



IAM

Petunjuk Konfigurasi Larangan Pengunggahan

File pada QQ

Versi 12.0.18



Log Perubahan

Tanggal	Deskripsi Perubahan
Nov 22, 2019	Dokumen versi 12.0.18 .

Daftar isi

1 Skenario Aplikasi	1
2 Langkah Konfigurasi	1
3 Hasil Tes	3
4 Pencegahan	5

1 Skenario Aplikasi

Tolak pengguna intranet untuk mengunggah dokumen dengan menggunakan QQ Syarat kondisi:

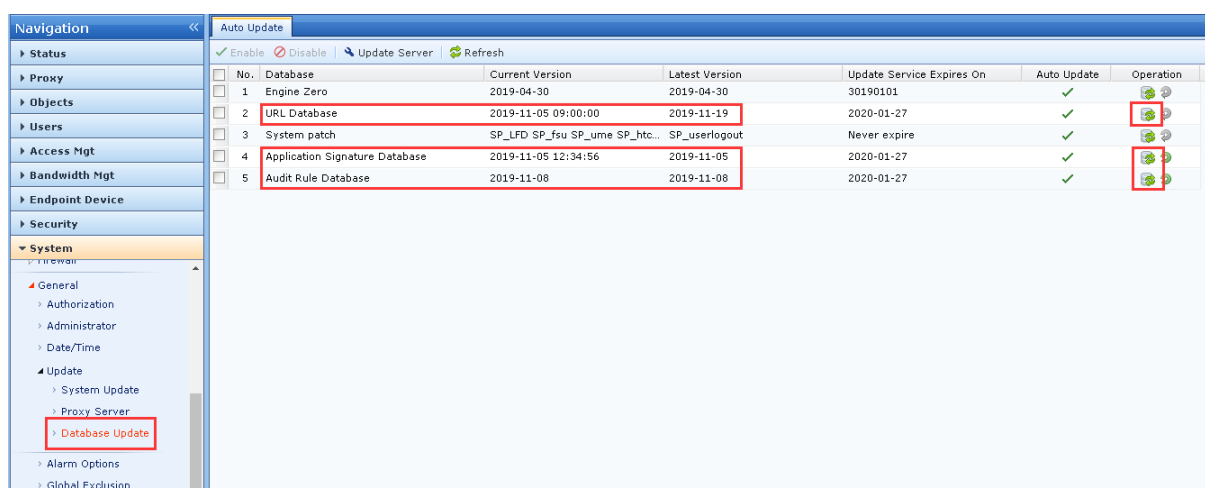
1. Siapkan satu perangkat IAM versi 11.0, dengan IP address 10.1.3.40.
2. Siapkan satu PC, dengan IP address 10.1.3.101.

2 Langkah Konfigurasi

Langkah pertama: perbaharui database ke versi yang terbaru.

[System] – [General] – [Update] – [Database Update], verifikasi apakah versi database yang saat ini adalah versi yang terbaru, harap pastikan bahwa [Application Signature Database] telah diupdate ke versi yang terbaru, jika tidak, klik [Update now] untuk memulai update ke versi terbaru.

Pastikan bahwa [URL Database], [Application Signature Database] dan [Audit Rule Database] memiliki 1 atau 2 update setiap bulannya.

