



IAM

Best Practices for Scenarios_Access Control Policy

Version 12.0.42



Change Log

Date	Change Description
July 26, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

CONTENT

Chapter 1 Scenario	1
Chapter 2 Configuration.....	1
Chapter 3 Configuration.....	3
3.1 Block Facebook.....	3
3.2 Block Gmail Outgoing Attachments	5
Chapter 4 Precaution.....	12

Chapter 1 Scenario

The R&D department of a software company has strict control over intranet users and needs to prohibit users from accessing Facebook during working hours. In addition, in order to ensure information security, users are prohibited from using Gmail to send files, and IAM can be used for behavior control related behaviors.

Chapter 2 Configuration

1. Check the authorization and database version to ensure that the rule base has been updated to the latest date. The application control policy for processing data packets relies on the database. If the database is not updated to the latest version, the identification of some traffic may be wrong.

The screenshot shows the Sangfor IAM12.6.42 web interface. The left sidebar contains a navigation menu with options like Status, Proxy, Objects, Users, Access Mgt, Bandwidth Mgt, Endpoint Device, Security, and System. The main content area is titled 'Licensing' and shows the 'Authorization Method: Authorization via Licensing Server'. It lists several licenses with their status and expiration dates. The 'Application Signature Database' and 'Sangfor URL Database' are highlighted with red boxes.

No.	Database	Current Version	Latest Version	Update Service Expires On	Auto Update	Operation
1	Engine Zero	2020-06-22	2020-07-21	2019-01-01	✓	⬇ ⬆
2	URL Database	2020-07-14 09:00:00	2020-07-21	2020-09-23	✓	⬇ ⬆
3	System patch	SP_LFD SP_ksu SP_ame SP_Htc SP_ves SP_WP_ SP_ser0101	2020-07-14	Never expire	✓	⬇ ⬆
4	Application Signature Database	2020-07-14 12:34:56	2020-07-14	2020-09-23	✓	⬇ ⬆
5	Audit Rule Database	2020-07-15	2020-07-15	2020-09-23	✓	⬇ ⬆

2. Ensure that network traffic passes through the IAM device in both directions. If the traffic is only one-way, then the application cannot be identified and controlled.

The screenshot shows the Sangfor IAM12.6.42 web interface. The left sidebar contains a navigation menu with options like Status, Proxy, Objects, Users, Access Mgt, Bandwidth Mgt, Endpoint Device, Security, and System. The main content area is titled 'Capture Packets' and shows a table of captured packets. The status bar at the top indicates 'Status: Program is running'.

No.	Name	Size	Download	Delete
1	2020-07-27-143016_eth0_tcpdump.pcap	360(KB)	Download	✗
2	2020-07-27-143016_eth2_tcpdump.pcap	874.62(KB)	Download	✗

