



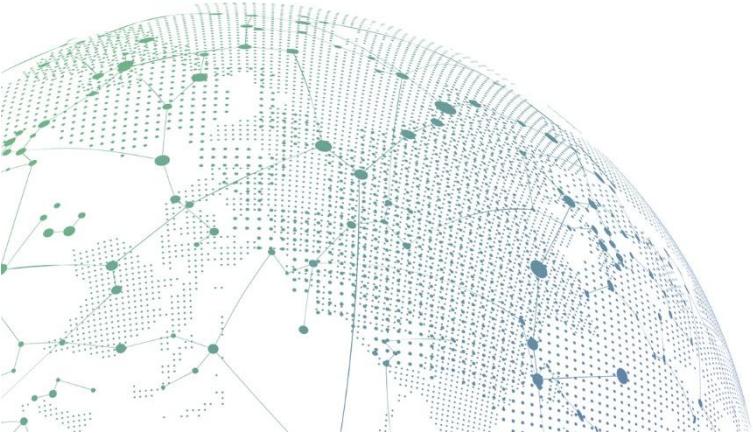
SANGFOR



IAM

MAC Open Authentication Configuration Guide

Version 12.0.18



Catatan Perubahan

Tanggal	Deskripsi Perubahan
6 Desember 2019	Versi 12.0.18 Rilis Dokumen

Konten

1 Skenario Aplikasi.....	1
2 Konfigurasi dan Tangkapan Layar.....	1
3 Uji Coba Hasil.....	3

1 Skenario Aplikasi

Pada IAM versi 12.0.18 dengan konfigurasi bridge, autentikasi berbasis kata sandi digunakan untuk pengguna intranet. Saat setelah login pertama kali menggunakan autentikasi akun kata sandi dan tidak ingin membutuhkan memasukan kata sandi untuk login selanjutnya dan dapat mengakses internet secara langsung. Perangkat tidak bisa menggunakan cookie-based authentication dan berharap bisa mencapai autentikasi terbuka menggunakan autentikasi berbasis Mac address.

Persyaratan:

1. Perangkat IAM 12.0.18
2. Satu PC ujicoba dengan IP Address ujicoba 192.168.19.6
3. Setelah pengguna terautentikasi untuk pertama kali menggunakan binding Mac addresses pengguna, pengguna tidak lagi membutuhkan untuk memasukan akun dan kata sandi untuk akses internet selanjutnya.
4. Setelah pengguna melakukan autentikasi kata sandi pertama kali, mereka bisa langsung mengakses internet terlepas dari IP address nya berubah atau cache pada browser telah dibersihkan.

2 Konfigurasi dan Tangkapan Layar

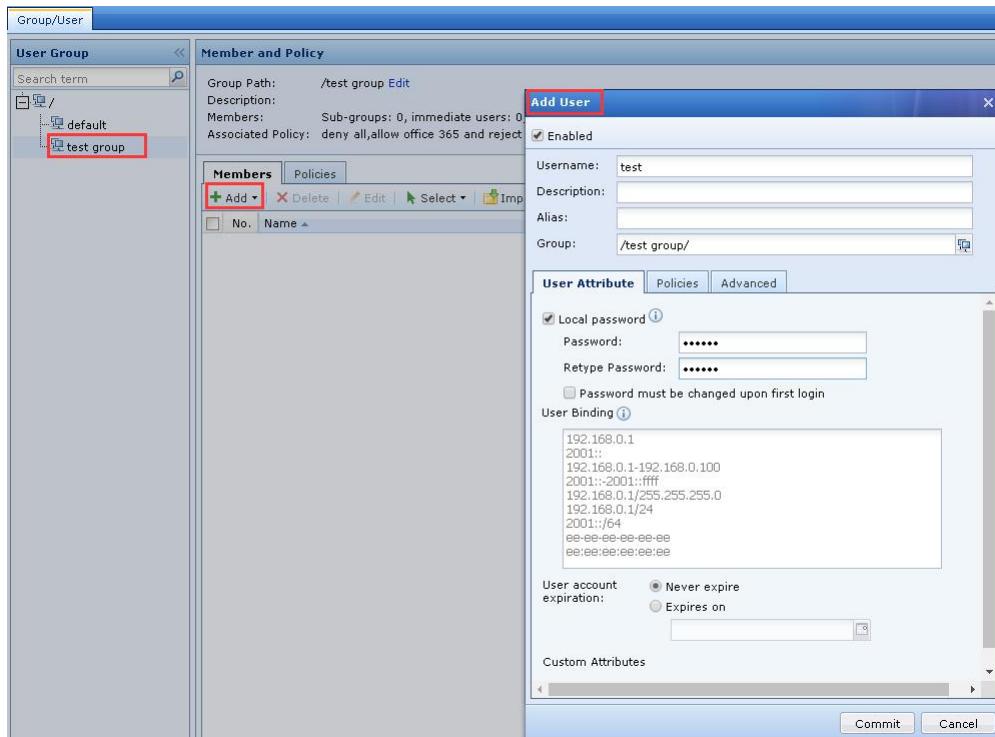
Langkah 1: Buat sebuah grup baru dan pengguna, dan konfigurasi nama pengguna dan kata sandi untuk pengguna tersebut.