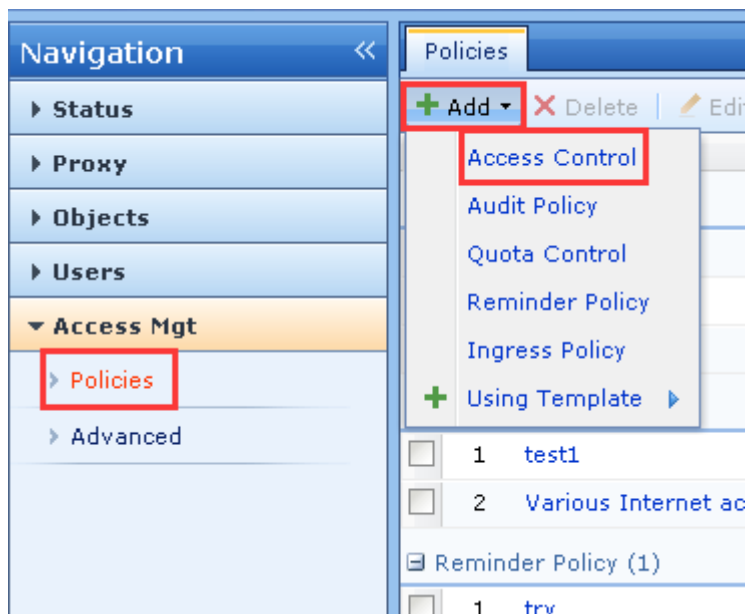


Ketika melakukan update database, harap pastikan bahwa masa berlaku lisensi masih valid, serta perangkat yang bisa mengunjungi situs web dan menyelesaikan domain secara normal.

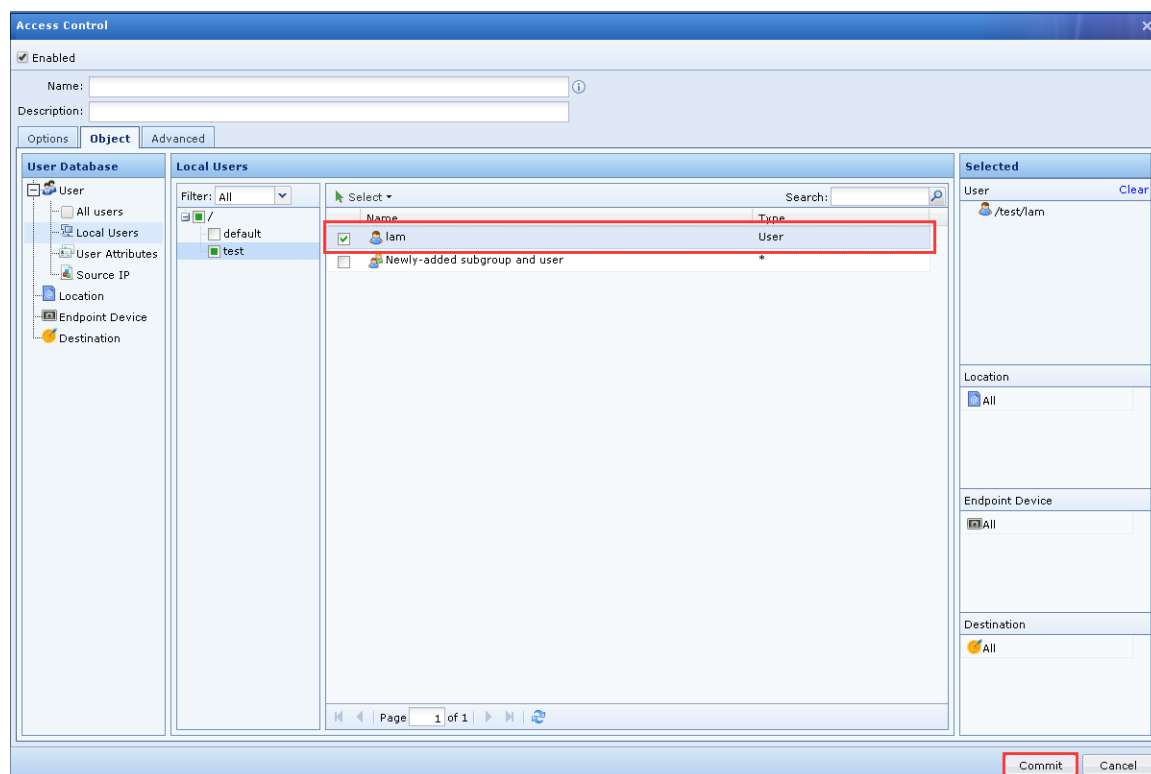
Langkah kedua: Konfigurasi access control policy.

Pada [Access Management] – [Policies], klik [Add] – [Access Control], masukkan nama untuk policy ini pada menu “Name”, kemudian pilih [Application], lanjutkan dengan klik [Add], pilih

aplikasi yang berhubungan dengan dokumen QQ atau transfer, **[Schedule]** sebagai All Day, **[Action]** sebagai Reject, **[Object]** bisa pilih all (untuk semua) atau specified user (untuk pengguna tertentu saya), selesaikan konfigurasi dengan meng-klik **[Commit]**, konfigurasi seperti diagram dibawah ini:



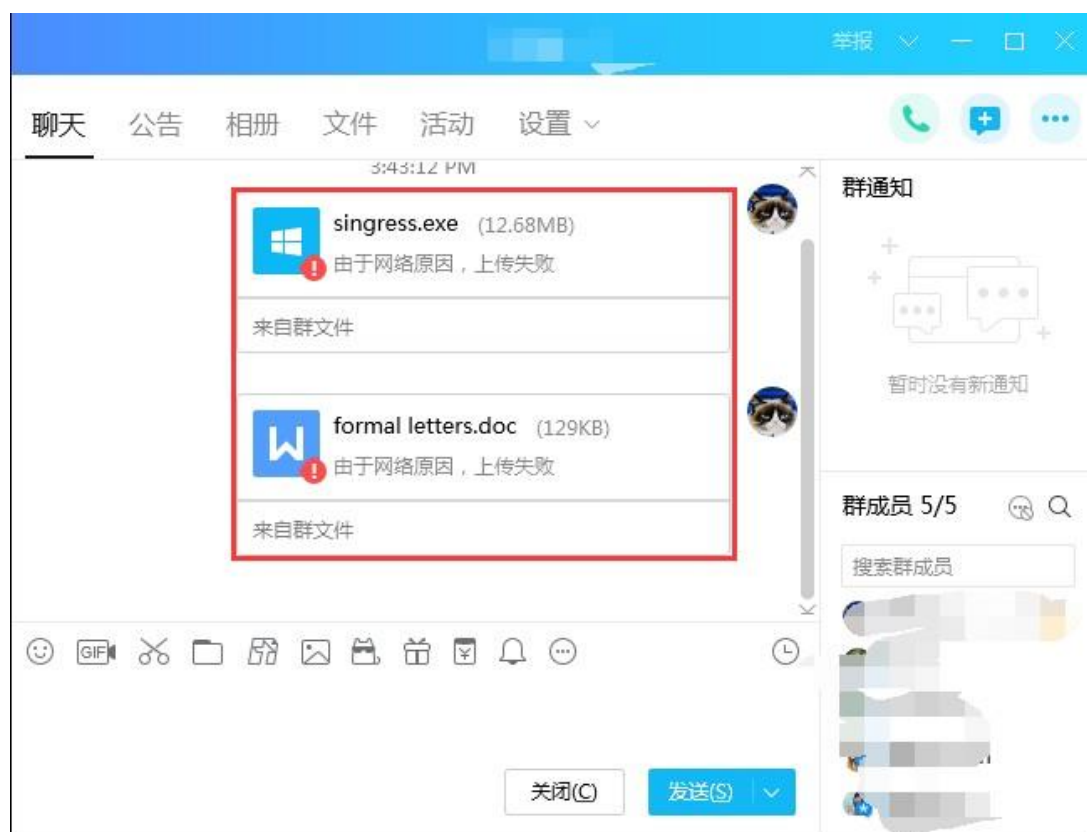
Ketika memilih **[Application]**, kamu bisa menggunakan menu search untuk mencari aplikasi, sebagai contoh, masukkan kata kunci "QQ", kita bisa melihat aplikasi yang berhubungan dengan QQ seperti **[QQSendFile]** dan **[WebQQ-SendFile]**, klik pada aplikasi **[QQSendFile]** maka kamu akan melihat **[Application Details]** pada bagian pojok kanan bawah, rinciannya meliputi nama aplikasi, tag, deskripsi, dan situs web resmi.



3 Hasil Tes

Setelah login pada QQ, baik pemindahan file secara offline maupun instant, perintah tersebut akan ditolak oleh perangkat IAM, bisa dilihat pada diagram dibawah.

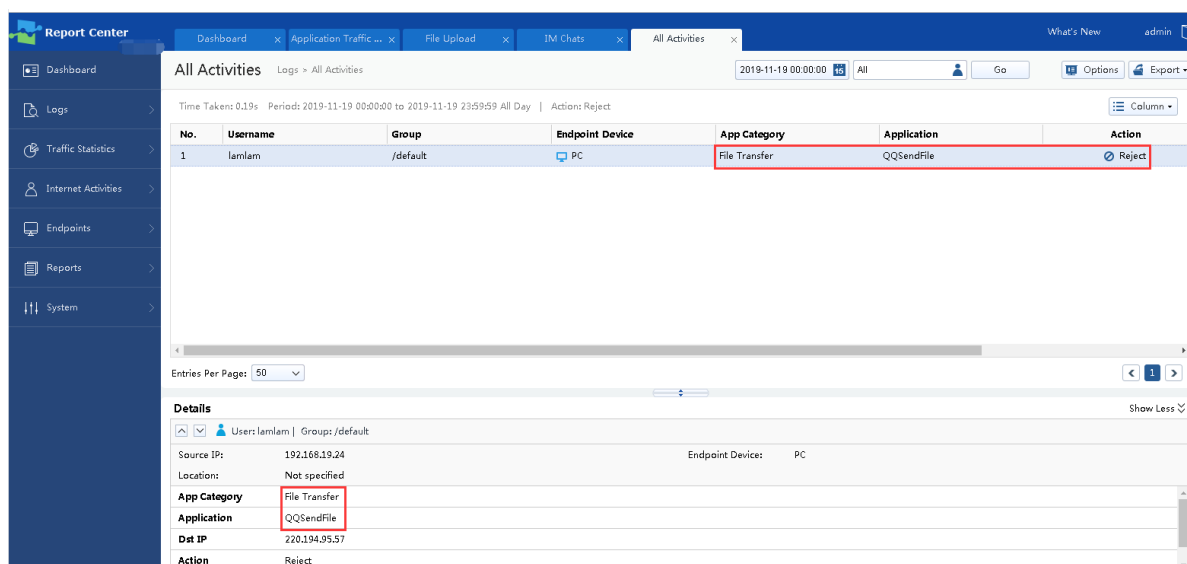
1. Pada tampilah layar ini bisa dilihat proses pengiriman file QQ tidak berhasil



2. Kita juga bisa cek **[Status] – [Internet Activities]**, kita bisa lihat secara real-time, bahwa transfer file QQ ditolak.

Navigation		Authentication Policy Internet Activities						
- Status - Dashboard - Online Users - Troubleshooting Center - Traffic Statistics Internet Activities - Locked Users - SaaS Applications - Security Events		Auto Refresh: 5 second(s) Filter Filter: Group (/) Objects: Outgoing Files Action: Reject Alert						
No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
1	8 minutes ago	lamlam	/default	192.168.19.24	File Transfer	QQSendFile	Reject	

3. Dari **[Internal Report Center] – [Logs] – [All Activities]**, kita bisa melihat bawah pemindahan file QQ ditolak QQ pada bagian file transfer



The screenshot shows the 'Report Center' interface with a sidebar on the left containing navigation links: Dashboard, Logs, Traffic Statistics, Internet Activities, Endpoints, Reports, and System. The main area is titled 'All Activities' and displays a table of activity logs. Below the table is a 'Details' section for the selected entry.