Access Control Policy

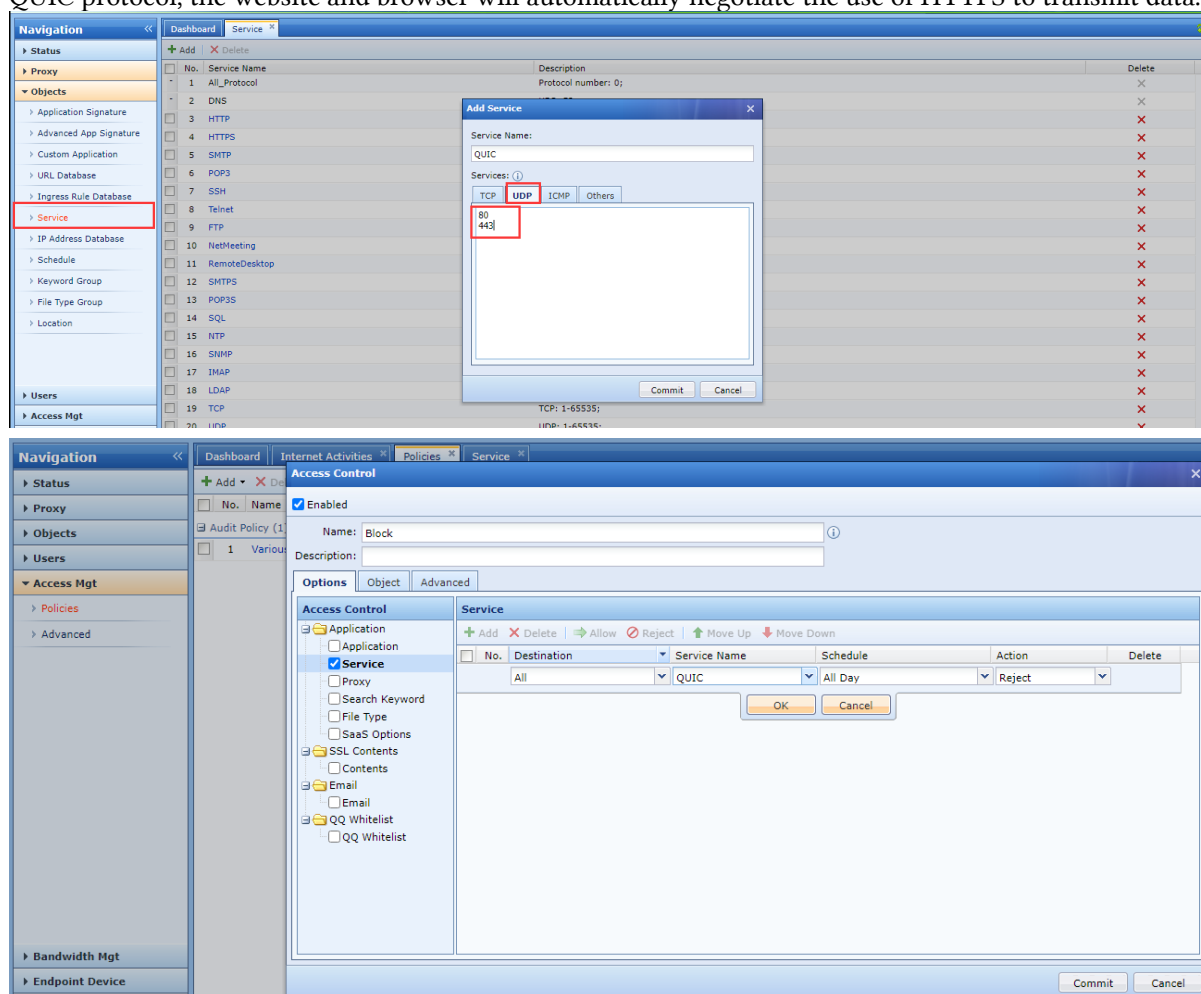
No.	Time	Source	Destination	Protocol	Length	Bytes in Flight	Info
8	2020/209 14:30:40.043783	192.168.1.3	216.58.196.36	TCP	66		50121 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	2020/209 14:30:40.043794	216.58.196.36	192.168.1.3	TCP	66		443 → 50121 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
10	2020/209 14:30:40.044082	192.168.1.3	216.58.196.36	TCP	54		50121 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
11	2020/209 14:30:40.044803	192.168.1.3	216.58.196.36	TLSv1.2	571	517	Client Hello
12	2020/209 14:30:40.044806	216.58.196.36	192.168.1.3	TCP	54		443 → 50121 [ACK] Seq=1 Ack=518 Win=65536 Len=0
13	2020/209 14:30:40.118146	216.58.196.36	192.168.1.3	TLSv1.2	1010		956 Server Hello, Certificate, Server Key Exchange, Server Hello Done
14	2020/209 14:30:40.120615	192.168.1.3	216.58.196.36	TLSv1.2	61		7 Alert (Level: Fatal, Description: Certificate Unknown)
15	2020/209 14:30:40.120619	216.58.196.36	192.168.1.3	TCP	54		443 → 50121 [ACK] Seq=957 Ack=525 Win=65536 Len=0
16	2020/209 14:30:40.120980	192.168.1.3	216.58.196.36	TCP	54		50121 → 443 [FIN, ACK] Seq=525 Ack=957 Win=2101248 Len=0
17	2020/209 14:30:40.120982	216.58.196.36	192.168.1.3	TCP	54		443 → 50121 [FIN, ACK] Seq=957 Ack=526 Win=65536 Len=0
18	2020/209 14:30:40.121832	192.168.1.3	216.58.196.36	TCP	54		50121 → 443 [ACK] Seq=526 Ack=958 Win=2101248 Len=0