Buat sebuah grup baru di bawah [Users]-[Users]-[Local Users] dan beri nama “test group”.

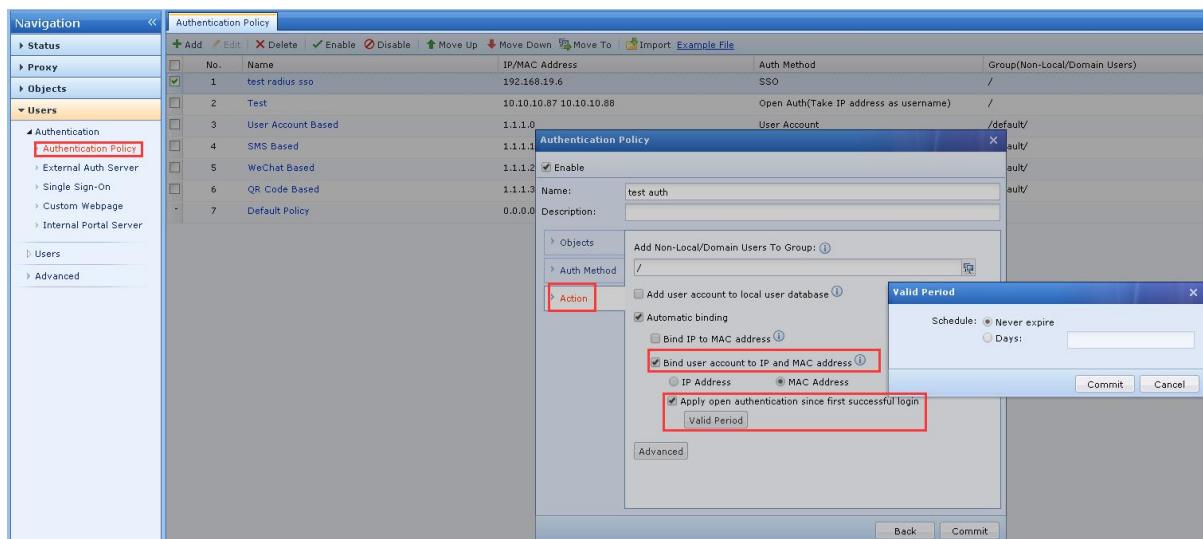
No.	Name	Policies	User Binding
1	default	deny all,Non-working related applications...	-
2	test group	deny all,allow office 365 and reject outlo...	-

Buat sebuah akun baru kedalam “test group” akun dan kata sandi nya: test/123456.

