SANGFOR

IAG

Branch Violation Reporting Configuration Guide

Version 13.0.15

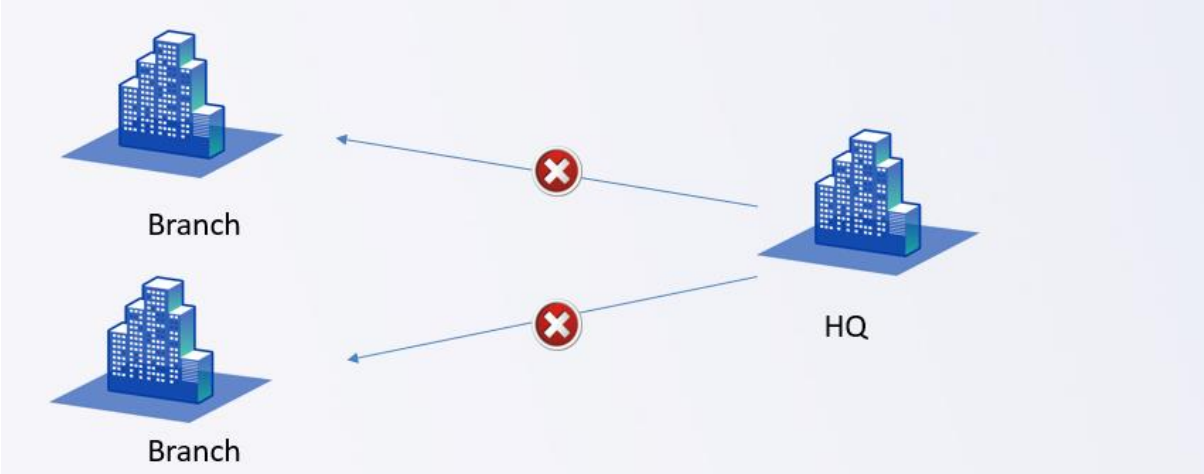
Change Log

Date	Change Description
September 14, 2020	Version 13.0.15 document release.

CONTENT

Chapter 1 Demand Background

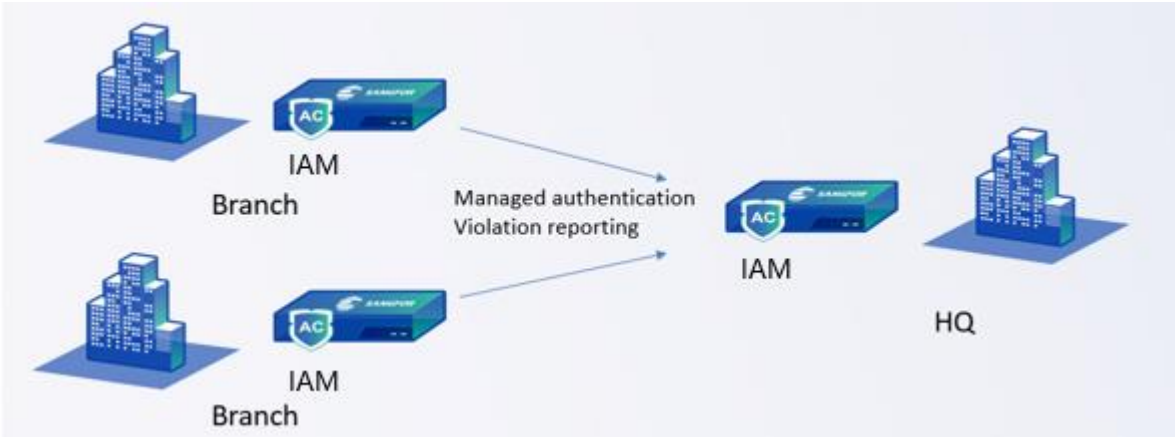
- In a multi-branch scenario, each branch cannot achieve unified authentication control.
- The headquarters cannot know the compliance status of the branch endpoints, and the branch endpoints cannot be visualized.



Chapter 2 Application Scenario

The function of violations reporting is mainly used in multi-branch scenarios. The managed authentication of each branch IAG is hosted in the headquarters IAG to achieve the managed authentication of the branches and the branch endpoints violation reporting function.

