

IAM

How to Automatically Bind User MAC Address Guide

Version 12.0.12

Change Log

Date	Change Description

CONTENT

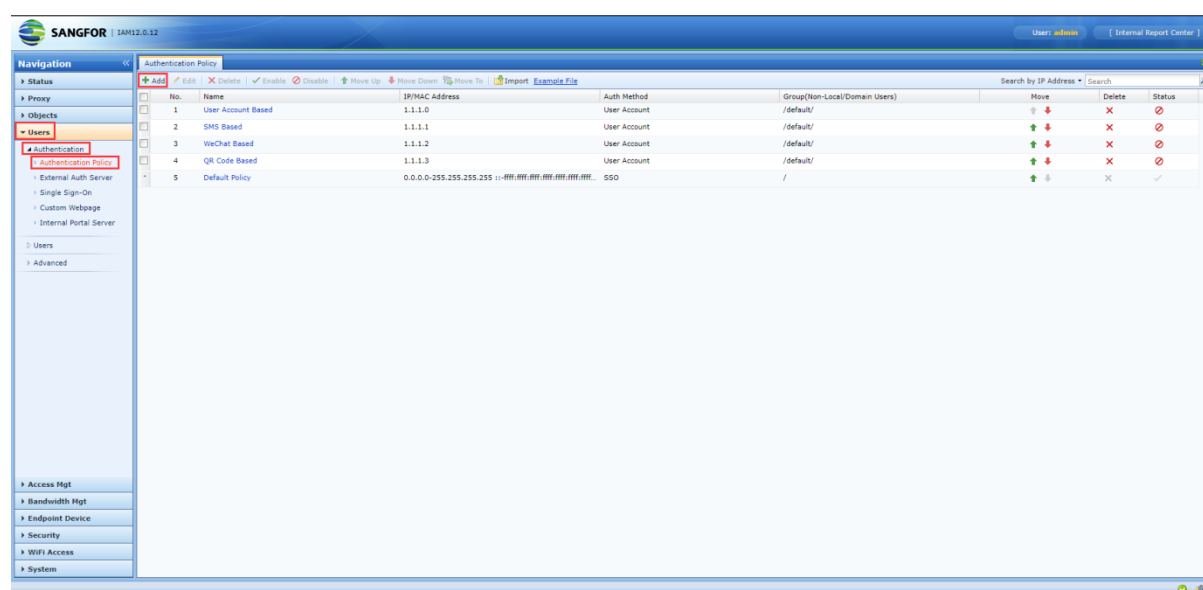
Chapter 1 Automatically Bind User MAC Address.....	1
1 Configuration	1
1.1 Add New Authentication Policy	1
1.3 Configure Action	3
1.4 layer intranet environment.....	4
1.4.1 Configure MAC acquisition across L3 network on IAM.....	5
1.4.2 Configure Authentication Policy	7
1.5 Testing Result.....	9
2 Precautious	11

Chapter 1 Automatically Bind User MAC Address

1 Configuration

1.1 Add New Authentication Policy

Go to [Users] – [Authentication] – [Authentication Policy] and add a new Authentication Policy.



1.2 Configure Objects and Auth Method

1. Name: Customize according to your preference.

Description: Customize according to your preference. (optional)

Objects: Enter the IP Segment of the intranet user or IP range (example:192.168.1.0/255.255.255.0)

Authentication Policy

☒ Enable

Name: Auto MAC Address Binding

Description: Optional

Objects

IP/MAC Address: 192.168.1.0/255.255.255.0

Auth Method

Action

Back Next

2. Auth Method: Select the authentication method according to actual needs.
(example: password based authentication)

Authentication Policy

☒ Enable

Name: Auto MAC Address Binding

Description:

Auth Method:

☐ Open authentication

☒ Password based

☐ Single Sign-On(SSO)

☐ Disabled (requests are rejected always)