IAM Configuration Guide



Langkah 2: Konfigurasi authentication policy, tambahkan sebuah authentication policy baru di [Users]-[Authentication Policy], isi pengaplikasian IP address: 192.168.19.6, pilih password based authentication untuk metode autentikasi, melalui aksi pemilihan [Bind user account to IP and Mac Address]-[Mac Address] dan kemudian ceklist pilihan [Apply open authentication since first succesful login], dan pilih [Valid Period] sebagai “Never expire” disini dan klik “commit”



Langkah 3: Pada saat pengguna akan online untuk pertama kali, masukan nama pengguna dan kata sandi serta tampilan “User Account” di [Online Users].

No need to tick

Remember me

Log In

Navigation

- Status
- Dashboard
- Online Users
- Troubleshooting Center
- Traffic Statistics
- Internet Activities
- Locked Users

User Group

Members
1 Users
default 0 Users
test group 1 Users

Members

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method
1	test	/test group	192.168.19.6	Verifying...	User Account

Langkah 4: Pengecekan hubungan Binding pengguna, di [Users]-[Users]-[Users Binding]

Authentication Policy User Binding Online Users Group/User

Add Edit Delete Advanced Advanced Search Select Import Export Example File Error Reports

Search by Username

Filter By fe-fc-fe-8a-34-10

Added Since 2019-12-06

Open Authentication Enable (Never expire)

Binding akan terlihat ketika pengguna melakukan autentikasi untuk pertama kali, perangkat akan otomatis melakukan binding terhadap MAC pengguna dan autentifikasi terbuka juga diaktifkan.

3 Uji Coba Hasil

Setelah perangkat online untuk pertama kali menggunakan autentikasi berbasis kata sandi, mereka dapat langsung mengakses internet setelah keluar jika mereka tidak melakukan pembersihan pada cache browser.

Keluarkan pengguna yang telah melakukan autentikasi menggunakan fungsi “Log out all users every day” dan lakukan online kembali.

Untuk konfigurasi “Log out all users every day” atau “Log out user who causes no flow in specified period” di [Users]-[Advanced]-[Authentication Options]-[Users Management], lakukan konfigurasi di [Log out all users every day] atau [Log out user who causes no flow in specified period], dan tunggu pengguna keluar sistem sebelum melakukan online kembali.

Navigation

- Status
- Proxy
- Objects
- Users
- Authentication
- External Auth Server
- Single Sign-On
- Custom Webpage
- Internal Portal Server
- Users
- Local Users
- User Import
- User Binding
- IP&MAC Binding
- Advanced

Authentication Policy User Binding Online Users Group/User Advanced

Category Authentication Options

User Management

Log out user who causes no flow in specified period
Period(minute): 120

Log out all users every day
Logout Time: 00:00

Lock user if authentication attempts reach the threshold
Max Attempts: 10
Lockout Period (mins): 1

Delete accounts inactive for too long a time
Days Being Inactive: 30

Auto remove MAC bindings when open authentication expires

Allow account to be bound with limited endpoints
Max Endpoints: 5

Address Changes and Conflicts Handling

IAM Configuration Guide

The screenshot shows the IAM Configuration Guide interface. The left sidebar has a 'Status' section with links like Dashboard, Online Users (which is selected), Troubleshooting Center, Traffic Statistics, Internet Activities, Locked Users, and Security Events. The main area has tabs for Authentication Policy, User Binding, Online Users (selected), Group/User, and Advanced. Under Online Users, there are buttons for Auto Refresh (5 seconds), Refresh, Filter, Lock, Unlock, and Logout. Below these are status filters: Status: All, Endpoint Device: All, Objects: none. A search bar and a tree view for User Group show '1 Users' under 'default' and 'test group'. The Members table lists one user: No. 1, Username(Alias) test, Group /test group, IP Address 192.168.19.6, Endpoint Device Verifying..., Auth Method Open, and Time Logged In/Out 2019-12-06 12:03:3. The 'Auth Method' and 'Time Logged In/Out' columns are highlighted with red boxes.

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Out
1	test	/test group	192.168.19.6	Verifying...	Open	2019-12-06 12:03:3



SANGFOR

Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang.
Dilarang menyebarluaskan 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.