SANGFOR

IAM

MAC Open Authentication Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 6, 2019	Version 12.0.18 document release.

CONTENT

1 Application Scenario 1
2 Configuration and Screenshots 1
3 Test Result 3
4 Precautions 5

1 Application Scenario

IAM 12.0.18 bridge deployment, password based authentication for intranet users. Want to achieve that after the first login of the account password authentication, do not need to enter the password next time when accessing Internet and can directly access the Internet. The mobile endpoint cannot operate well at cookie-based authentication, and hope to achieve open authentication based on the MAC address.

Requirements:

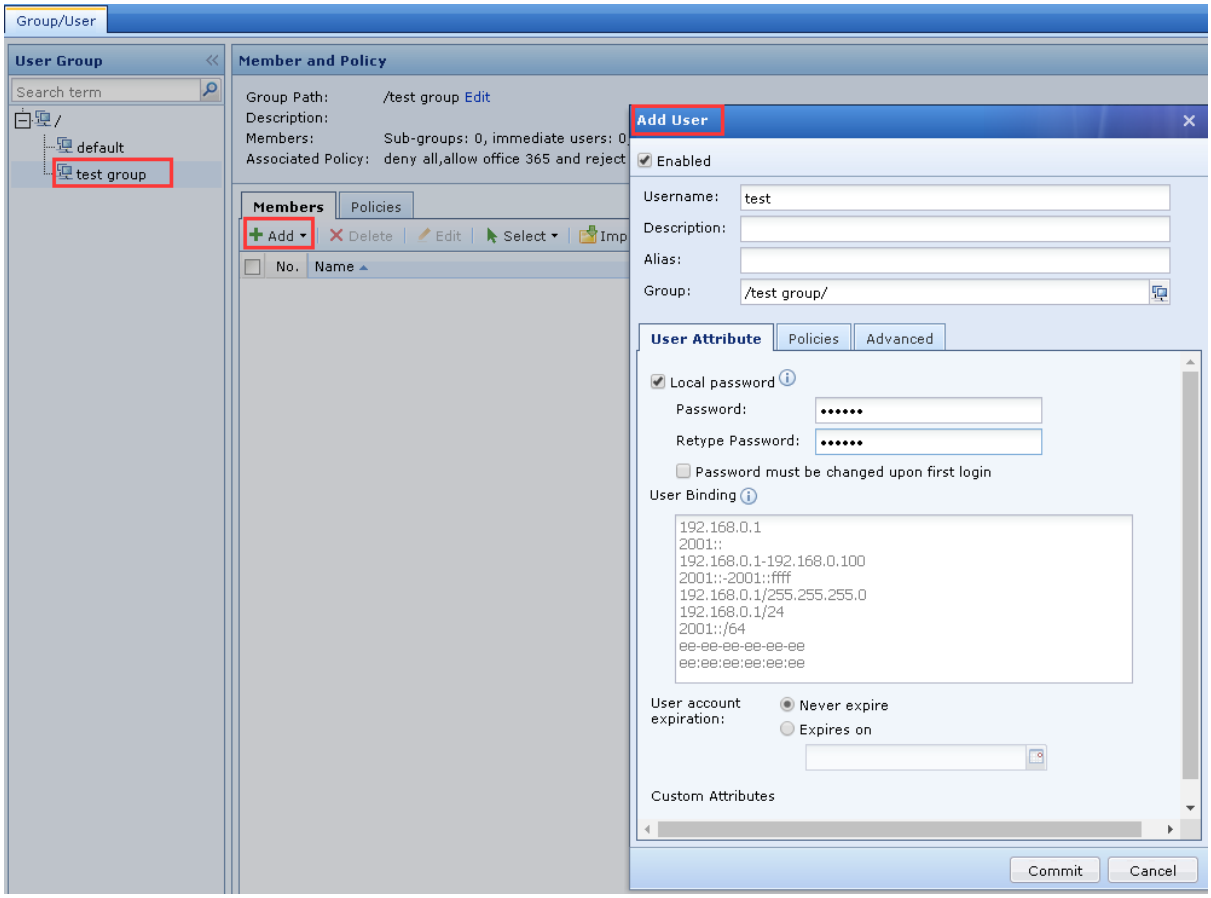
1. One IAM 12.0.18.
2. One testing PC, the test IP address is 192.168.19.6.
3. After the user is authenticated for the first time by binding the user's MAC address, the user does not need to enter the account and password for the next Internet access.
4. After the user performs the password authentication for the first time, they can directly access the Internet regardless of whether the IP changes or the browser cache is cleared.