Auth Server: Local user database

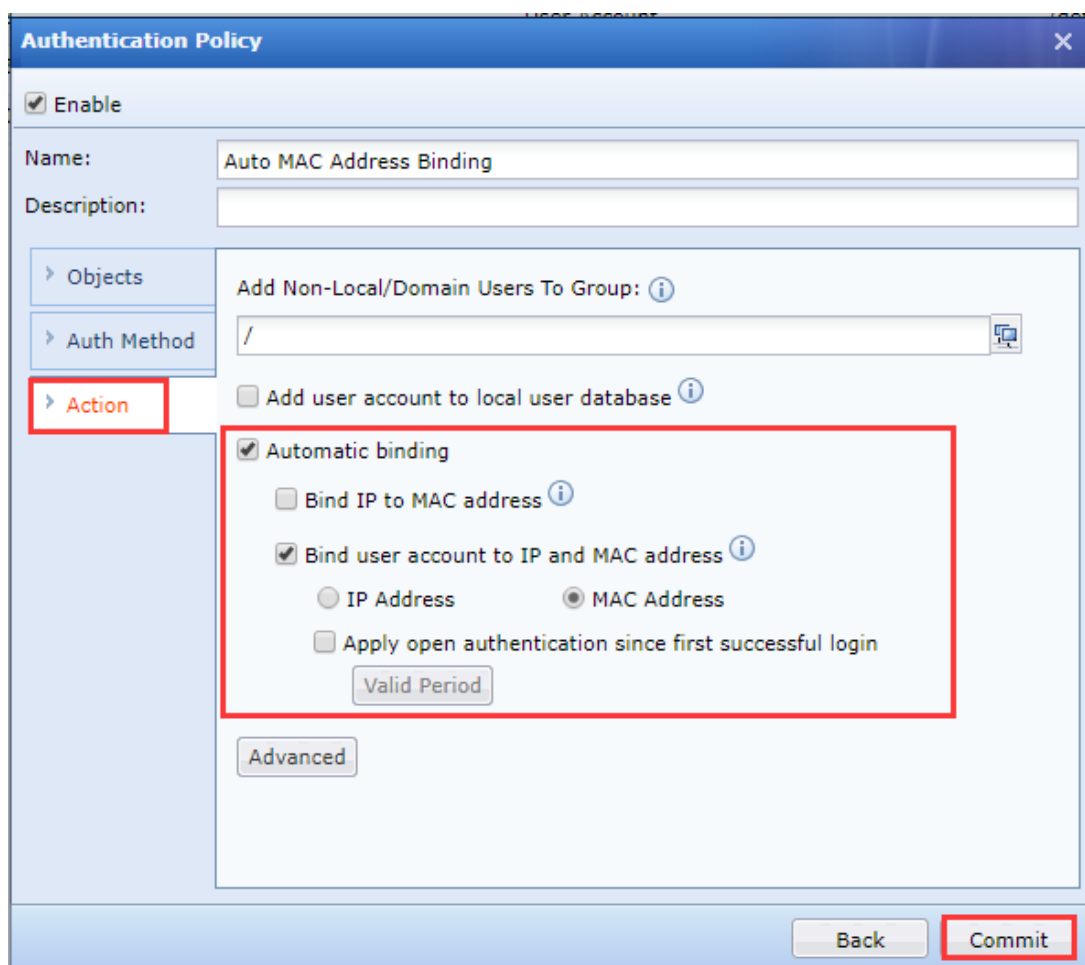
Captive Portal: Page: Without Slideshow Preview