No.	Username	Group	Endpoint Device	App Category	Application	Action
1	lamiam	/default	PC	File Transfer	QQSendFile	Reject

Details	
Users: lamiam Groups: /default	
Source IP:	192.168.19.24
Location:	Not specified
App Category	File Transfer
Application	QQSendFile
Dst IP	220.194.95.57
Action	Reject

4 Pencegahan

1. Jika database tidak bisa diperbaharui, silakan periksa:

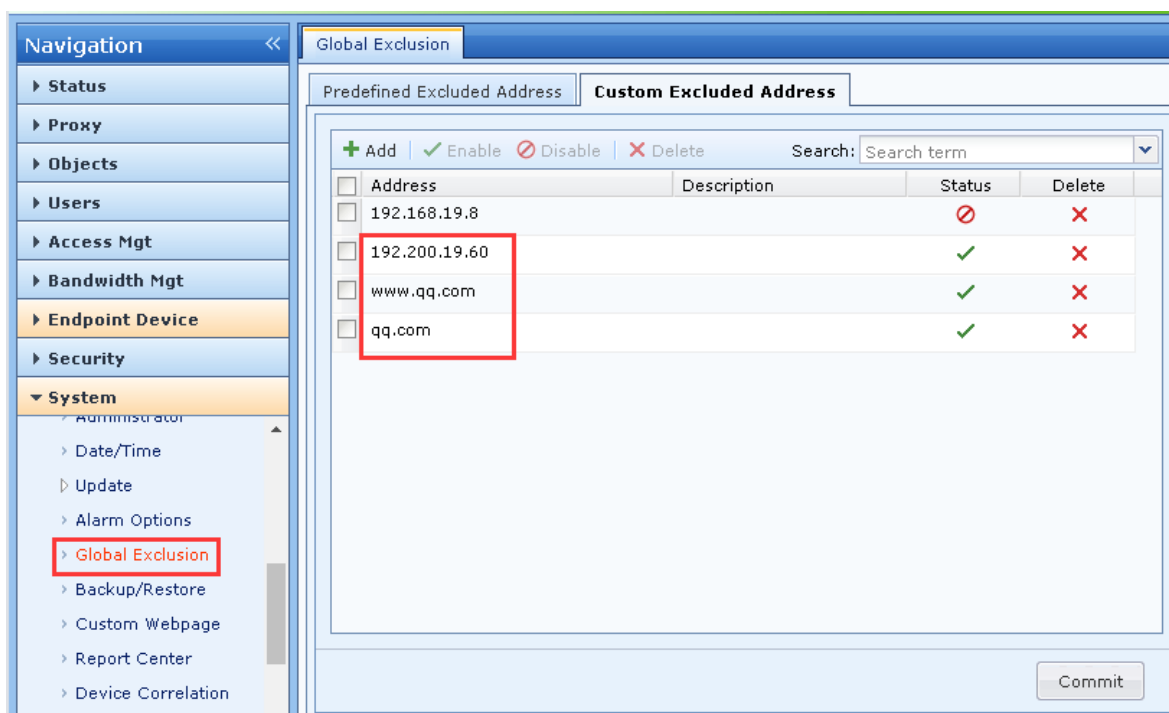
Pastikan masa berlaku lisensi masih valid.

Harap pastikan bahwa perangkat dapat mengunjungi situs web dan menyelesaikan domain secara normal, karena pembaruan database terhubung ke server dengan port 80 untuk melakukan pembaruan. Dengan menggunakan konsol pada **[System] – [Diagnostics] – [Web Console]**, telnet yang merupakan nama domain dengan nomor port, seperti contoh: telnet www.baidu.com 80. Jika didapat “connect OK”, Berarti bahwa alat bisa akses ke internet dan menyelesaikan domain secara normal. Jika koneksi gagal, silahkan cek konfigurasi DNS dan apakah konfigurasi proxy bertindak sebagai proxy untuk IAM dalam mengakses jaringan internet.