2 Configuration and Screenshots

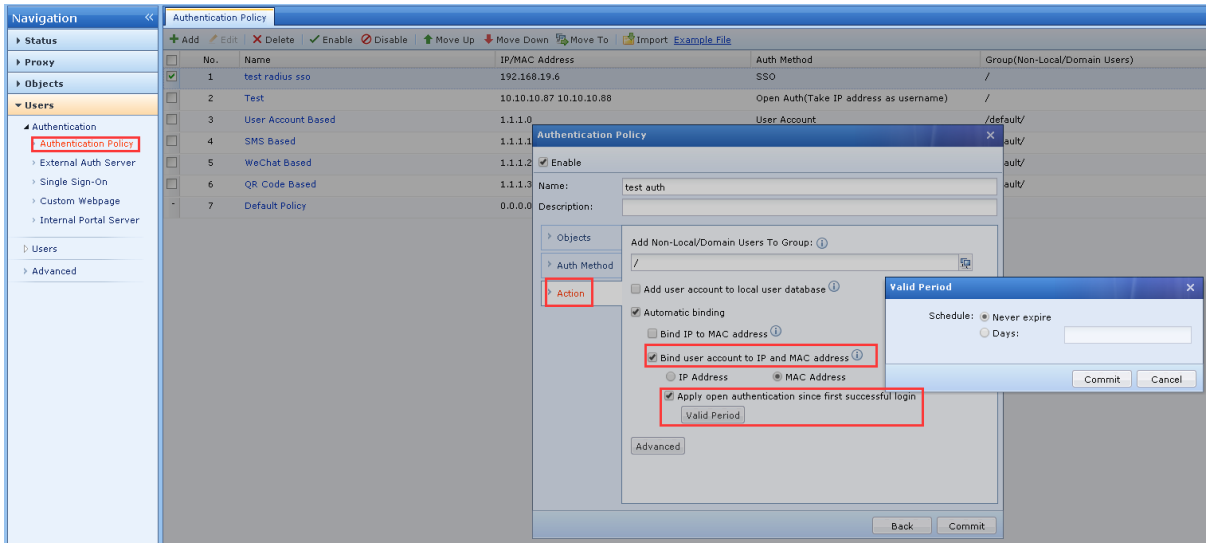
Step 1: Create a new group and user, and configure the user name and password for the user.

Create a new group under [Users]-[Users]-[Local Users] and name it as “test group”.

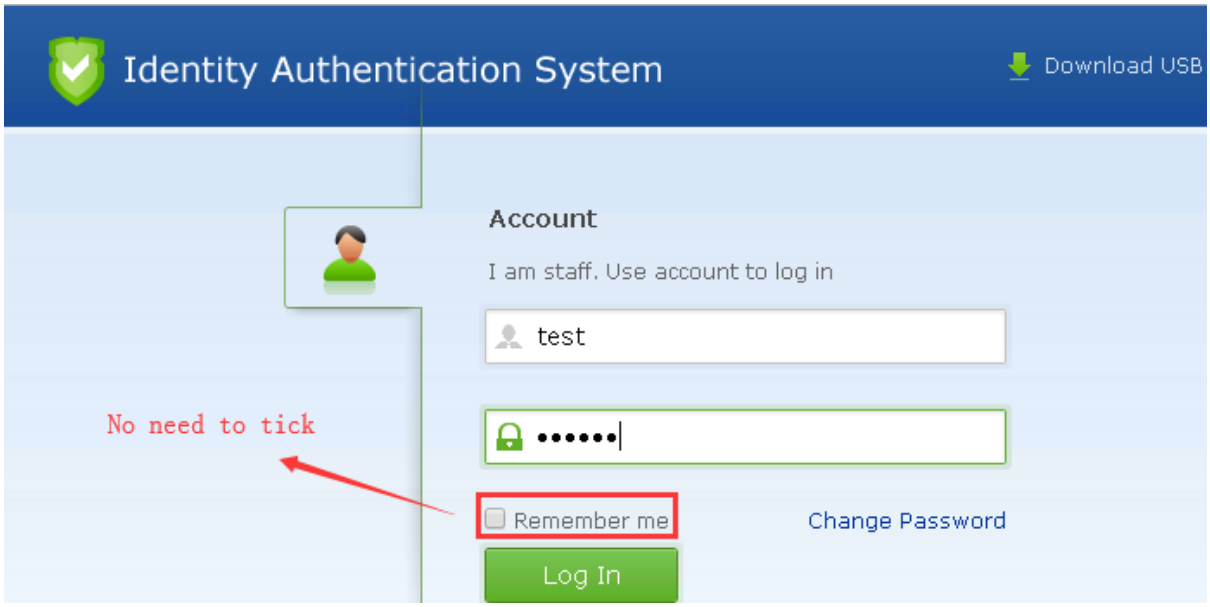
Create a new account in the “test group”, the account and password is: test/123456.