Login Redirection: Previously visited webpage

Back Next

1.3 Configure Action

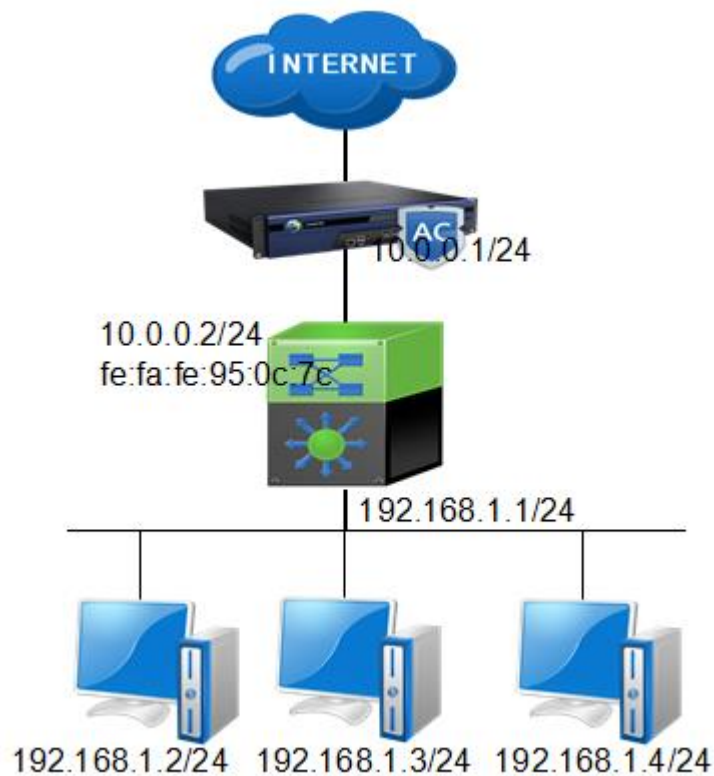
1. Check [Automatic binding] and [Bind user account to IP and MAC address].
Select [MAC Address] and click [Commit].



[Precautions] The binding will not work if only checked [Automatic binding] option without checking [Bind user account to IP and MAC address] option.

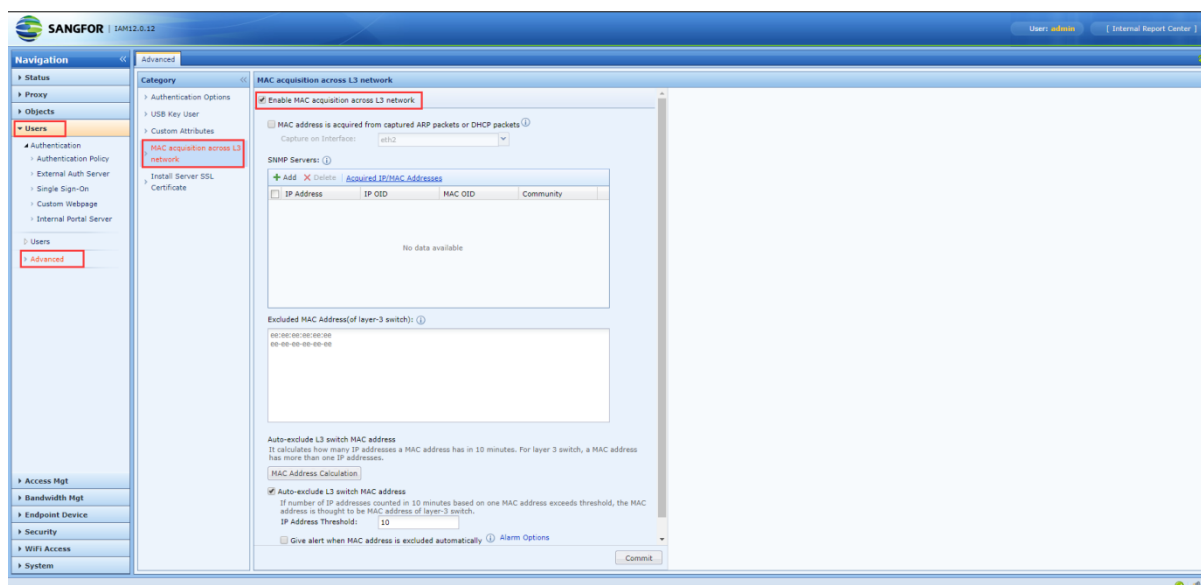
1.4 layer intranet environment

The IAM is deployed on the network, but the user's data is passed through the gateway (Layer 3 switch). In the case the data passing through the device, you need to enable the " MAC acquisition across L3 network " on the device, and the snmp service needs to be enabled on the Layer 3 switch.



1.4.1 Configure MAC acquisition across L3 network on IAM

1. Go to [Users] > [Advanced] > [MAC acquisition across L3 network] to enable the function. Configuration is show in below.



