



IAM

CAS Authentication Configuration Guide

Version 12.0.18



Change Log

Date	Change Description
Dec 24, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Content requirements	1
1 Product Introduction	1
2 Application Scenario	1
3 Requirement Condition	1
4 Configuration Idea	1
5 Configuration Guide with Screenshot	1
5.1 Testing environment and topology	1
5.2 External authentication server configuration	2
5.3 Authentication policy configuration	2
5.4 Testing result	3
6 Precaution	4

Chapter 1 Content requirements

1 Product Introduction

IAM cooperate with CAS server to implement third-party password authentication.

2 Application Scenario

Client had deploy CAS server (**Central authentication server**) in their network, CAS server protected internal user ID and password information. Currently the client has apply the IAM device in their network, so the client want to enable password authentication on IAM, but using the credential data in CAS server for third party password authentication.

3 Requirement Condition

1. IAM device with version 12.0.18 or above
2. Prepare a PC that able to communicate in the network.
3. Client had install CAS server, get a testing account from the client as well as get the CAS authentication link, for example <https://ip:8443/cas/login>.

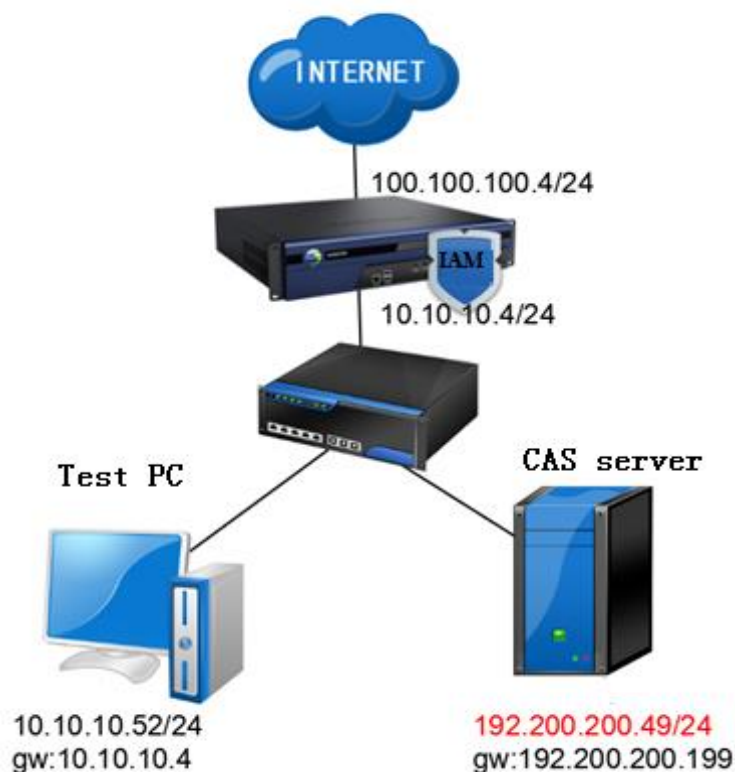
4 Configuration Idea

1. Configure an External Authentication Server on IAM device.
2. Configure an Authentication policy on IAM device.

5 Configuration Guide with Screenshot

5.1 Testing environment and topology

The deployment mode for this testing environment is Route mode.



5.2 External authentication server configuration

Configure an External Authentication Server follow with the diagram below. Fill in the [URL] with CAS server authentication link, and [Keyword] and [Version] will follow the default value.