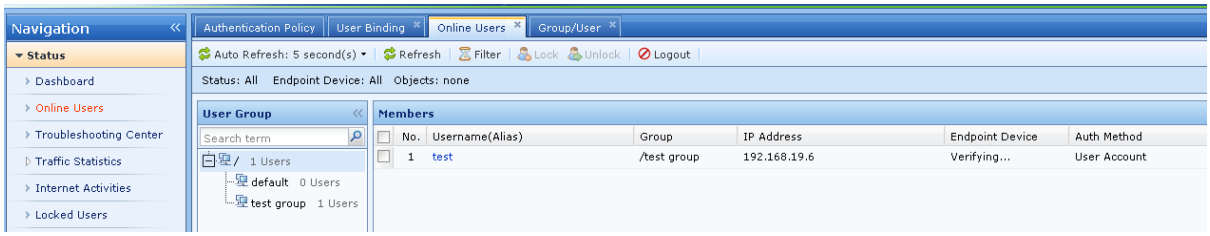


Step 2: Configure the authentication policy, add a new authentication policy in [Users]-[Authentication Policy], fill in the applicable IP: 192.168.19.6, select password based authentication for the authentication method, in the action select [Bind user account to IP and MAC address]-[MAC Address] and then check [Apply open authentication since first successful login], and select [Valid Period] as "Never expire" here, and click "Commit".

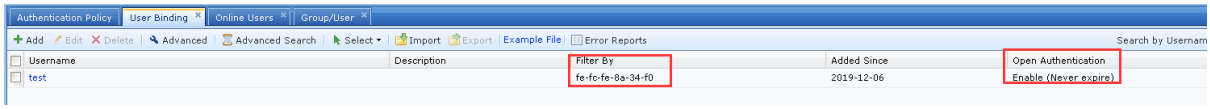


Step 3: The user goes online for the first time, enters the user name and password, and displays "User Account" in [Online Users].





Step 4: Check the user binding relationship, in [Users]-[Users]-[User Binding].



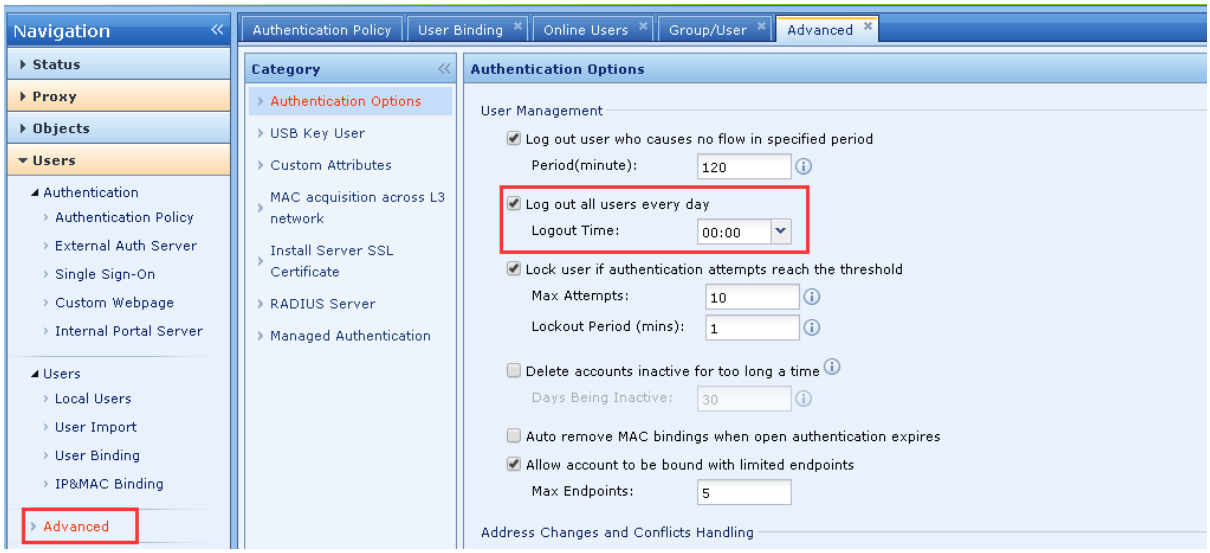
It can be seen that when the user authenticates for the first time, the device will automatically bind the user's MAC, and open authentication is also enabled.

