkat IAM 11.0.
2. Lan menggunakan proxy ke Internet.

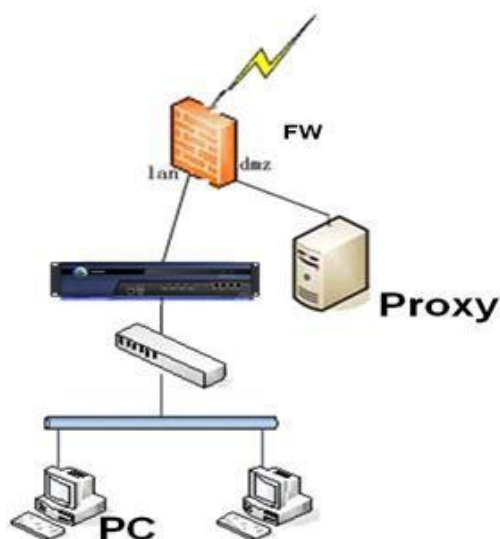
1.3 Panduan Konfigurasi

1. Proxy server di arah Wan.
2. Proxy server di arah Lan.
3. Menggunakan Pengontrol ISA.

1.4 Konfigurasi and Gambar

1.4.1 Proxy Server di zona Wan

Proxy single sign on dengan mode pemantauan dapat juga selesai single sign-on dengan memantau masuk data. Proxy Server ada di arah jaringan eksternal, seperti yang ditunjukkan pada gambar:



1.4.1.1 Proses Aliran Data

1. Pengguna pergi online melalui proxy server, dan perangkat memantau interaksi antara PC dan proxy server.

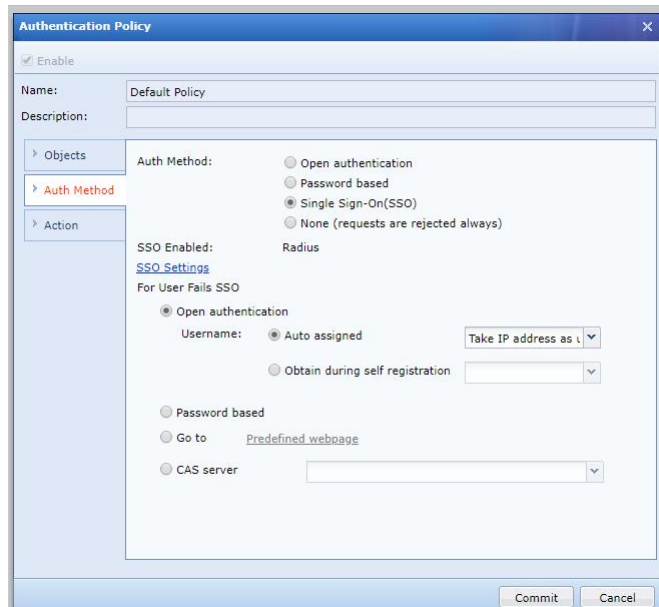
2. PC berhasil diautentikasi oleh proxy server serta perangkatnya.

1.4.1.2 Panduan Konfigurasi

1. Mengatur kebijakan autentikasi.

Mengatur kebijakan autentikasi untuk ip pengguna SSO yang diperlukan atau alamat mac

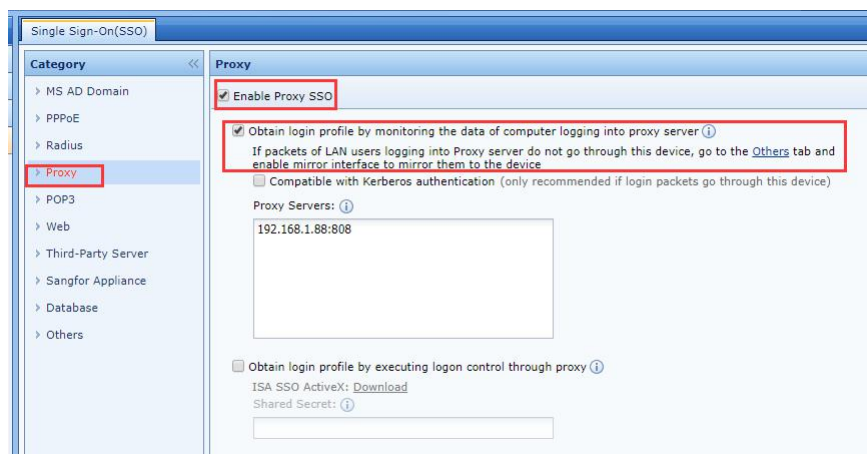
All styles have been created, you can just click to paint the fonts.