The screenshot shows the IAM configuration interface. On the left, the **Navigation** pane has **External Auth Server** selected under **Users**. The main area shows the **Auth Server** tab with a table of authentication servers. A **+ Add** button is highlighted. A **Third-Party Auth System** dialog is open, showing the following configuration:

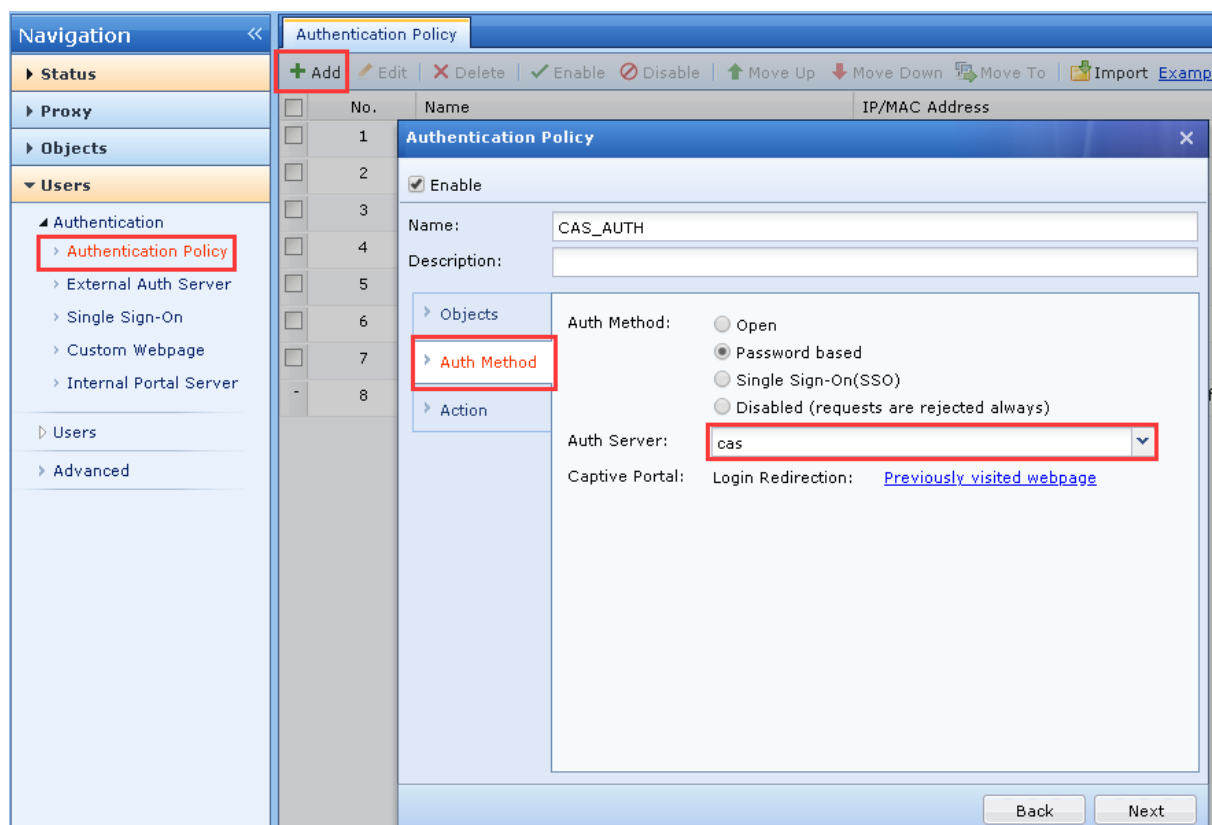
- Enable:** ☒
- Name:** cas
- URL:** https://192.200.200.49:8443/cas/login
- Keyword:** cas:serviceResponse>cas:authenticationSuccess>cas:user
- Version:** cas2.0

Below the fields, the text **follow default** is displayed. The **Commit** and **Cancel** buttons are at the bottom right of the dialog.

Note: Check version can choose cas2.0 or cas3.0. CAS server with V4.0.0 and previous version will used cas2.0 protocol, else will used cas3.0 protocol.

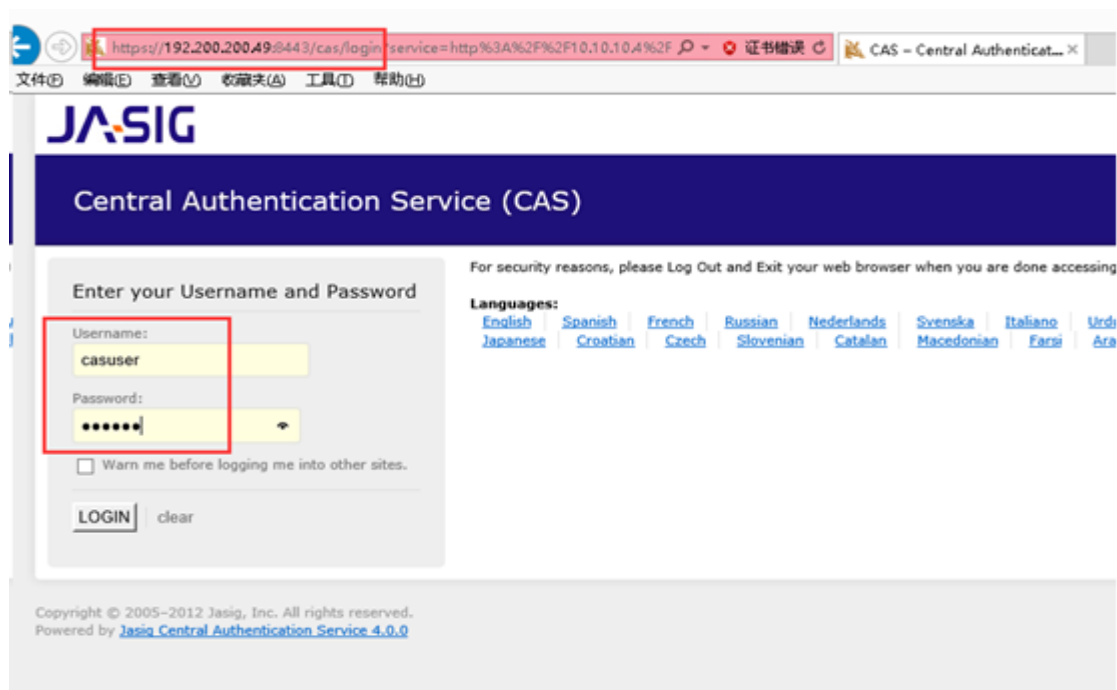
5.3 Authentication policy configuration

For the authentication policy, ensure that understand the authenticate object before configure the policy, select [Password based] as the authentication method, the [Auth Server] select the CAS server that created previously.



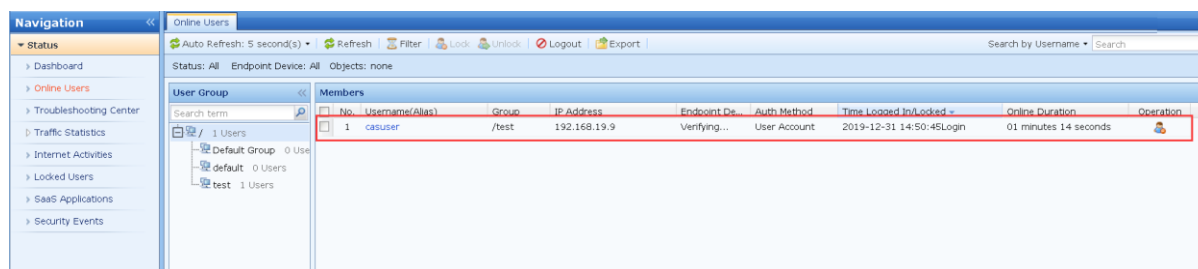
5.4 Testing result

By using an internal PC start internet browsing to redirect to CAS authentication page, insert username and password with result login successful.



Note: CAS username and password is generally defined in `deploterConfigContext.xml` file in the CAS installation directory, the user account usually defined by the customer, you may ask for a testing account from the Client.

As diagram below, we able to see the PC has login on IAM device.



6 Precaution

1. Route and bridge deployment mode support CAS authentication.
2. If the client's environment CAS server is located at external network of IAM, then the testing we need to add the CAS server address to global exclusion list, otherwise will not redirect to the CAS authentication page.



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