



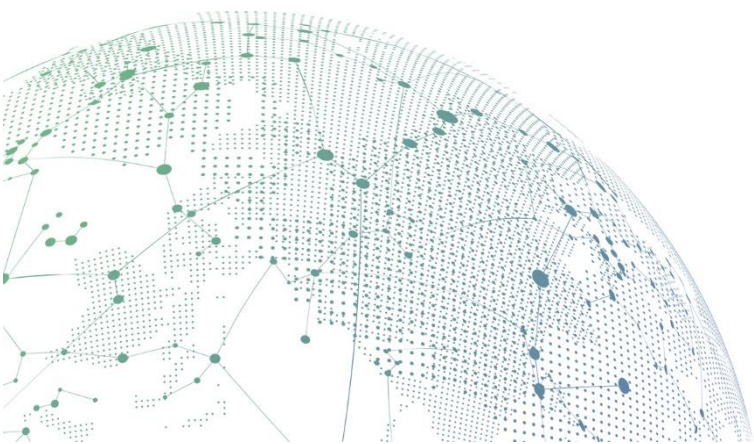
SANGFOR



IAG

Panduan Konfigurasi Pelaporan Pelanggaran Branch

Versi 13.0.15



Catatan Perubahan

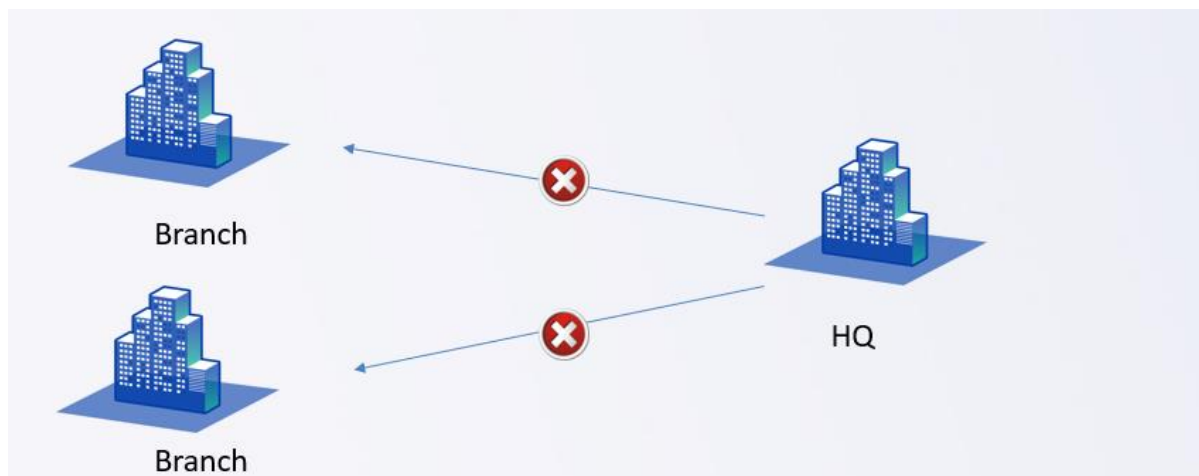
Tanggal	Deskripsi Perubahan
September 14, 2020	Rilis Dokumen Versi 13.0.15 .

Daftar Isi

Bab 1 Latar Belakang Permintaan	1
Bab 2 Skenario Aplikasi	1
Bab 3 Konfigurasi	1
3.1 Langkah Konfigurasi:	2
3.2 Kasus Konfigurasi:	2
3.2.1 Konfigurasi Branch	2
3.2.2 Konfigurasi Headquarter	4
3.2.3 Hasil Pengujian	4
Bab 4 Tindakan Pencegahan	6

Bab 1 Latar Belakang Permintaan

- Dalam skenario multi-branch, setiap branch tidak dapat mencapai kesatuan kontrol autentikasi.
- Headquarters tidak dapat mengetahui status dari branch endpoint, dan branch endpoint tidak dapat divisualisasikan.



Bab 2 Skenario Aplikasi

Fungsi dari pelaporan pelanggaran terutama digunakan dalam skenario multi-branch. Managed authentication dari setiap branch IAG di host di headquarter IAG untuk mencapai managed authentication dari branch dan pelaporan pelanggaran fungsi.

Skenario: Perusahaan besar biasanya memiliki berbagai branch, masing-masing di kota yang berbeda. Mereka deploy satu IAG di setiap branch dan satu IAG di headquarter dan konfigurasi managed authentication di branch IAG ke headquarter IAG.



Bab 3 Konfigurasi

3.1 Langkah Konfigurasi:

Branch:

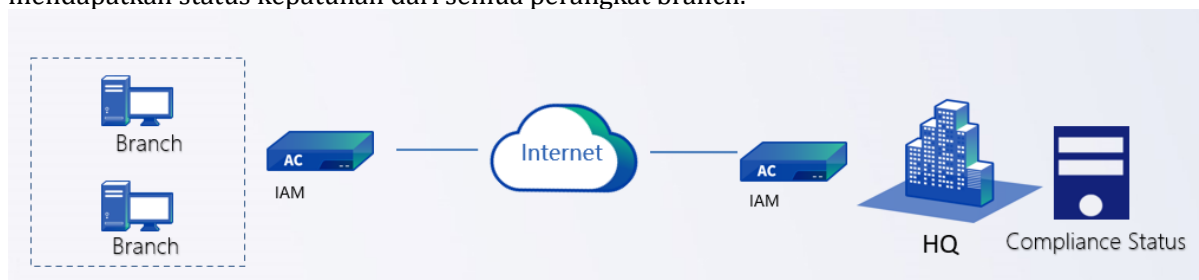
1. Konfigurasi managed authentication dan host branch IAG ke headquarter IAG.
2. Konfigurasi endpoint check policy untuk mendapatkan status kepatuhan perangkat branch.

Headquarters:

1. Aktifkan fungsi autentikasi center untuk memperoleh informasi laporan kepatuhan dari branch endpoint .

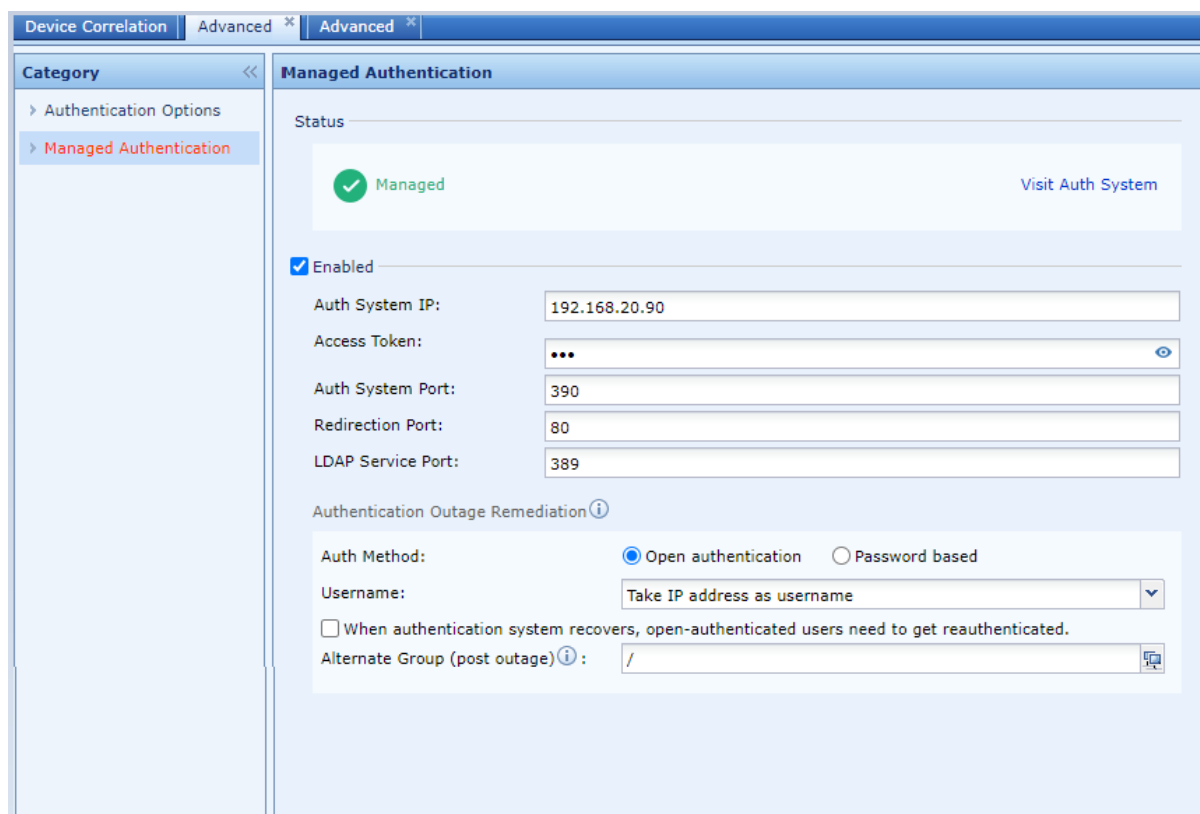
3.2 Kasus Konfigurasi:

Headquarter pelanggan deploy IAG, dan setiap branch juga deploy IAG. Pada saat yang sama, beberapa endpoint pemeriksaan policy diaktifkan. Saat ini, headquarters berharap untuk mendapatkan status kepatuhan dari semua perangkat branch.

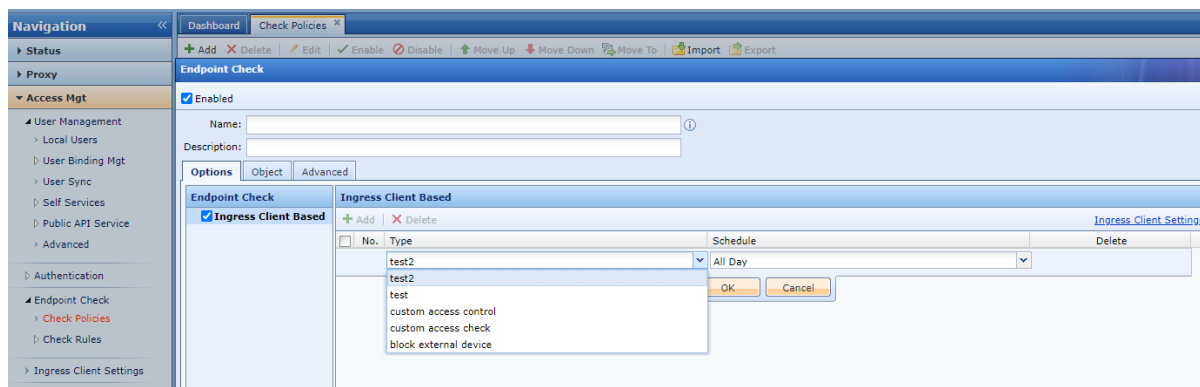


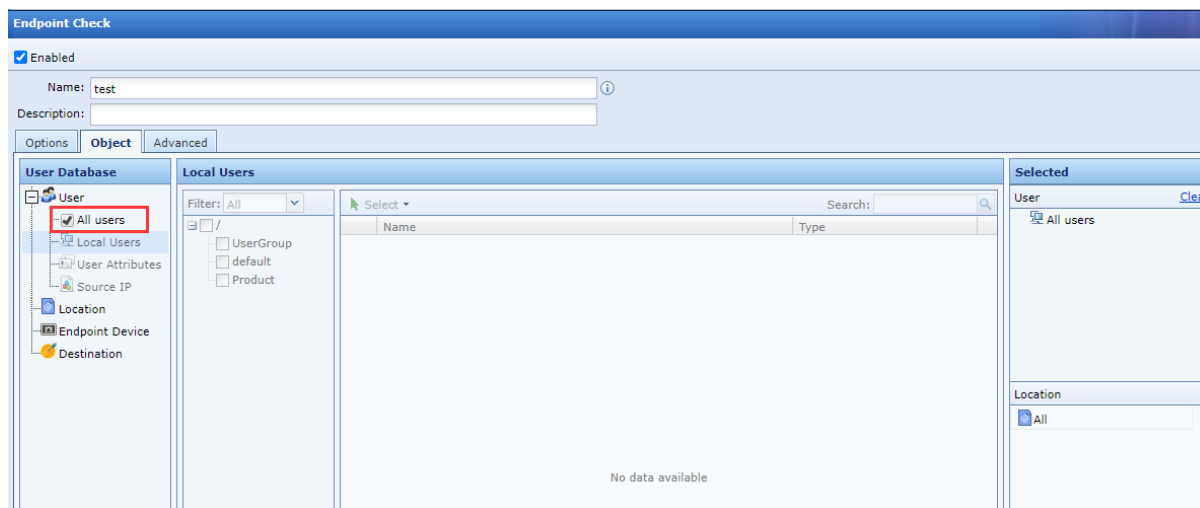
3.2.1 Konfigurasi Branch

Konfigurasi managed authentication dan host branch IAG ke headquarter IAG autentikasi center



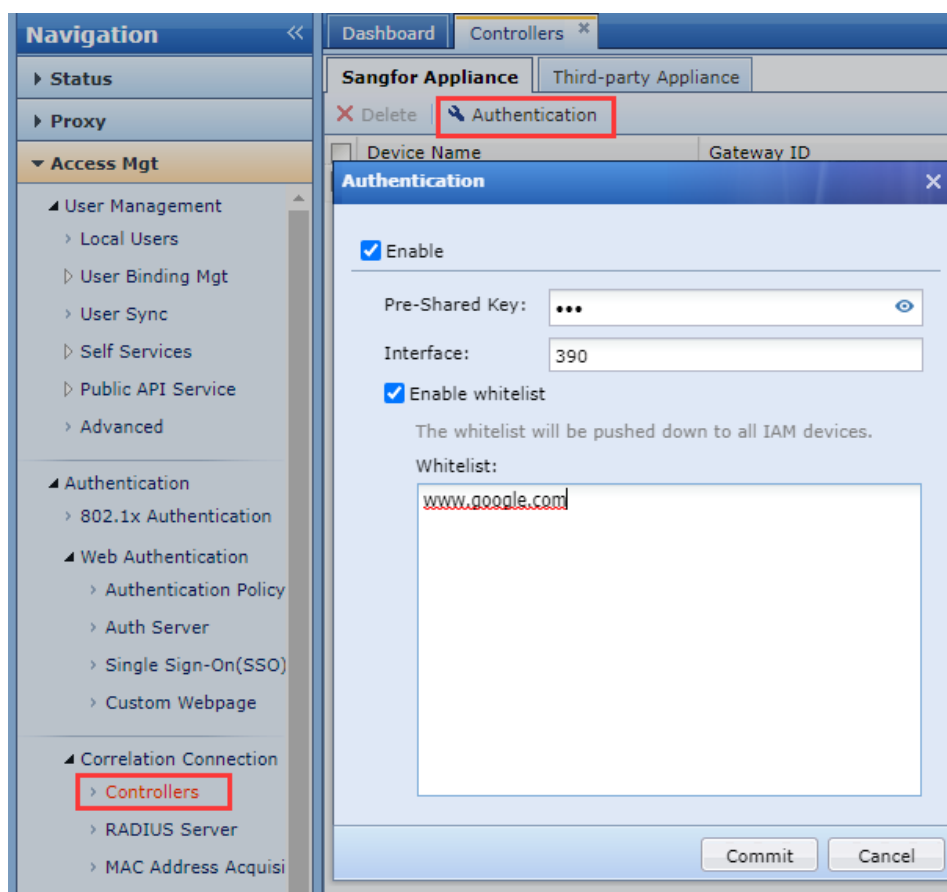
Konfigurasi endpoint pemeriksaan policy untuk mendapatkan compliance status dari branch endpoint.





3.2.2 Konfigurasi Headquarter

Enable fungsi authentication center untuk mendapatkan compliance status dari branch endpoint.



3.2.3 Hasil Pengujian

Online status dan hasil pemeriksaan endpoint pengguna branch:

Panduan Konfigurasi IAG Versi 13.0.15

The first screenshot shows the 'View Casual User' window for user 192.168.19.95. The 'Policies' tab is active, showing a list of policies applied to the user. The 'Check Result' tab shows a green checkmark indicating the endpoint has passed the check.

The second screenshot shows the 'View Casual User' window for user 192.168.20.83. The 'Check Result' tab is active, showing a green checkmark indicating the endpoint has passed the check. A red box highlights the 'Passed' status in the 'Check Result' column of the table.

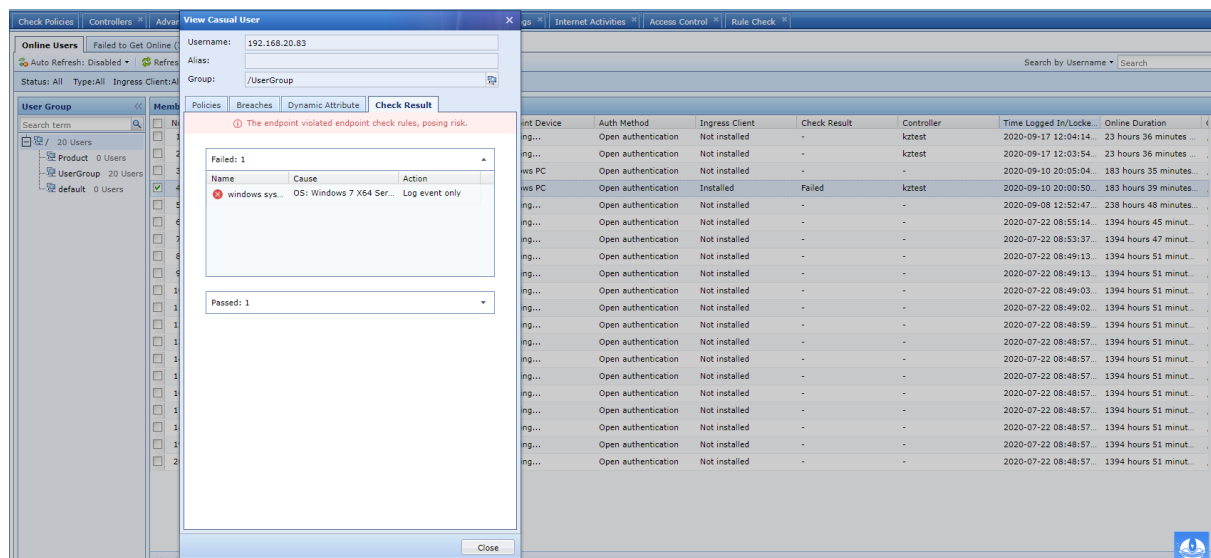
Endpoint Device	Auth Method	Ingress Client	Check Result	Time Logged In/Locked
Verifying...	Open authentication	Not installed	-	2020-09-17 12:04:14Lo
Verifying...	Open authentication	Not installed	-	2020-09-17 12:03:54Lo
Network	Open authentication	Not installed	-	2020-09-10 20:05:04Lo
Windows PC	Open authentication	Installed	Passed	2020-09-10 20:00:50Lo
Verifying...	Open authentication	Not installed	-	2020-09-08 12:52:47Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:55:14Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:53:37Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:49:13Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:49:13Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:49:03Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:49:02Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:48:59Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:48:57Lo
Verifying...	Open authentication	Not installed	-	2020-07-22 08:48:57Lo

Headquarter managed authentication berhasil, Anda dapat melihat status online pengguna branch.

The first screenshot shows the 'Sangfor Appliance' window with the 'Advanced' tab selected. The 'Status' column shows 'Active' for the device 'kztest'.

The second screenshot shows the 'Online Users' window with the 'Advanced' tab selected. The 'Check Result' column shows 'Failed' for the user 192.168.20.83.

No.	Time	Username	Group	IP Address	Controller	Name	Check Result	Details
1	2020-09-18 09:40:46	192.168.20.83	/UserGroup	192.168.20.83	local	windows system	illegal	OS: Windows 7 X64 Service Pack 1 (BuildNumber 7601)
2	2020-09-18 09:40:44	192.168.20.83	/UserGroup	192.168.20.83	local	Test	legal	checking



Bab 4 Tindakan Pencegahan

1. Setelah managed authentication di hidupkan, high availability active-active mode tidak didukung.
2. IAG sebagai authentication center tidak dapat menambahkan ke CM/BBC.



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