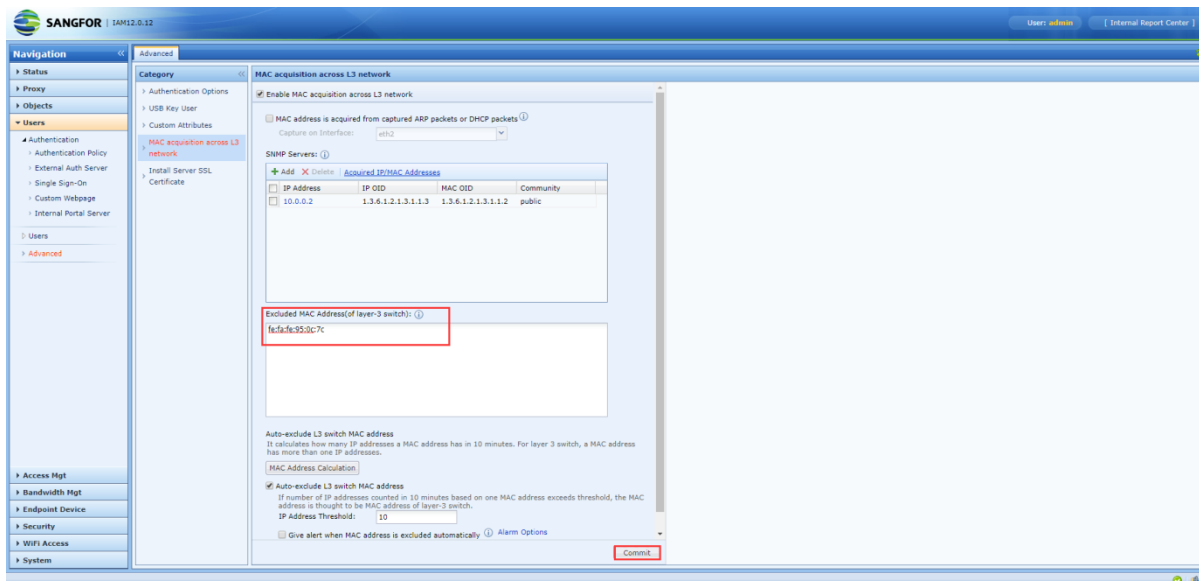
2. Add new SNMP server

IP Address : IP of layer 3 switch (must be able to communicate with IAM)

IP OID/MAC OID: Get the OID of IP and MAC from layer 3 switch

Community: The configured community value when snmp is enabled.

3. Add the MAC address of the layer 3 switch to [Excluded MAC Address(of layer 3 switch)] and click Commit.



1.4.2 Configure Authentication Policy

1. After the configuration for [MAC acquisition across L3 network], follow the steps above to configure authentication policy. (When testing for MAC address binding, recommend to use MAC address as username. Do not bind user address info to avoid binding wrong info and cause unable to surf internet.).

Authentication Policy

☒ Enable

Name:

Description:

> Objects

> **Auth Method**

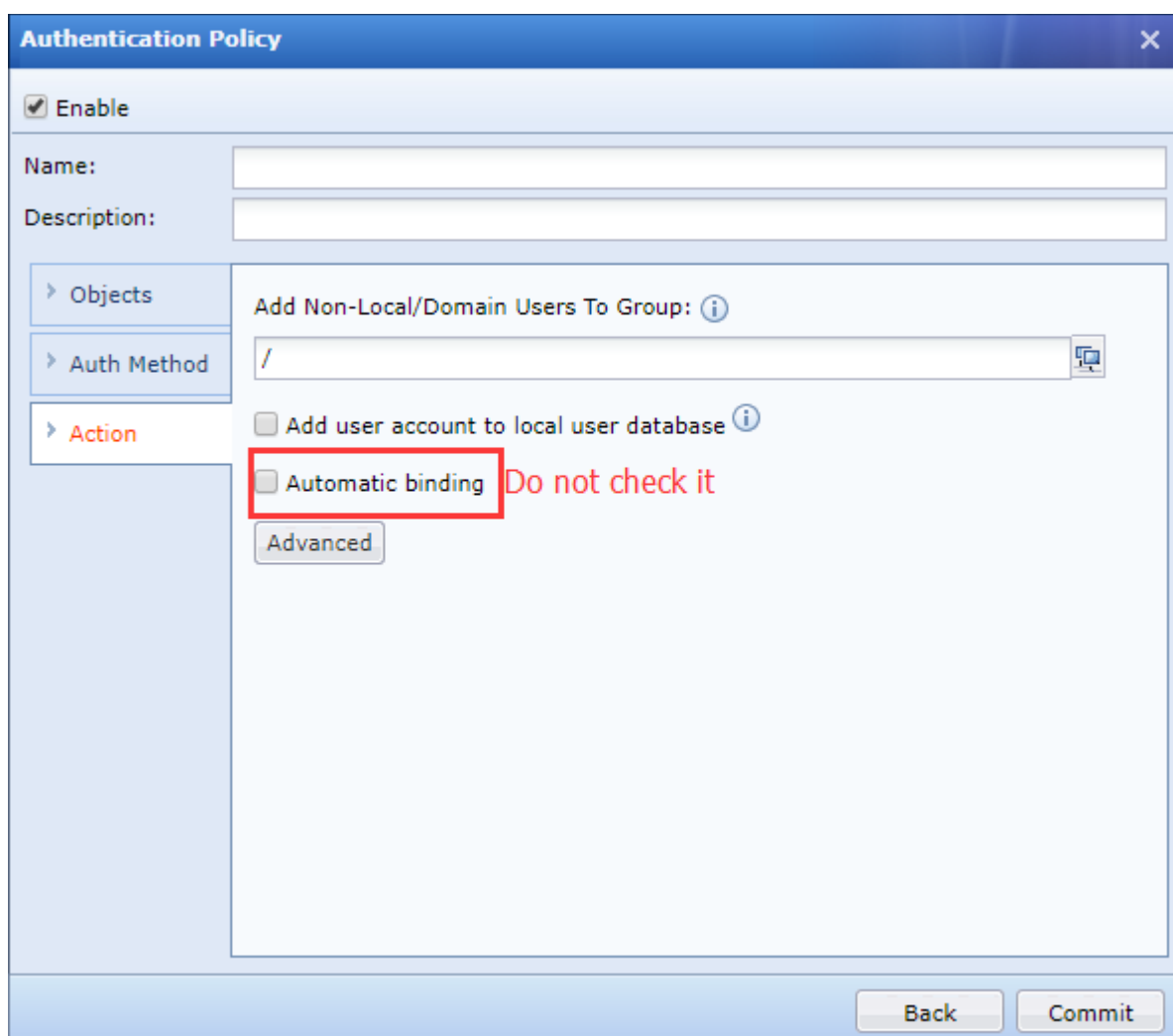
> Action

Auth Method: ☒ Open authentication
☐ Password based
☐ Single Sign-On(SSO)
☐ Disabled (requests are rejected always)

Username:

Back Next

2. Configure Action.

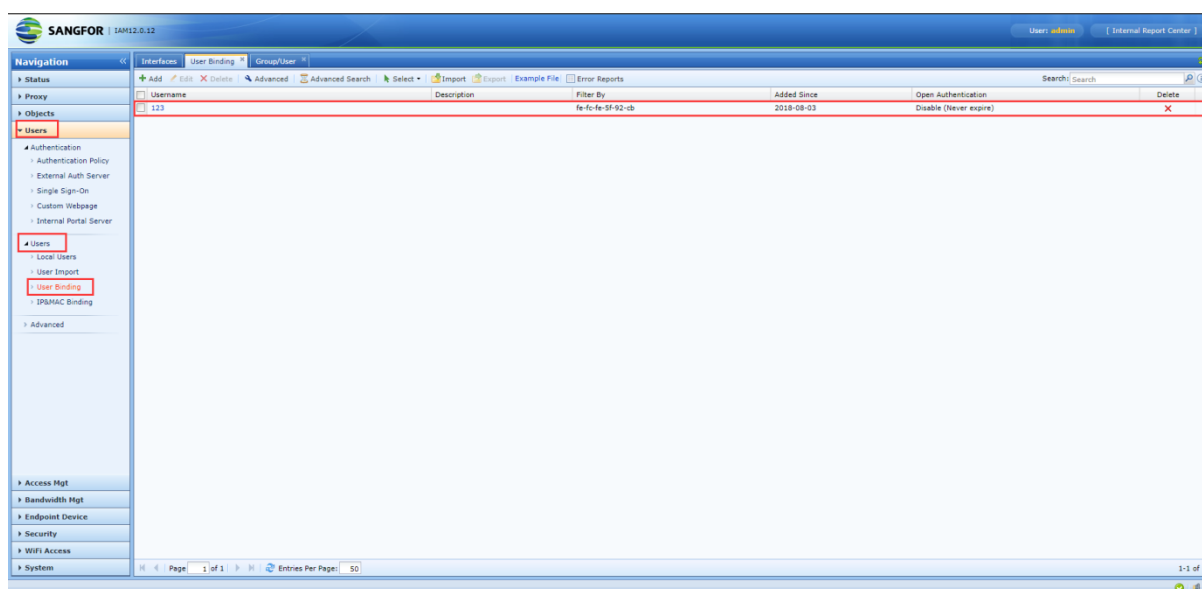
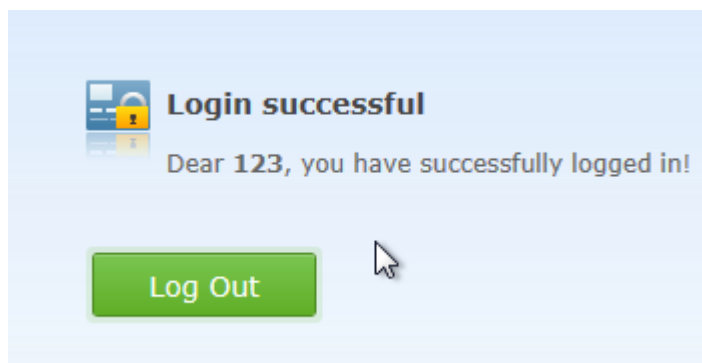