Pastikan komunikasi antara IAM dan server berhasil. Kamu bisa melakukan test koneksi server pada **[System] – [General] – [Update] – [Database Update] – [Update server]**. Kamu bisa melakukan test dengan server yang berbeda untuk memastikan bahwa komunikasi berjalan normal. Jika koneksi berjalan normal, maka gunakan server yang berbeda untuk memperbaharui database.

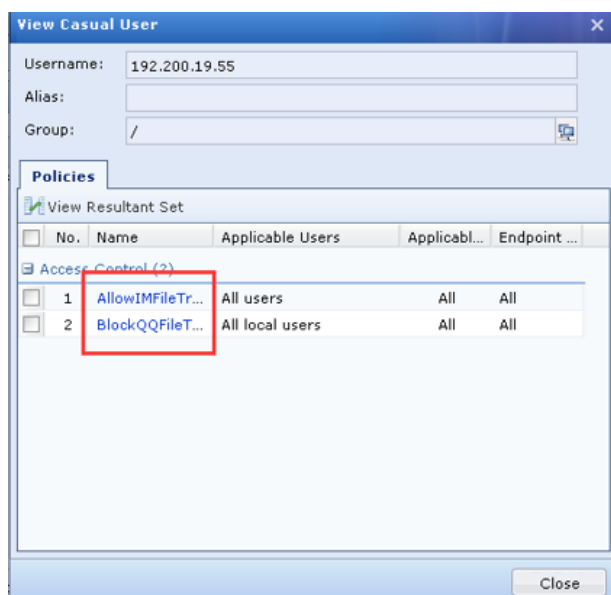
Direkomendasikan untuk merujuk pada link berikut untuk mendapatkan detail konfigurasi lebih lanjut:

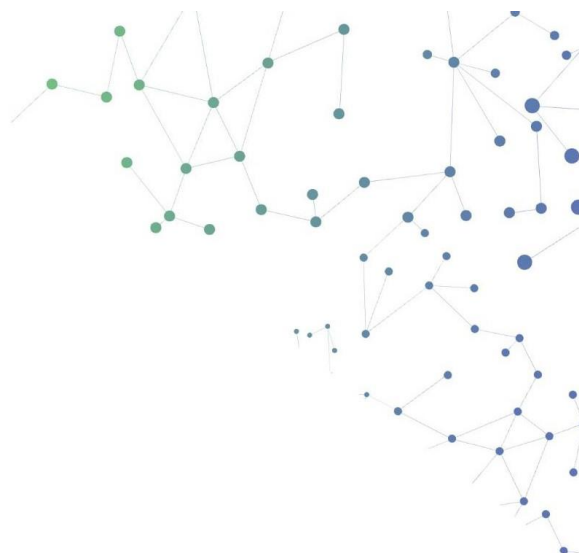
2. Kebijakan hanya akan berlaku kepada user setelah diotorisasi oleh IAM. Jika user bisa mengakses internet tanpa melalui perangkat, atau alamat IP user, nama domain QQ ditambahkan pada pengecualian global, ini tidak akan berpengaruh kepada kebijakan.



3. Peraturan kebijakan yang sama adalah untuk keseluruhan mulai dari level atas sampai bawah, ketika kondisi cocok dengan kebijakan, maka seterusnya tidak akan cocok dengan kebijakan berikutnya.

Sebagai contoh, diagram dibawah menunjukkan user telah menetapkan 2 kebijakan. Kebijakan pertama memperbolehkan transfer file IM, dan yang kedua adalah mencegah transfer file QQ. Seperti yang kita lihat kebijakan pertama berada diatas kebijakan kedua, sehingga transfer file QQ akan diperbolehkan. apabila kita mau mencegah transfer file QQ, adalah dengan menggeser kebijakan kedua keatas ke urutan teratas, kemudia kebijakan itu akan berlaku mencegah transfer file QQ diikuti dengan memungkinkan transfer file IM.





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