2. Konfigurasi Proxy SSO.

Masuk ke [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], periksa [Enable proxy SSO] dan klik untuk [Memperoleh masuk profil dengan memantau data komputer yang masuk ke proxy server]

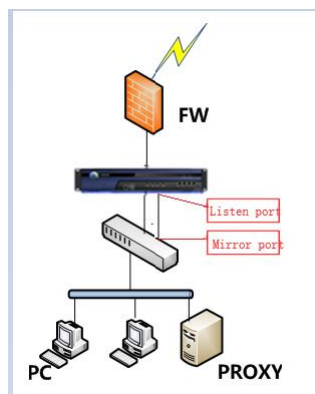
Di dalam [Proxy Server], masukkan ip Proxy Server dan mendengarkan port jika memiliki banyak proxy server, ini perlu menambahkan baris demi baris, disini kita masukkan Proxy server dan mendengarkan port.



3. Tes Masuk.

PC masuk ke Proxy server, setelah masuk berhasil akan online.

1.4.2 Proxy Server di zona LAN



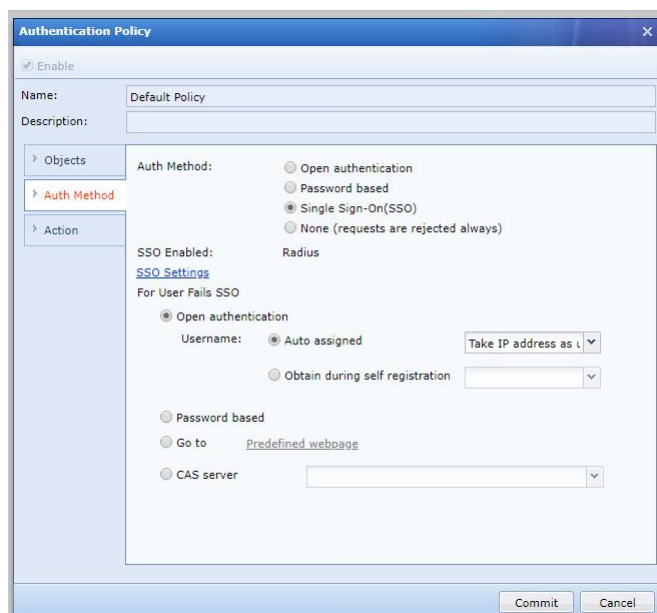
1.4.2.1 Proses Aliran Data

1. Pengguna pergi online melalui proxy server, dan data autentikasi tidak diteruskan oleh IAM.
2. Konfigurasi mirror port di switch untuk mirror data dari PC ke proxy server ke IAM.
3. PC berhasil diautentikasi oleh proxy server serta perangkatnya.

1.4.2.2 Panduan Konfigurasi

1. Langkah Konfigurasi
Mengatur Kebijakan Autentikasi

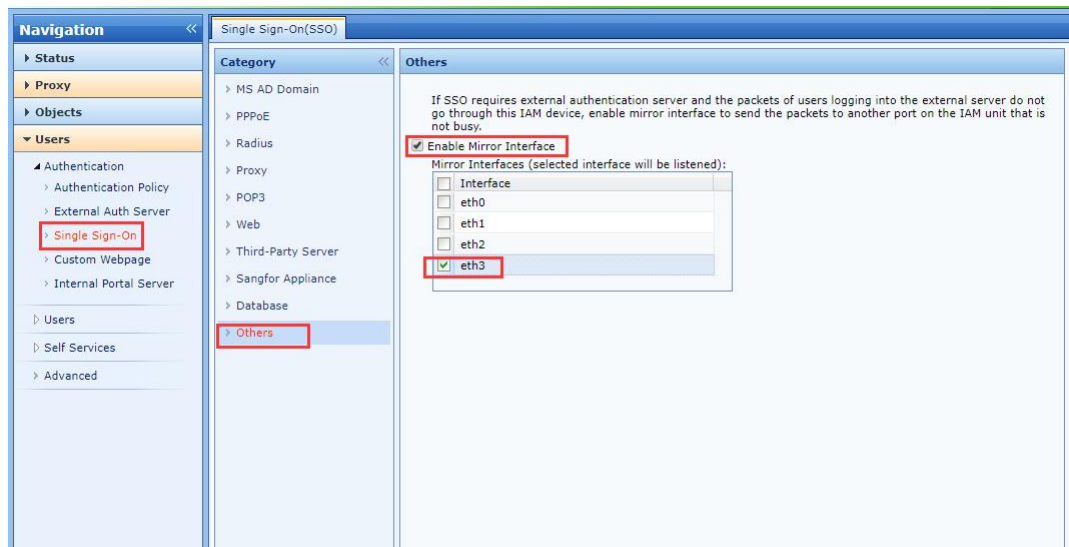
Mengatur kebijakan autentikasi untuk ip pengguna SSO yang diperlukan atau alamat mac.



2. Konfigurasi Proxy SSO

Masuk ke [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], periksa [Enable proxy SSO] dan klik untuk [Memperoleh masuk profil dengan memantau data komputer yang masuk ke proxy server]

Di dalam [Proxy Server], masukkan ip Proxy Server dan mendengarkan port jika memiliki banyak proxy server, ini perlu menambahkan baris demi baris, jika masuk data tidak melewati perangkat, anda perlu mengatur mirror port dan menghubungkan mirror port ke mirror port dari switch yang meneruskan masuk data. Klik opsi lain untuk mengatur mirror port dari perangkat. Mirror port perlu di atur sebagai port jaringan gratis. Jangan tetapkan port jaringan sebagai mirror port jaringan.

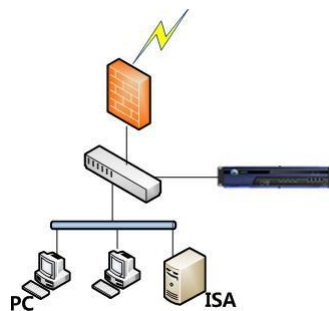


3. Tes Masuk

PC masuk ke Proxy server, setelah masuk berhasil akan online.

1.4.3 Menggunakan Metode ISA

Metode kontrol ISA dapat digunakan untuk server ISA di jaringan internal. Ketika data masuk ke ISA tidak melewati perangkat, plug-in ekstensi terdaftar di server ISA, dan informasi setelah PC masuk ke ISA diberitahukan ke perangkat melalui plug-in tambahan. Masuk pada perangkat. Seperti gambar dibawah ini:



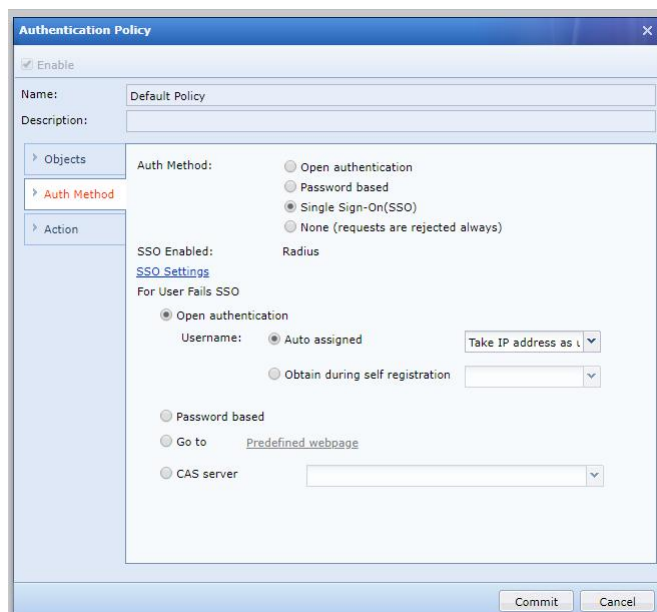
1.4.3.1 Proses Aliran Data

1. PC melewati proxy HTTP dan autentikasi proxy dari ISA;
2. ISA mengirimkan informasi bahwa PC berhasil masuk ke perangkat IAM;
3. IAM peralatan secara otomatis melewati autentikasi PC dan melepaskan data internet PC.

1.4.3.2 Panduan Konfigurasi

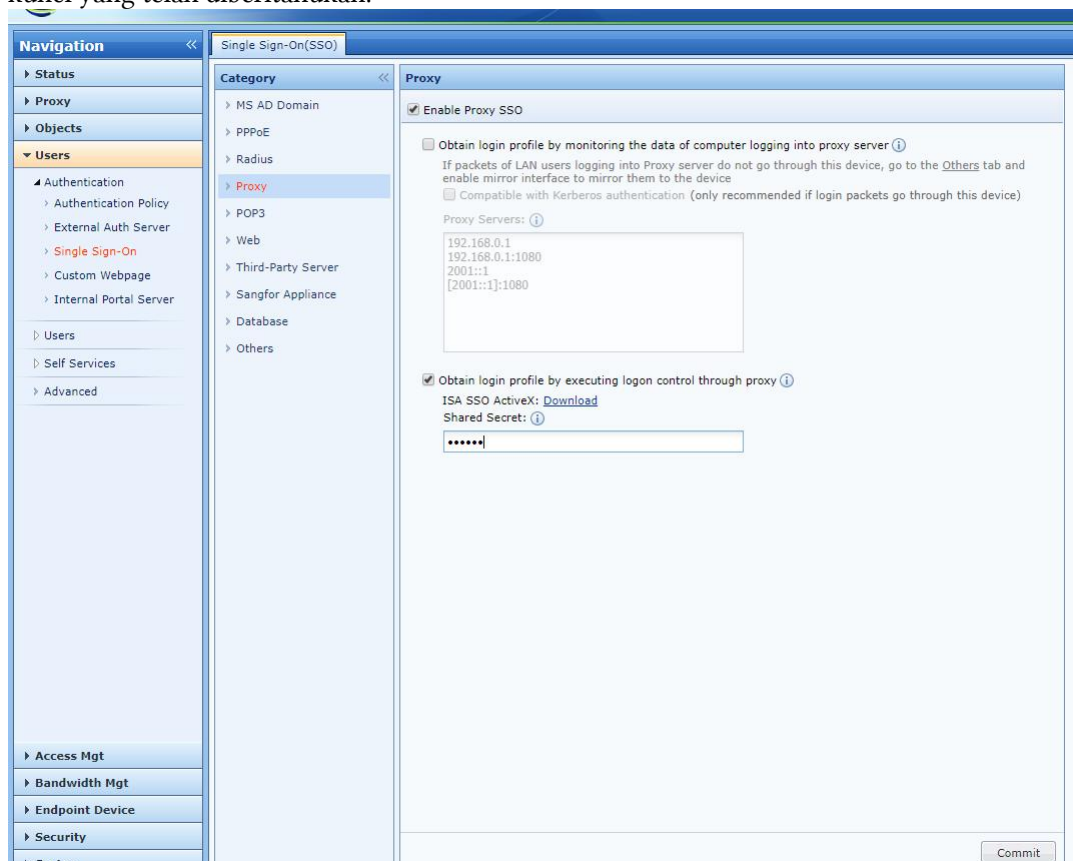
1. Mengatur kebijakan autentikasi

Mengatur kebijakan autentikasi untuk ip pengguna SSO yang diperlukan atau alamat mac.



2. Konfigurasi Proxy SSO

Masuk ke [Users] -> [Authentication] -> [Single Sign on] -> [Proxy], periksa [Enable proxy SSO] dan klik untuk [Memperoleh profil masuk dengan menjalankan kontrol masuk melalui proxy] dan masukkan kunci yang telah diberitahukan.



1.4.3.3 Konfigurasi Kontrol ISA Single Sign-on

Unduh ISA single sign-on kontrol dan contoh di perangkat, konfigurasi server ISA, daftarkan plug-in, dan konfigurasi SangforAC.ini.

1. Plugin MyAuthFilter.dll ditempatkan di direktori instalasi ISA, seperti C: \ Program Files \ ISA Server \
2. Jalankan regsvr32 "C: \ Program Files \ ISA Server \ MyAuthFilter.dll" XML plugin

3. Taruh itu sampel konfigurasi SangforAC.ini di root direktori drive C. [Konfigurasi]

IAMip = 192.168.0.1 alat IP address

kunci = 123 Paket data enkripsi kunci untuk masuk ke ISA, yang harus sama dengan yang disetel di perangkat

putaran = 30 interval minimum (satuan: detik) untuk setiap IP address mengirim masuk paket data.

Tujuannya adalah untuk mencegah setiap IP address mengirim masuk paket data setiap saat sesi baru diakses ke situs website baru.

logpath = debug log path. Jika kosong, ini berarti log dimatikan. Jika sudah diisi, ini berarti log dihidupkan. Setel ke nonaktif. Silahkan nyalakan bila perlu.

maxlogsize = 1 Ukuran maksimal dari debug file log (satuan: MB). Ketika file log mencapai level sebelumnya, ini akan dikosongkan secara otomatis.

charset = UTF-8 supports UTF-8, UTF-16, GB2312, GB18030, BIG5

Konfirmasikan bahwa "Sangfor ISA Auth Filter" plugin diaktifkan ISA panel plugin.

Tes masuk

PC masuk ke Proxy server, setelah masuk berhasil akan online.

Bab 2 Perhatian

2.1 Proxy Server di zona WAN

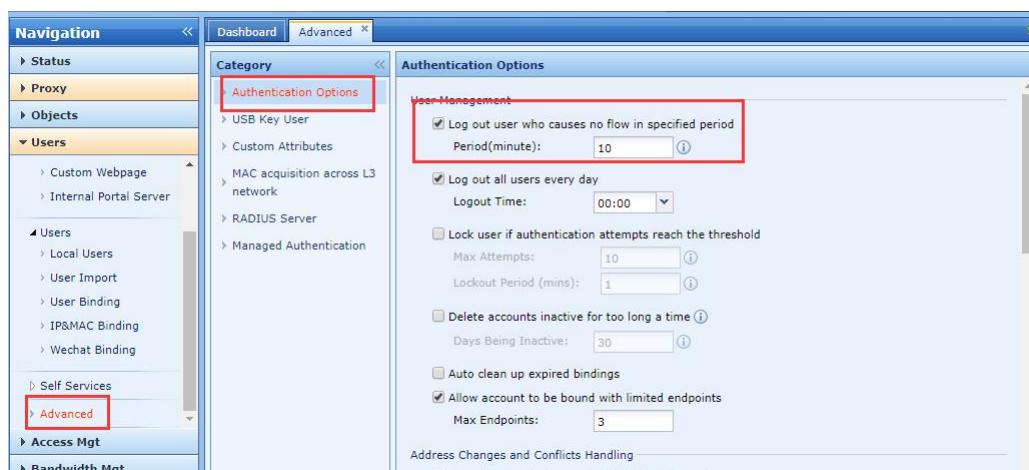
1. Jika proxy server adalah server ISA dan server ISA menggunakan "windows integrated identity authentication" metode, Anda perlu memeriksa [Kompatibel dengan metode autentikasi kerberos] untuk menyelesaikan single sign-on, dan metode ini hanya berlaku untuk paket masuk yang melewati perangkat AC dalam kasus ini, ini tidak berlaku untuk mirror mode, dan tidak didukung dalam bypass mode.
2. Dalam skenario ini, Jika [Tampilan peringatan] dipilih di [Authentication Policy] → [Post-Authentication Processing] → [Advanced Options], Anda perlu mengkonfigurasi pengalihan dari port DMZ, jika tidak Anda tidak akan dapat mengakses Internet melalui autentikasi.

2.2 Proxy Server di zona LAN

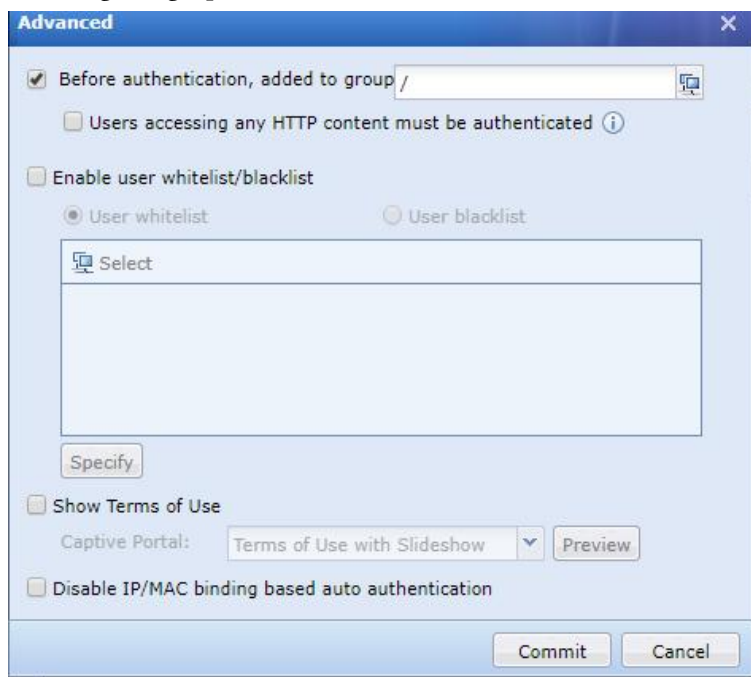
Jenis login ini data tidak melewati IAM, dan metode pemantauan yang menggunakan mirror data tidak mendukung [Kompatibel metode autentikasi Kerberos]

2.3 Menggunakan Metode Kontrol ISA

1. Setiap saat Anda memodifikasi file SangforAC.ini, Anda perlu mendaftarkan ulang plugin.
2. Plug-in ISA tidak dapat mengaktifkan pengguna domain untuk secara otomatis keluar perangkat saat pengguna domain keluar atau mematikan komputer. Namun, Anda dapat atur periode waktu tunggu di konsol perangkat agar pengguna secara otomatis keluar dari perangkat. Seperti gambar dibawah ini:



3. Kunci server IAM dan ISA harus sama, dan kunci ini tidak boleh sama dengan kunci single sign-on .
4. Server ISA harus merilis data yang terhubung ke port UDP 1773 dari perangkat IAM.
5. Jika proxy server berada di area IAM WAN, Anda harus memberikan akses ke proxy server sebelum autentikasi pengguna.
6. Bagaimana memberikan izin?
- 7 . Di [Authentication Policy]-[Action]-[Advanced], periksa [Before authentication, added to group] dan mengatur grup.



Teruskan IP dan port proxy server di setelan izin internet grup pengguna ini.



Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc.

SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing.

Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.