Scenario: Large companies usually have various branches, each in a different city. They deployed one IAG in each branch and one IAG in the headquarters and configure managed authentication on the branch IAG to the headquarters IAG.



Chapter 3 Configuration

3.1 Configuration Steps:

Branch:

1. Configure managed authentication and host the branch IAG to the headquarters IAG.

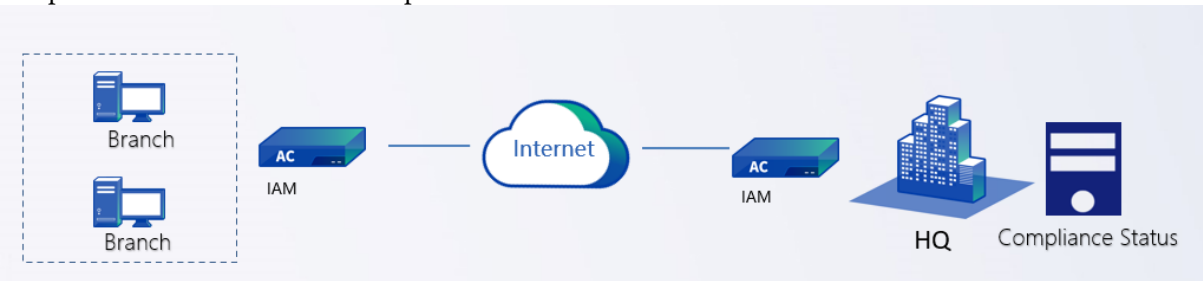
2. Configure endpoint check policies to obtain the compliance status of branch endpoints.

Headquarters:

1. Enable the authentication center function to obtain the compliance report information of the branch endpoints.

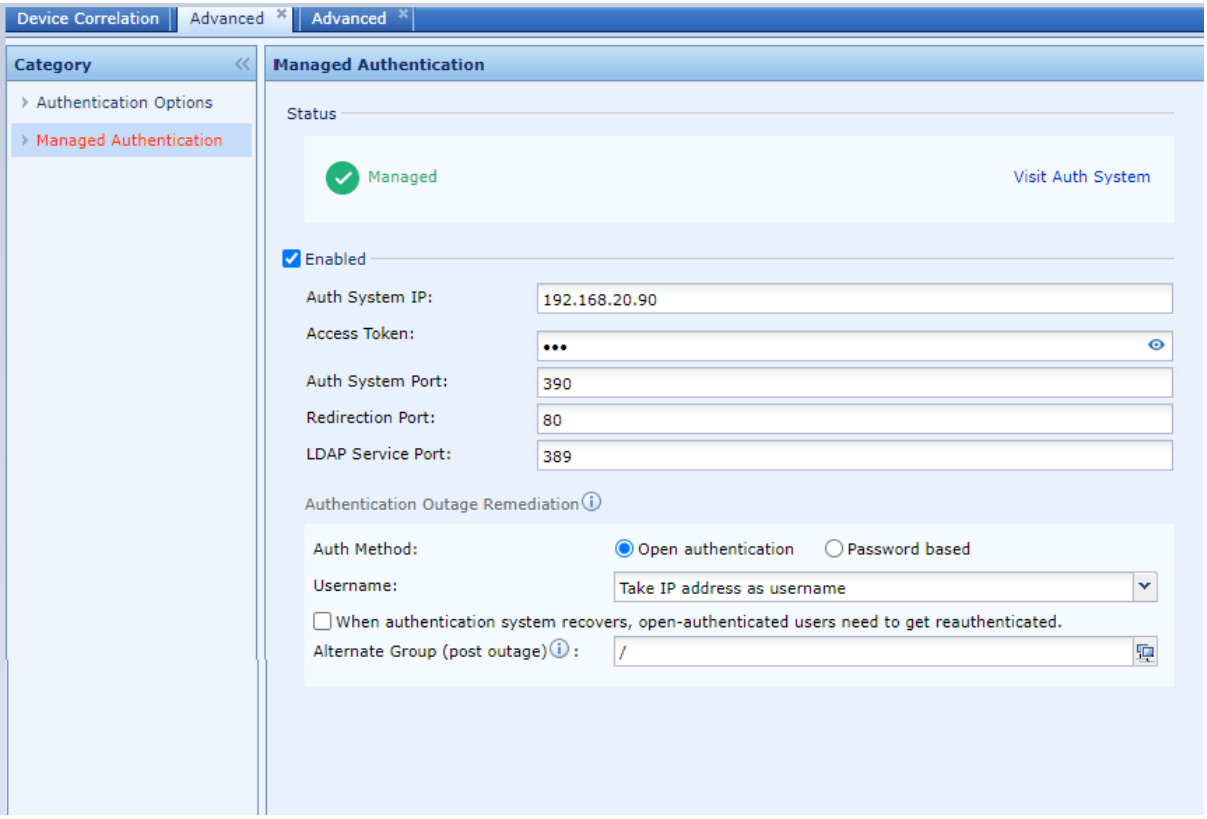
3.2 Configuration Case:

The customer's headquarters deployed an IAG, and each branch also deployed an IAG. At the same time, some endpoint checking policies are enabled. Currently, the headquarters hopes to obtain the compliance status of all branch endpoints.

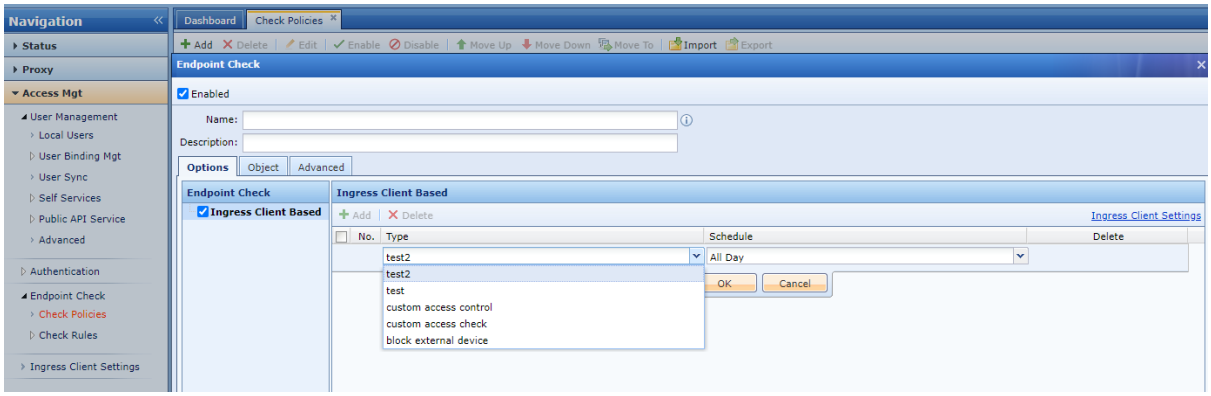


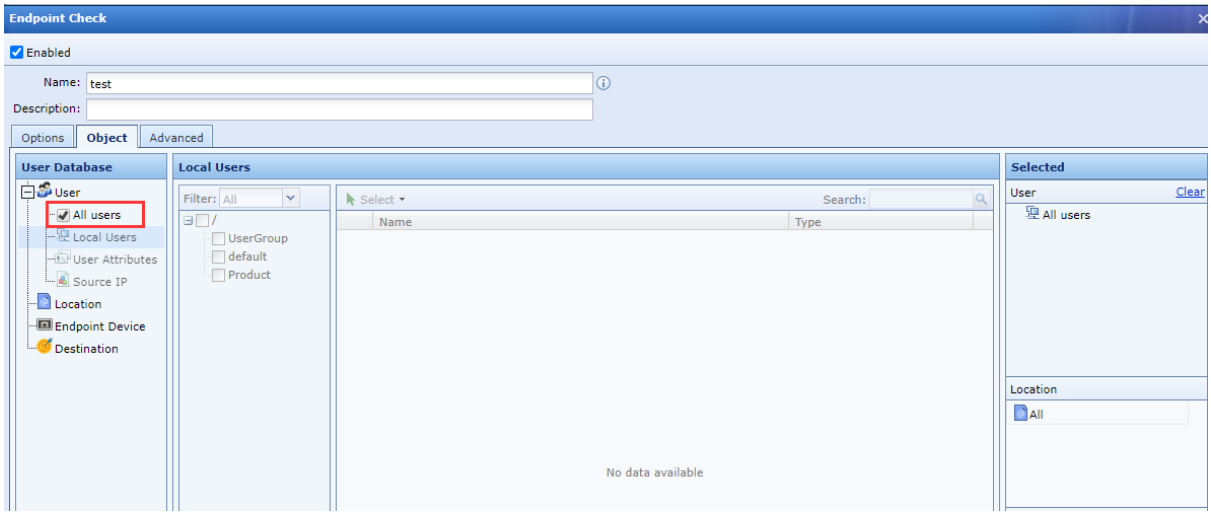
3.2.1 Branch Configuration

Configure managed authentication and host the branch IAG to the headquarters IAG authentication center.



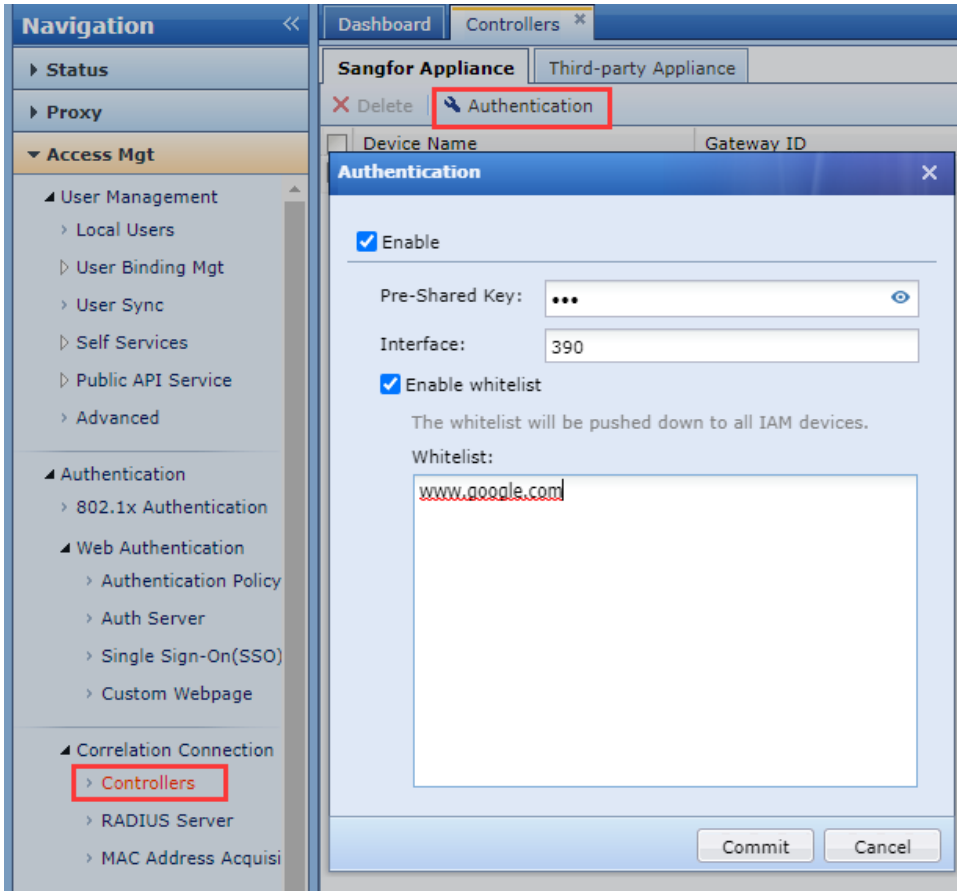
Configure endpoint checking policies to obtain the compliance status of branch endpoints.





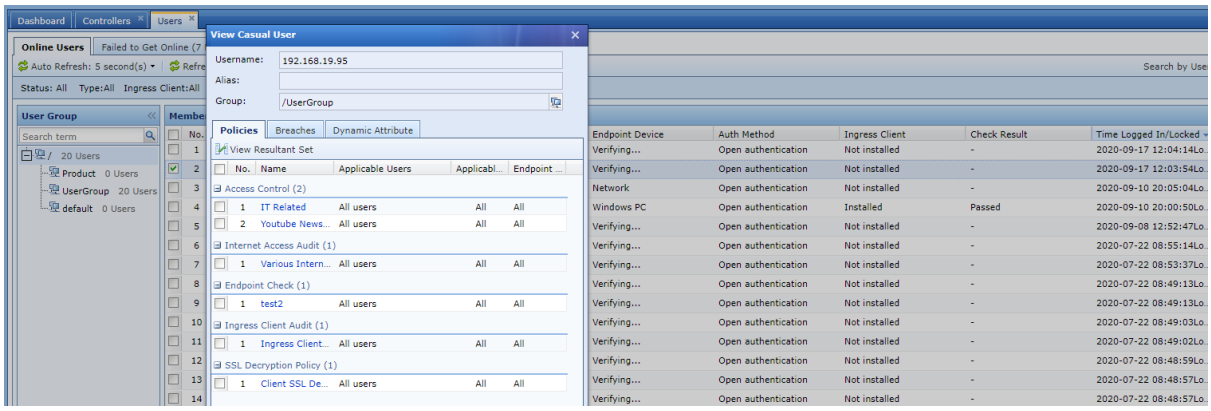
3.2.2 Headquarters Configuration

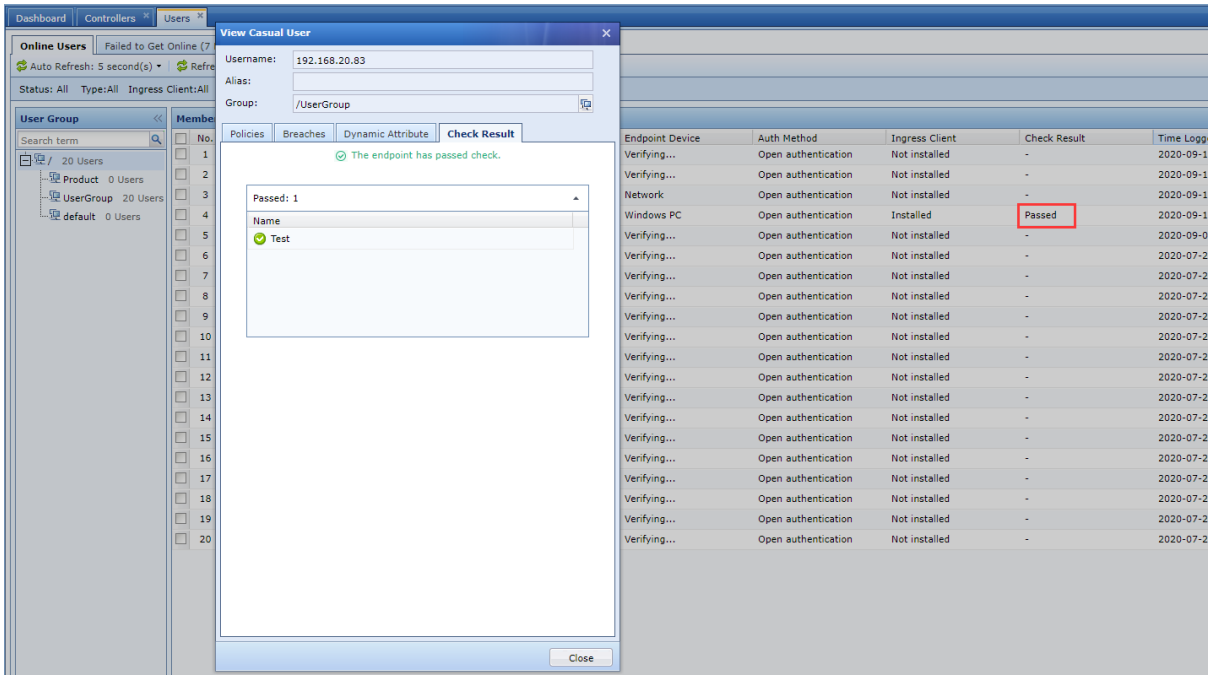
Enable the authentication center function to obtain the compliance status of the branch endpoints.



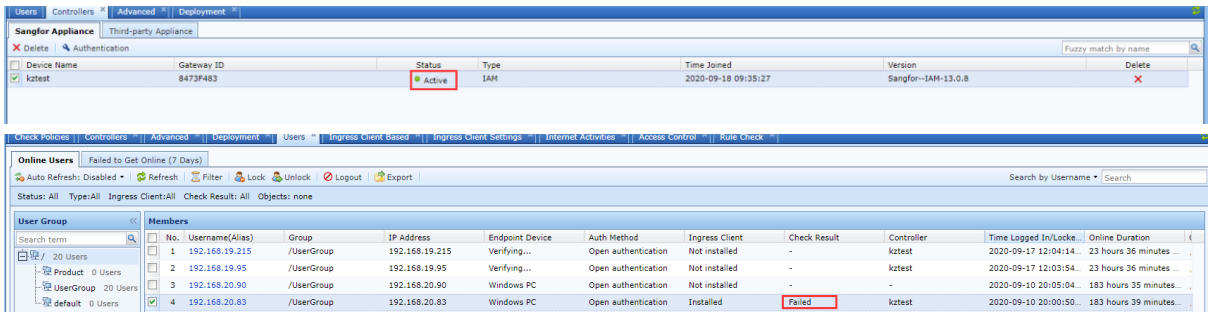
3.2.3 Testing Result

Online status and endpoint check results of branch users:

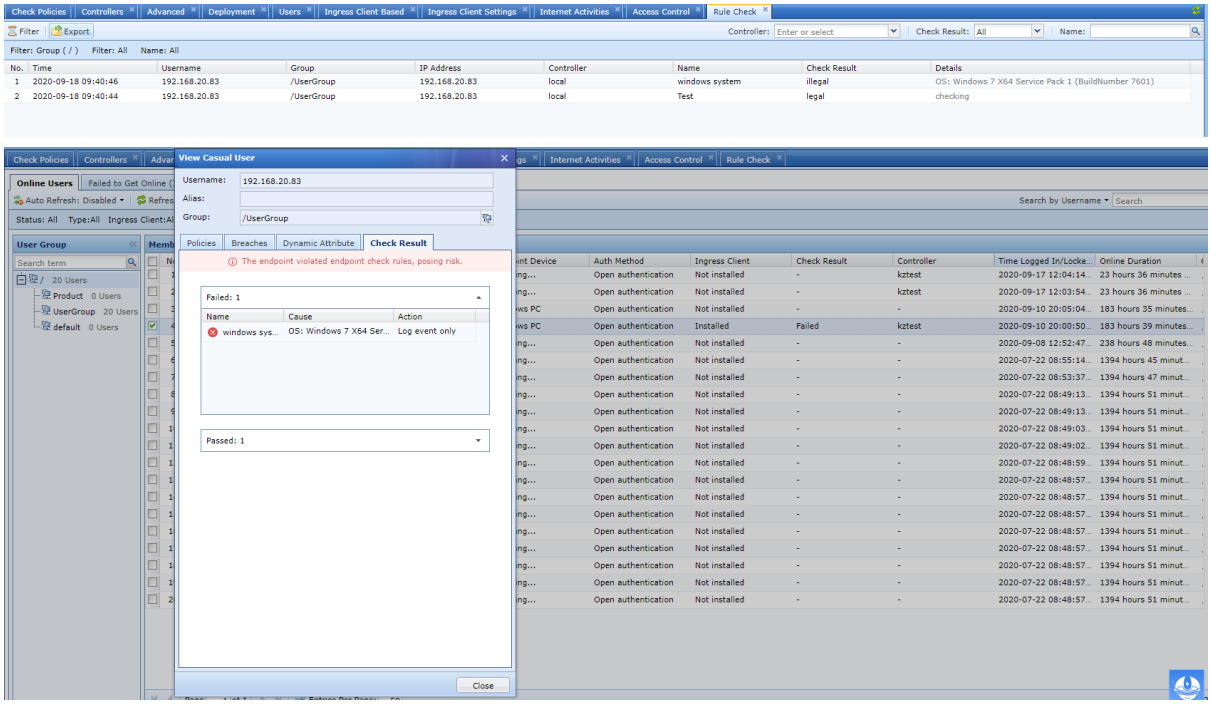




Headquarters managed authentication success, you can see the online status of branch users.



Headquarters managed authentication success, you can see the compliance status of branch users.



Chapter 4 Precautions

1. After the managed authentication is turned on, high availability active-active mode is not supported.

2. IAG as an authentication center cannot add into CM/BBC.