The screenshot shows the 'Authentication Policy' configuration window. The 'Enable' checkbox is checked. The 'Name' and 'Description' fields are empty. The 'Action' tab is selected in the left sidebar. In the main area, the 'Add Non-Local/Domain Users To Group' field contains a slash (/). Below it, the 'Add user account to local user database' checkbox is unchecked. The 'Automatic binding' checkbox is also unchecked and is highlighted with a red rectangular box. To the right of this box, the text 'Do not check it' is written in red. An 'Advanced' button is located below the 'Automatic binding' checkbox. At the bottom right, there are 'Back' and 'Commit' buttons.

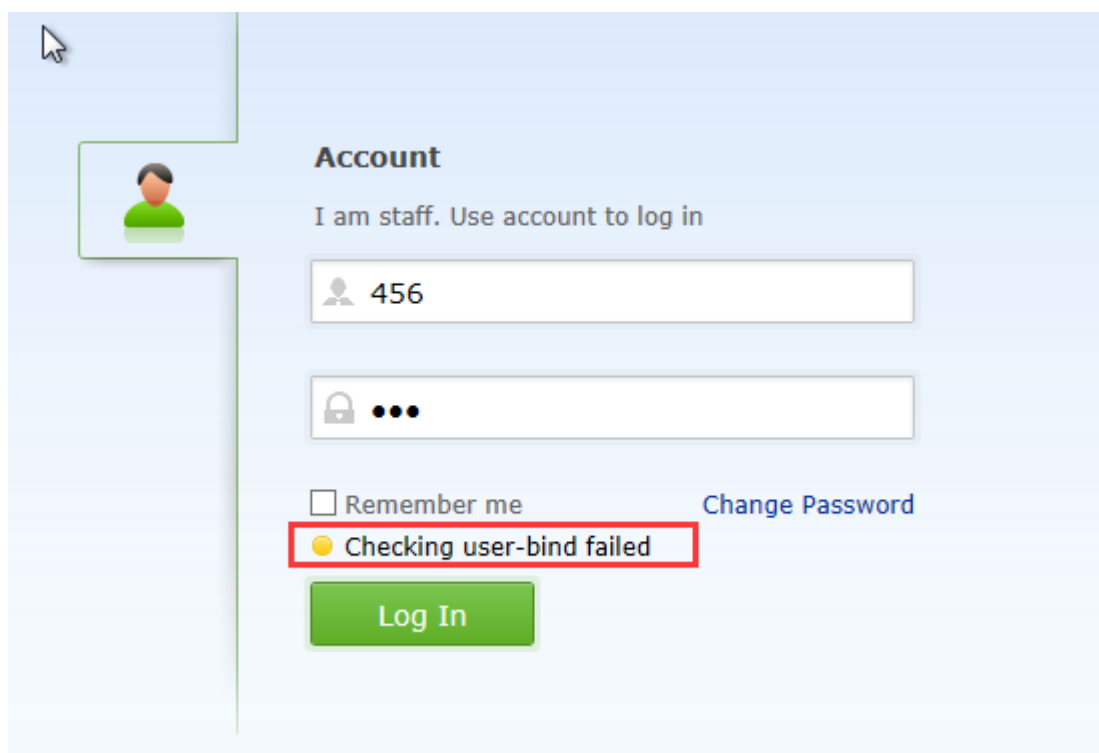
3. After configured the policy, you may see the username in [Status] > [Online User]. You can select a few users to compare the mac address inside the device and the intranet user pc when the usernames showing different mac addresses.
 - a. If the MAC address is the same, there is no problem for MAC acquisition across L3 network configuration. You can bind the user's mac address information.
 - b. If the MAC address is different, continue to check the configuration for MAC acquisition across L3 network until there are no problems;