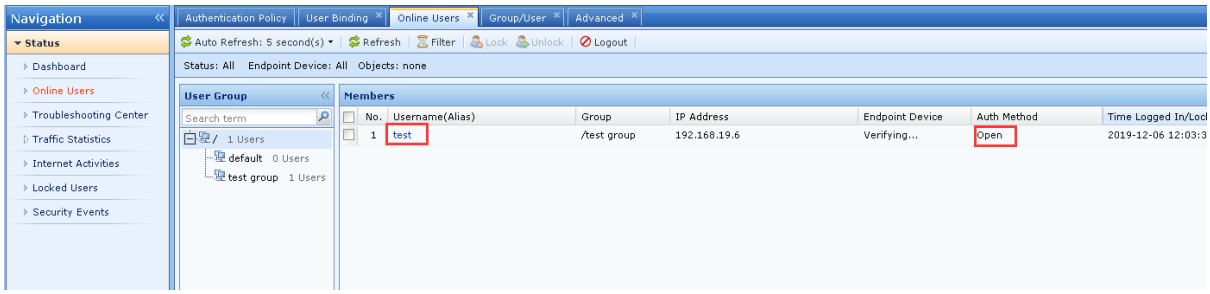
3 Test Result

After the user goes online for the first time with password based authentication, they can access the Internet directly after being logged out if they did not clear the browser cache.

Log out the users who have passed the authentication using “Log out all users every day” function and go online again.

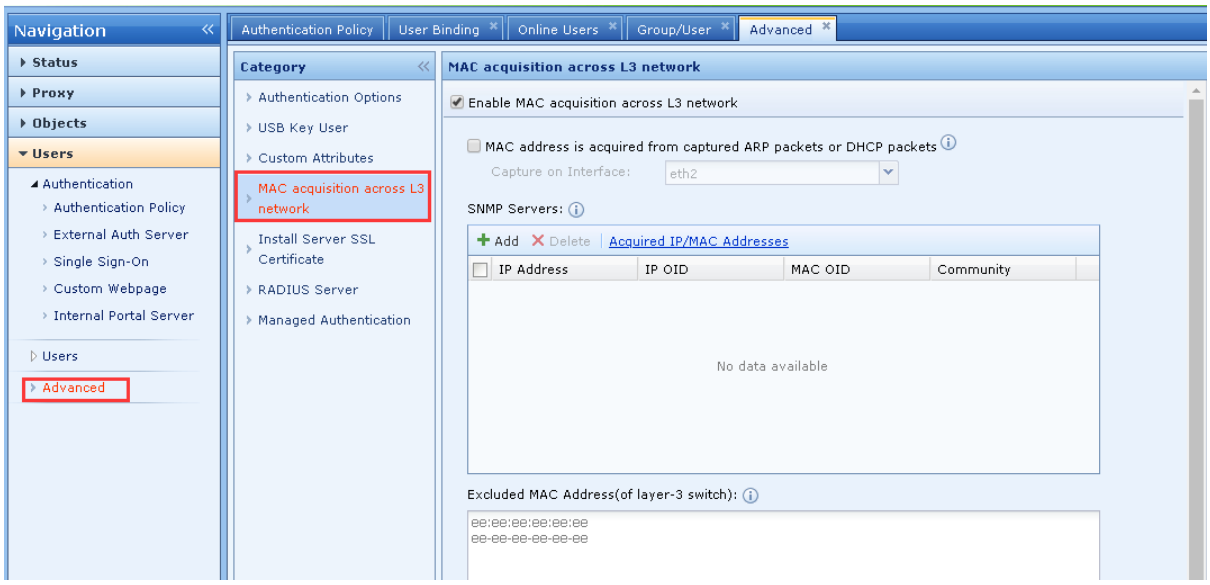
To configure “Log out all users every day” or “Log out user who causes no flow in specified period”, in [Users]-[Advanced]-[Authentication Options]-[User Management], configure [Log out all users every day] or [Log out user who causes no flow in specified period], and wait for the user to be logged out before going online again.


Navigation
Status
Proxy
Objects
Users
Authentication
Authentication Policy
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
USB Key User
Custom Attributes
MAC acquisition across L3 network
Install Server SSL Certificate
RADIUS Server
Managed Authentication
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


Navigation
Status
Dashboard
Online Users
Troubleshooting Center
Traffic Statistics
Internet Activities
Locked Users
Security Events
Authentication Policy
User Binding
Online Users
Group/User
Advanced
Auto Refresh: 5 second(s)
Refresh
Filter
Lock
Unlock
Logout
Status: All
Endpoint Device: All
Objects: none
User Group
Search term
/ 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...
Open

4 Precautions

1. MAC open authentication is related to the internal network environment. If the IAM is in a three-layer environment, you need to configure the MAC acquisition across L3 network first. The location is [Users]-[Advanced]-[MAC acquisition across L3 network], when the IAM can recognize the MAC address of the end user of the internal network, then only you can enable the MAC address binding in the authentication policy.



2. The MAC open authentication has nothing to do with the user's logout method. During the open authentication, any of the logout methods can support the next open authentication.
3. During the open authentication period, when the IP address of the PC changes, the next time you access the Internet, you can still access the Internet directly.

SANGFOR