



IAM

Panduan Konfigurasi Otentikasi CAS

Versi 12.0.18



Perubahan Catatan

Tanggal	Deskripsi Perubahan
Dec 24, 2019	Rilis dokumen versi 12.0.18.

Daftar Isi

Bagian 1 Requirement.....	1
1 Pengenalan Produk.....	1
2 Skenario aplikasi.....	1
3 Persyaratan kondisi.....	1
4 Ide konfigurasi.....	1
5 Panduan konfigurasi dengan Screenshot.....	1
5.1 Pengecekan topologi dan kebutuhan lainnya.....	1
5.2 Konfigurasi External Auth Server.....	2
5.3 Konfigurasi Authentication Policy.....	2
5.4 Hasil pengujian.....	3
6 Tindakan pencegahan.....	3

Bagian 1 Requirement

1 Pengenalan Produk

IAM berkomunikasi dengan server CAS untuk mengimplementasikan otentifikasi password dengan pihak ketiga.

2 Skenario aplikasi

Klien telah melakukan pemasangan server CAS (Central authentication server) pada jaringan mereka, server CAS melindungi informasi ID pengguna dan kata sandi internal. Saat ini klien melakukan implementasi perangkat IAM pada jaringan mereka dan mereka ingin mengaktifkan otentikasi kata sandi di IAM, tetapi menggunakan data kredensial di server CAS untuk otentikasi kata sandi pihak ketiga.

3 Persyaratan kondisi

1. Perangkat IAM menggunakan versi firmware 12.0.18 atau di atasnya.
2. Menyiapkan sebuah PC yang dapat berkomunikasi pada jaringan.
3. Klien telah melakukan instalasi CAS server, klien memberikan akun untuk melakukan pengujian serta memberikan link otentikasi CAS, misalnya <https://ip:8443/CAS/login>.

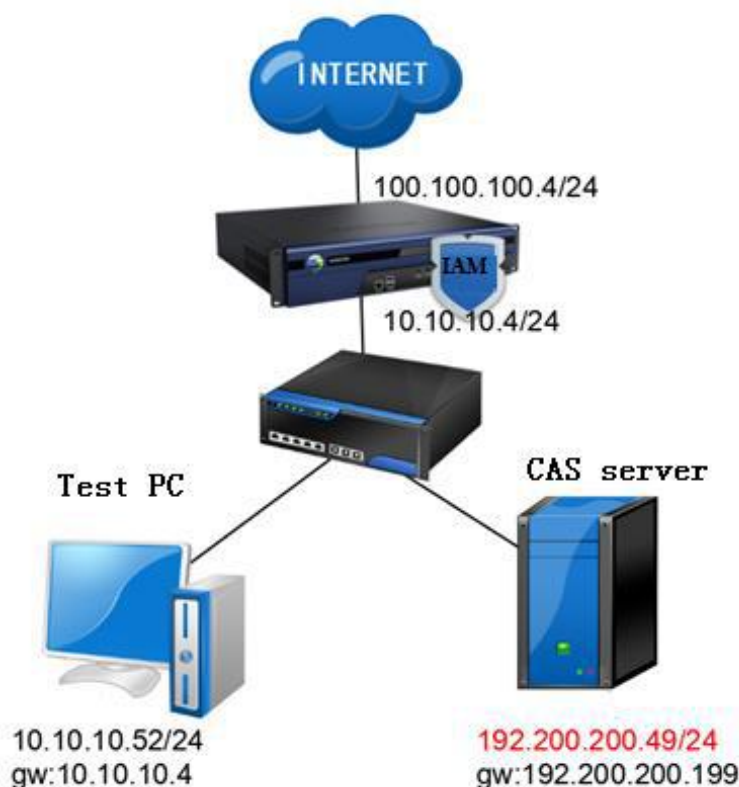
4 Ide konfigurasi

1. Melakukan konfigurasi External Authentication Server pada perangkat IAM.
2. Melakukan konfigurasi Authentication Policy pada perangkat IAM.

5 Panduan konfigurasi dengan Screenshot

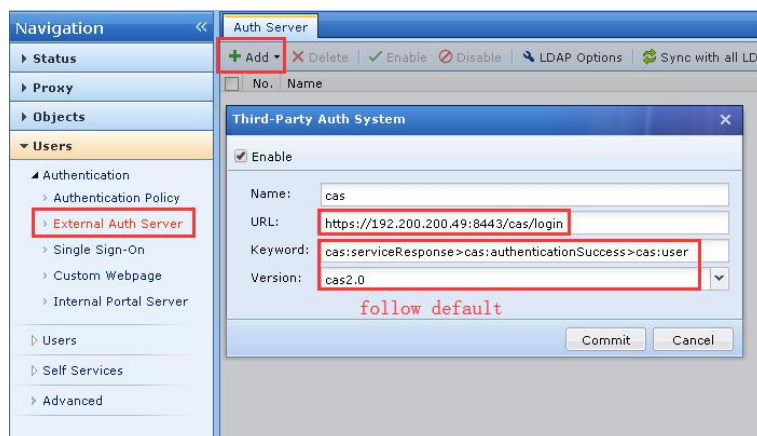
5.1 Pengecekan topologi dan kebutuhan lainnya

Mode implementasi pada ruang lingkup pengujian ini adalah Route mode.



5.2 Konfigurasi External Auth Server

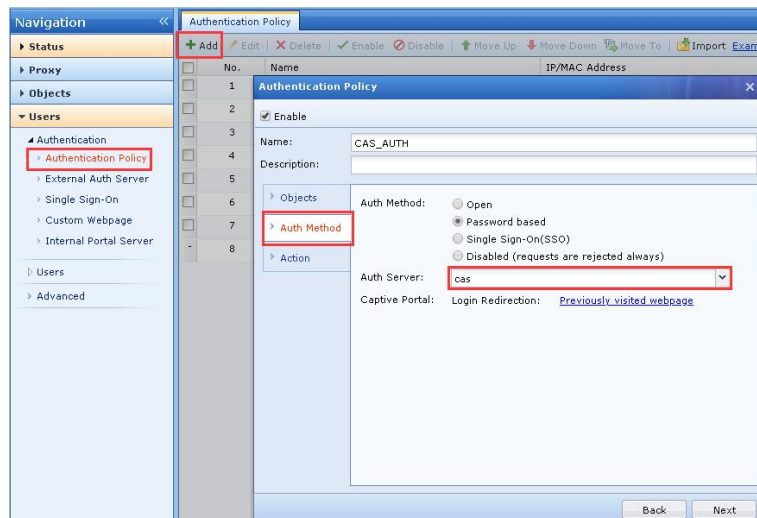
Untuk melakukan konfigurasi server otentikasi eksternal, anda dapat mengikuti langkah-langkah pada diagram di bawah ini. Isi [URL] dengan link otentikasi server CAS dan bagian [keyword] serta [version] akan mengikuti nilai default.



Catatan: Check versi dapat memilih cas2.0 atau cas 3.0. CAS server dengan versi V4.0.0 dan versi sebelumnya akan menggunakan protokol cas2.0, selain versi tersebut akan menggunakan protokol cas3.0.

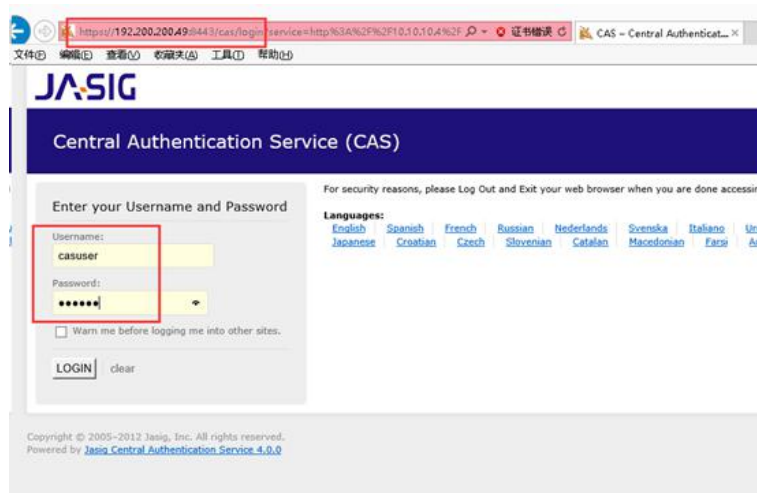
5.3 Konfigurasi Authentication Policy

Untuk konfigurasi Authentication Policy, pastikan bahwa anda dapat memahami objek otentikasi sebelum melakukan konfigurasi kebijakan, pilih [password based] sebagai metode otentikasi, pada bagian [Auth Server] pilih CAS server yang telah dibuat sebelumnya.



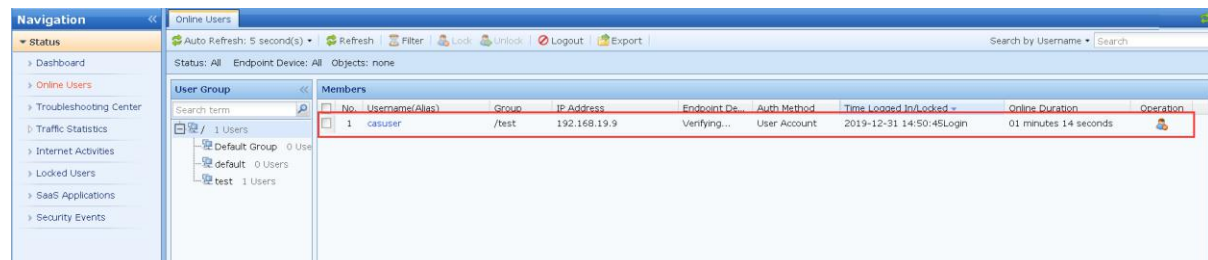
5.4 Hasil pengujian

Gunakan PC internal untuk mulai melakukan browsing internet untuk menuju ke halaman otentikasi CAS, kemudian masukkan username dan password dan kemudian hasil otentikasi akan berhasil.



Catatan : nama pengguna dan kata sandi CAS pada umumnya didefinisikan dalam file `deploterConfigContext.xml` di direktori instalasi CAS, akun pengguna biasanya ditentukan oleh pelanggan, anda dapat meminta akun pengujian dari klien.

Pada diagram dibawah ini, kita dapat melihat bahwa PC telah login pada perangkat IAM.



6 Tindakan pencegahan

Klik **tambah** dan periksa [Social Media Account]

1. Mode implementasi Route dan bridge dapat mendukung otentikasi menggunakan server CAS.
1. Apabila server CAS berada di jaringan external IAM, kita perlu menambahkan alamat server CAS ke global exclusion list, apabila tidak kita lakukan, maka tidak dapat dilakukan akses ke halaman

otentikasi CAS.



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.