1.5 Testing Result

1. The user who surf internet passing through the device will automatically bind the mac to the device. You can view the binding relationship in [Users]--[Users]-[User Binding].

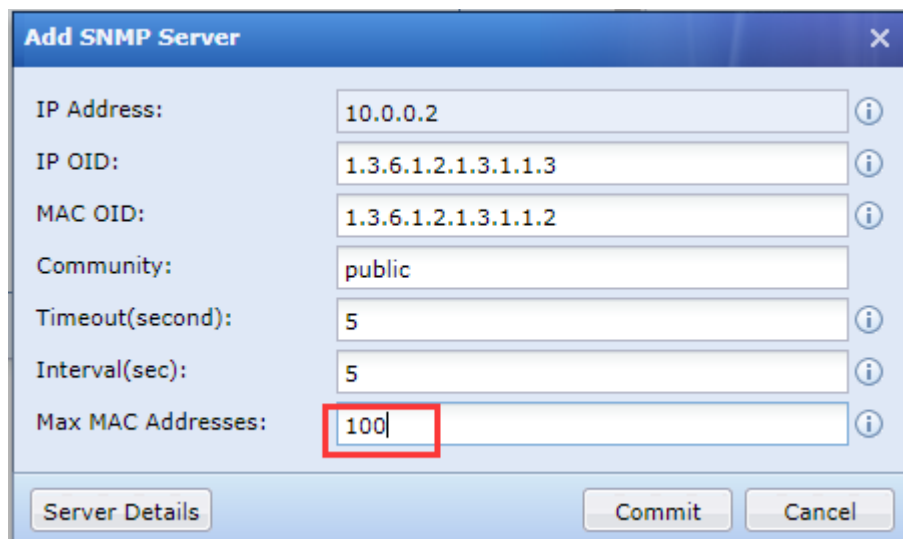


2. The user is unable to surf internet when using other account.



2 Precautions

1. In the case of a Layer 3 switch, if you correctly configure the "MAC acquisition across L3 network" but cannot obtain the correct MAC address of the user, it is recommended to change the value of "Maximum number of each acquisition" to a smaller value(50 or 100). Refer the following screen shot for configuration. This is because too much reading at a time will cause a timeout, the number is too large, the package will be fragmented.



2. Related oid values:

Cisco switches: The IP MAC OID are device defaults

IP OID: 1.3.6.1.2.1.3.1.1.3

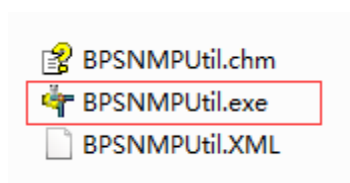
MAC OID: 1.3.6.1.2.1.3.1.1.2

Huawei/Huasan switches: Most OID values are as follows:

IP OID::1.3.6.1.2.1.4.22.1.3

MAC OID: 1.3.6.1.2.1.4.22.1.2

3. How to get the OID value of a Layer 3 switch
 - a. Contact the switch manufacturer to obtain oid value information
 - b. use the tool to scan out the oid value of the switch





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc