SANGFOR

IAM

How to Set Up to Allow Only Local Users to Authenticate Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Oct 30, 2019	Version 12.0.18 document release.

CONTENT

1 Application Scenario 1
2 Configuration and Screenshots 1
3 Testing Result 3
4 Precautions 3

1 Application Scenario

In order to improve management, only the users added by the administrator in the local users are allowed to access the Internet, and users who are not in the local users are not allowed to authenticate.

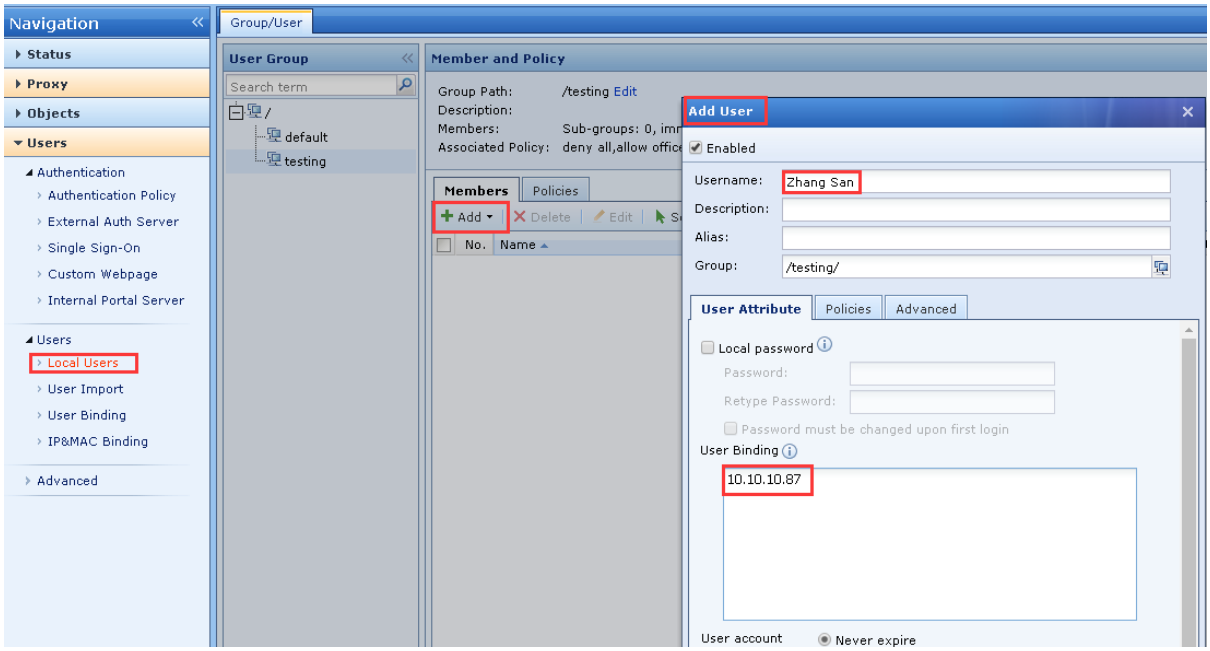
Requirements:

1. A device with IAM 12.0.18.
2. Two PC, two testing users are Zhang San and Li Si, IP address are 10.10.10.87 and 10.10.10.88, Zhang San added to the local users, Li Si did not.

2 Configuration and Screenshots

Create a user Zhang San in the local users and bind 10.10.10.87. Do not configure Li Si.

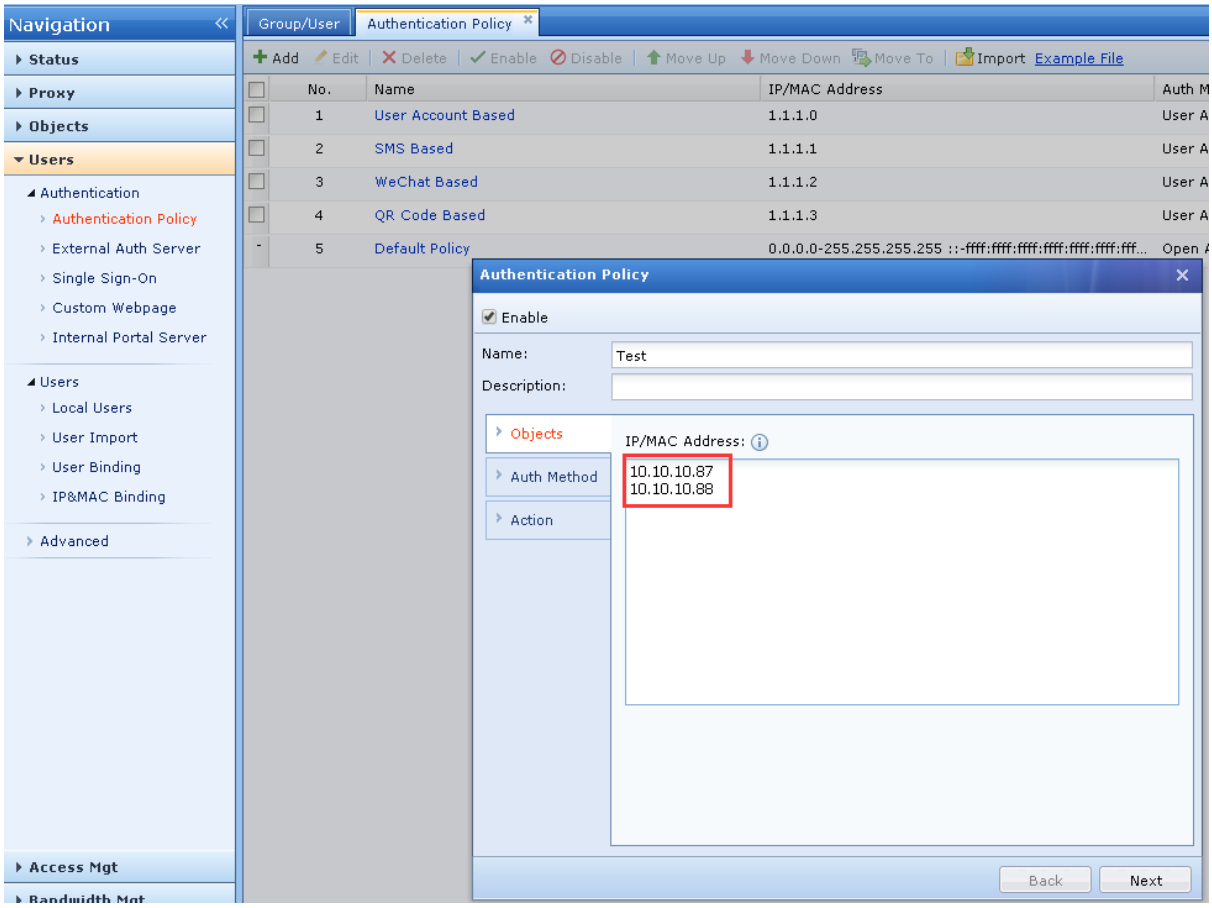
In [Users]--[Users]---[Local Users], select the test group, [Add] a user Zhang San, and bind the user's IP address in the user attribute.



Click "Commit", you can see Zhang San and the attribute is "Created by administrator".

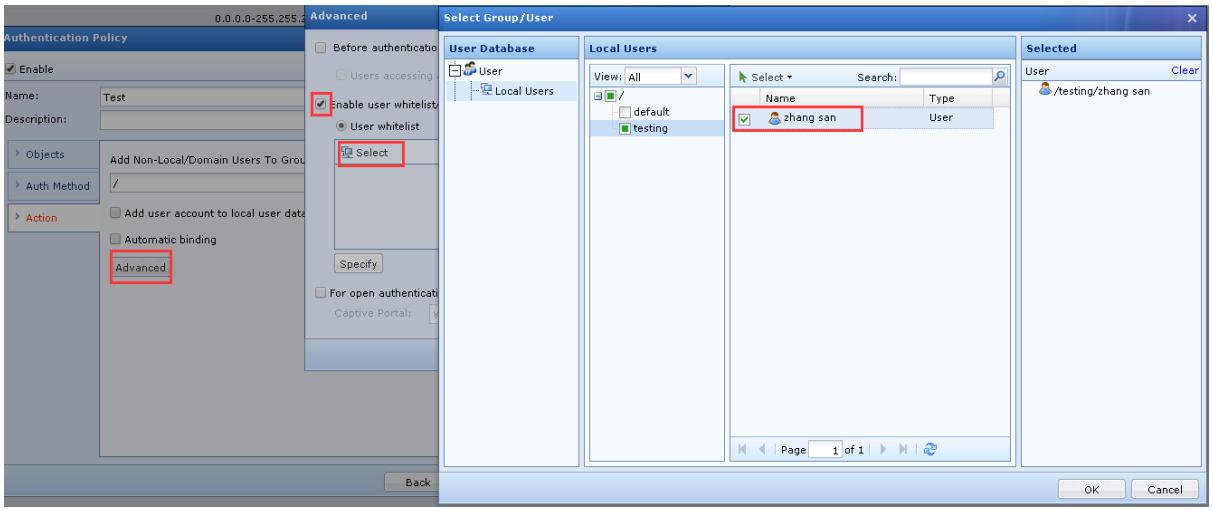
Configure user whitelist/blacklist

Add [Authentication Policy] and write intranet network segment to the [IP/MAC Address], in this case we will write testing IP addresses 10.10.10.87 and 10.10.10.88.

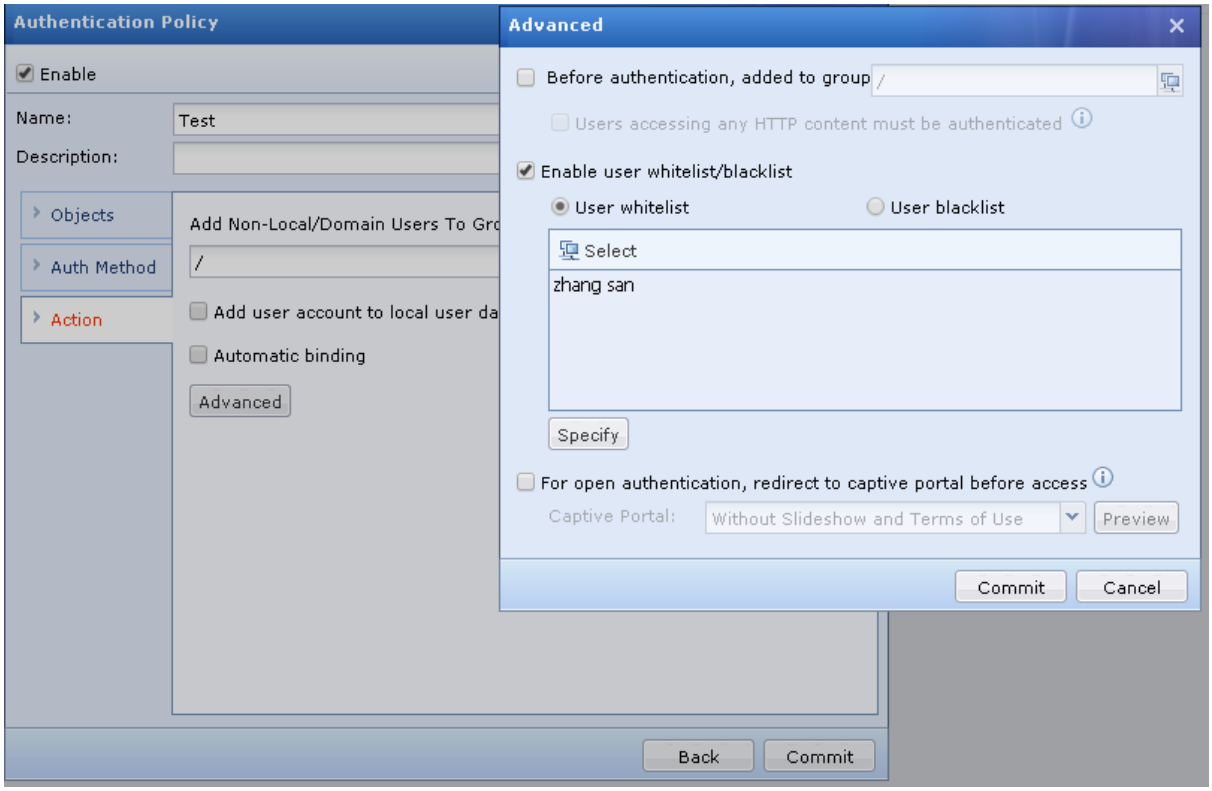


[Auth method] can be selected according to the intranet environment. Here, we will choose open authentication.

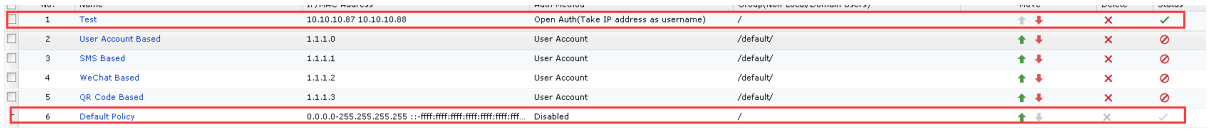
[Action] Click [Advanced]---[Enable user whitelist/blacklist], select [User whitelist], and you will be redirected to the [Group/User] interface to select users who have already existed locally which is “Zhang San", click "OK".



After confirming, you will see the user "Zhang San" in [User whitelist].



Change the default policy to disabled.



[Note]:

According to the order of matching from top to bottom, Zhang San and Li Si will match the "test" policy, but because the user whitelist/blacklist is configured, only Zhang San can be authenticated normally, Li Si cannot authenticate, and online user only can see the address of 10.10.10.87. Any other IP addresses other than these two will match the default policy, directly disable authentication and all the requirements are configured.

3 Testing Result

Zhang San can access Internet normally, Li Si cannot access the Internet, online user can only see Zhang San this user, as shown below:

4 Precautions

1. The matching order of the policies start matching from the top to bottom.
2. User whitelist/blacklist can select one or more groups at the same time, allowing authentication or not allowing authentication.

3. When the authentication method is [open authentication] and the IP address of the intranet user is dynamic, we cannot bind the user's IP address, instead we will bind the user's mac address. If the intranet is a layer three environment, the MAC acquisition across L3 network has to be configured.

SANGFOR

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