3. Configure audit policies. Actual applications often contain multiple rules. It is necessary to check which rules the application traffic is recognized by the IAM database.

The screenshots illustrate the configuration of an Audit Policy in the Sangfor IAM system. The first screenshot shows the 'Policies' management interface with a list of policies. The second screenshot shows the 'Audit Policy [Various Internet activities and traffic]' configuration window, where the 'Object' tab is selected. The 'Object' tab displays a list of applications, including 'Web-based BBS posting', 'Web Mail contents', 'Web-based attachment upload', and 'Web-based text upload'. The 'Application' tab is also visible, showing a list of applications. The third screenshot shows the 'Edit IP Group' dialog box, where the 'Name' is 'Test' and the 'IP Address' is '192.168.1.3'. The 'Selected' list on the right shows the 'Test' IP group selected.

4. Now many websites and browsers use the QUIC protocol to transmit data, and the data encrypted by

the QUIC protocol cannot be controlled, so the QUIC protocol needs to be disabled. After disabling the QUIC protocol, the website and browser will automatically negotiate the use of HTTPS to transmit data.

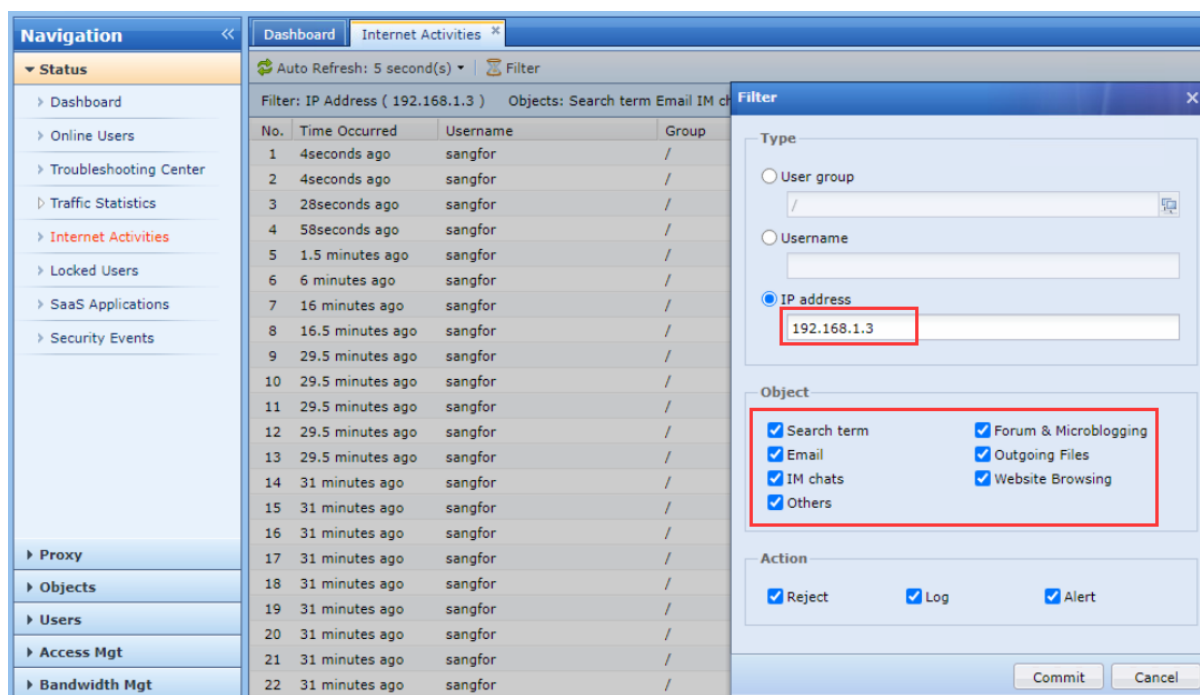


Chapter 3 Configuration

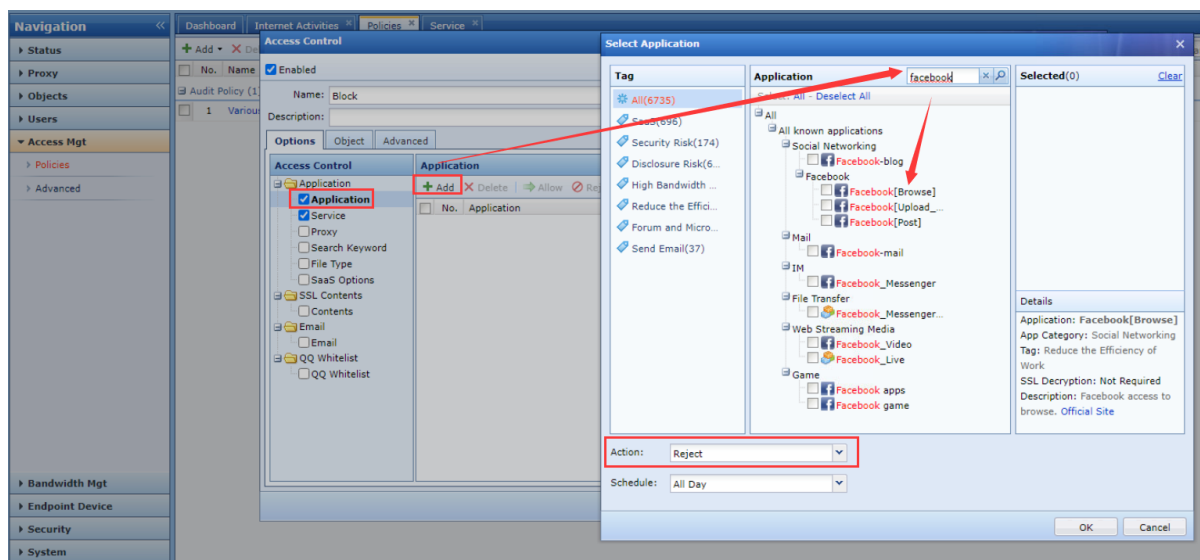
3.1 Block Facebook

1. Use a browser to access facebook.com, and check which rules Facebook traffic has been recognized in Internet Activities.

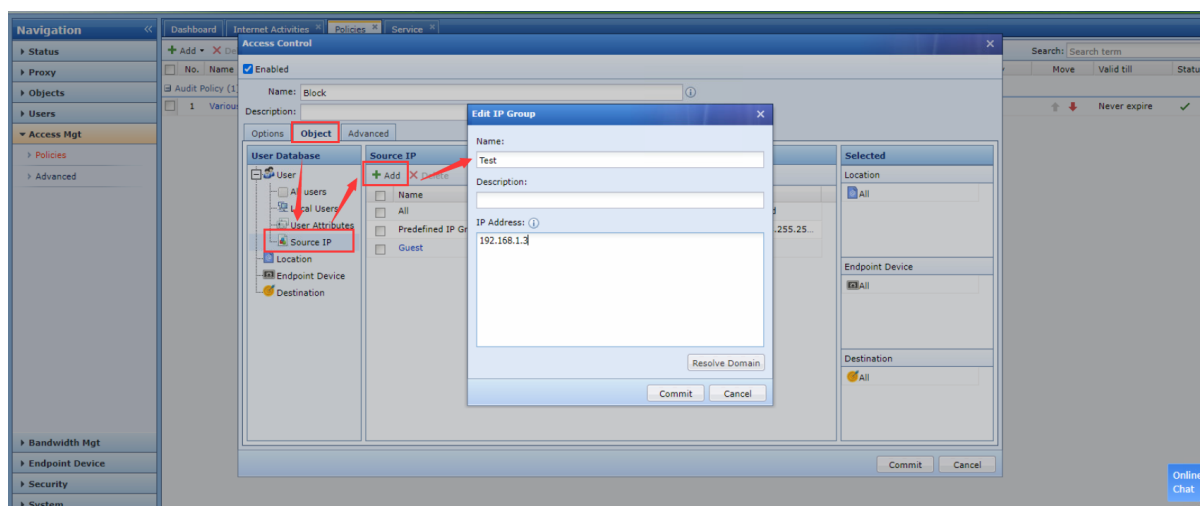
Access Control Policy



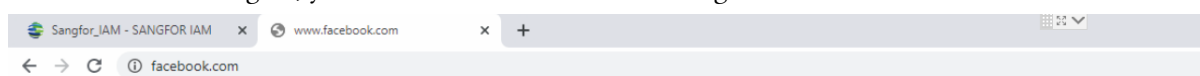
2. Add the corresponding Facebook[Browse] rule in the application control policy, and select the action as reject.



3. Select the users who needed to be matched by the policy, you can choose by username or by source IP.



4. Access Facebook again, you can see that Facebook is no longer accessible.



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_RESET

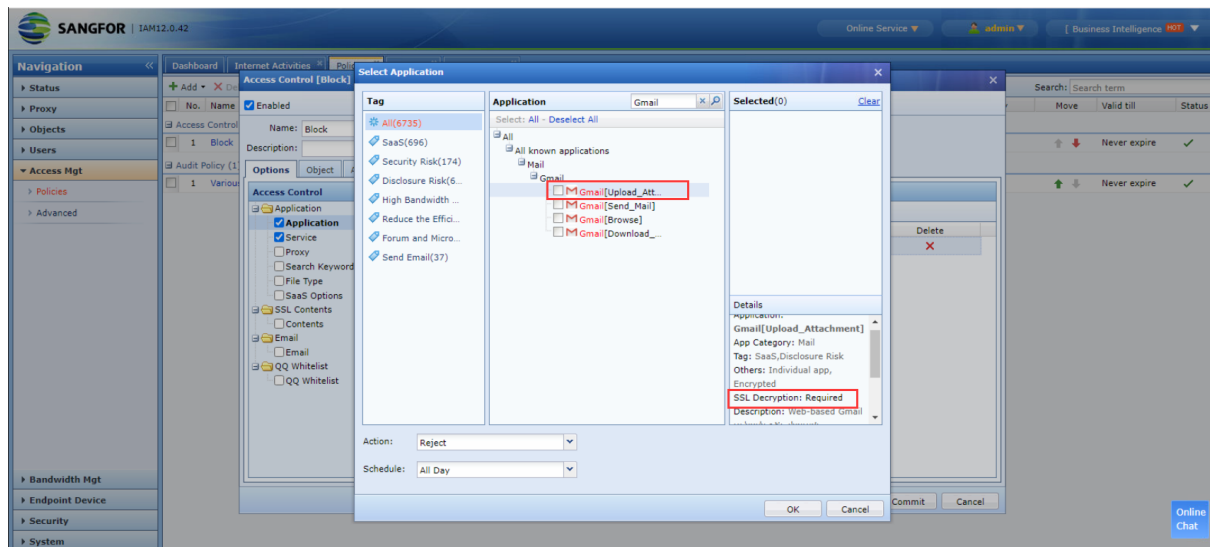
Reload

Details

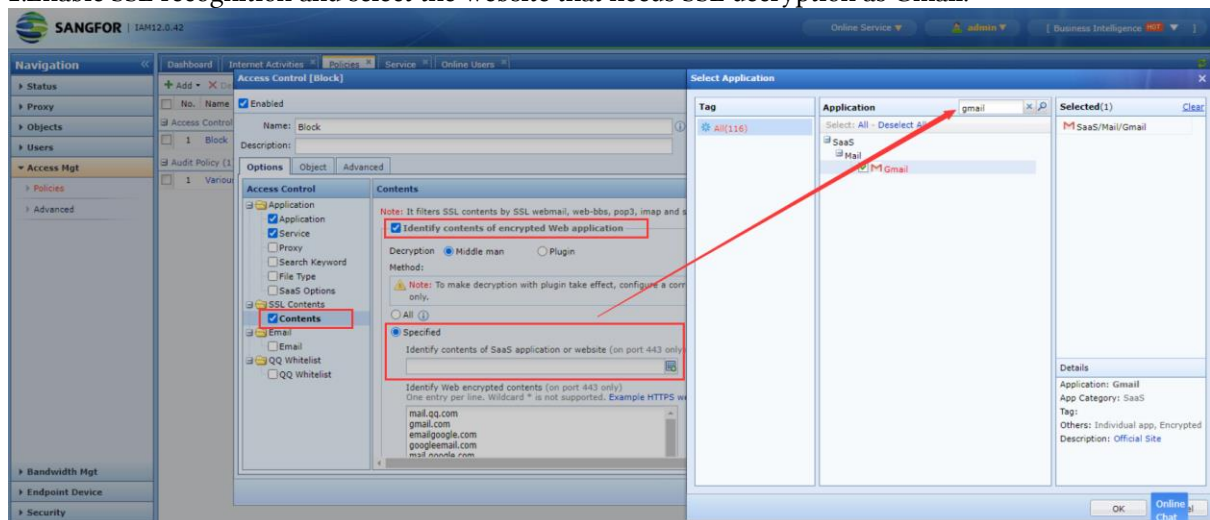
3.2 Block Gmail Outgoing Attachments

1. If you want to perform more detailed control on the behavior of the https website, such as allowing browsing but not uploading attachments, then you need to check the IAM rule description to determine whether you need to decrypt the traffic of the relevant domain name. For example, after querying the description of the rule base, you can know that Gmail uploading attachments needs to enable SSL data decryption.

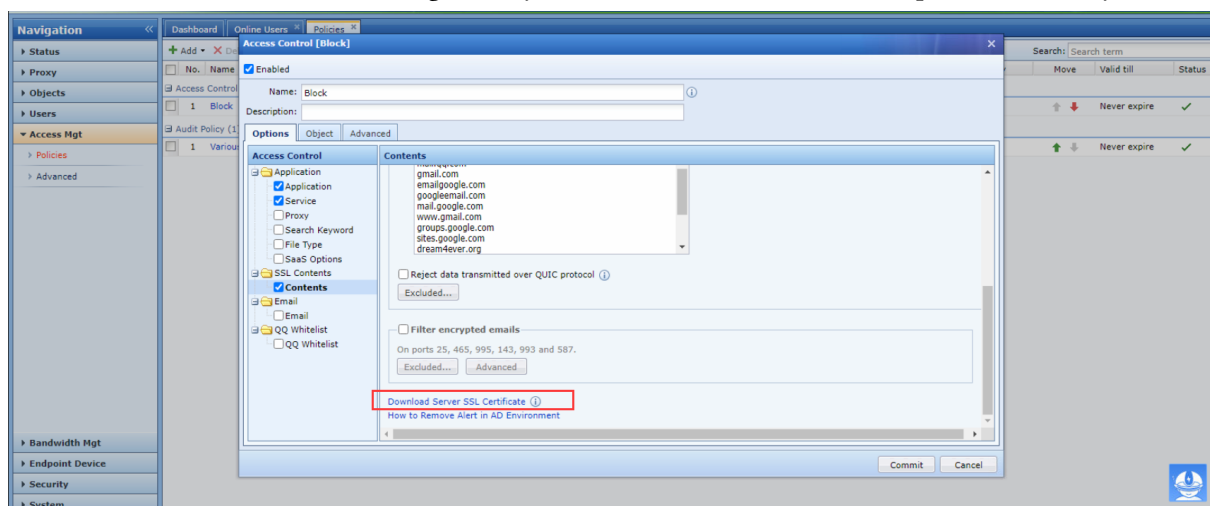
Access Control Policy

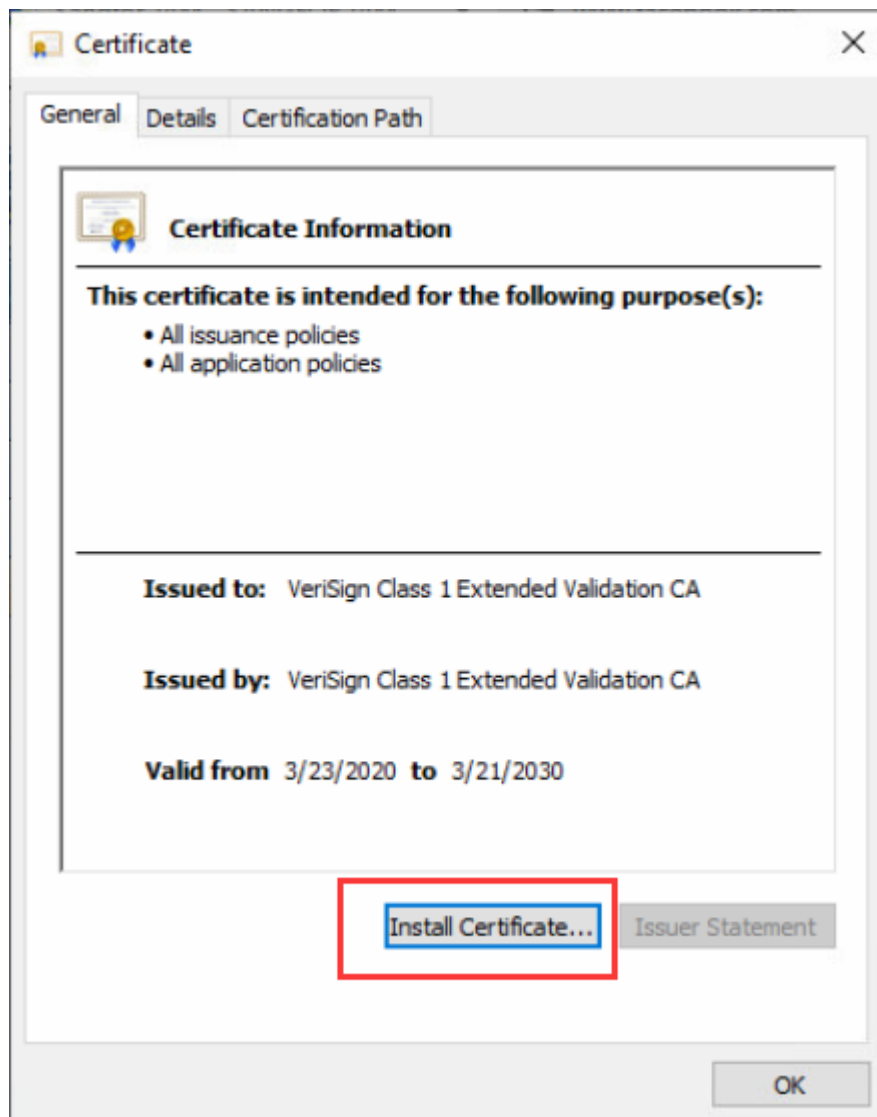


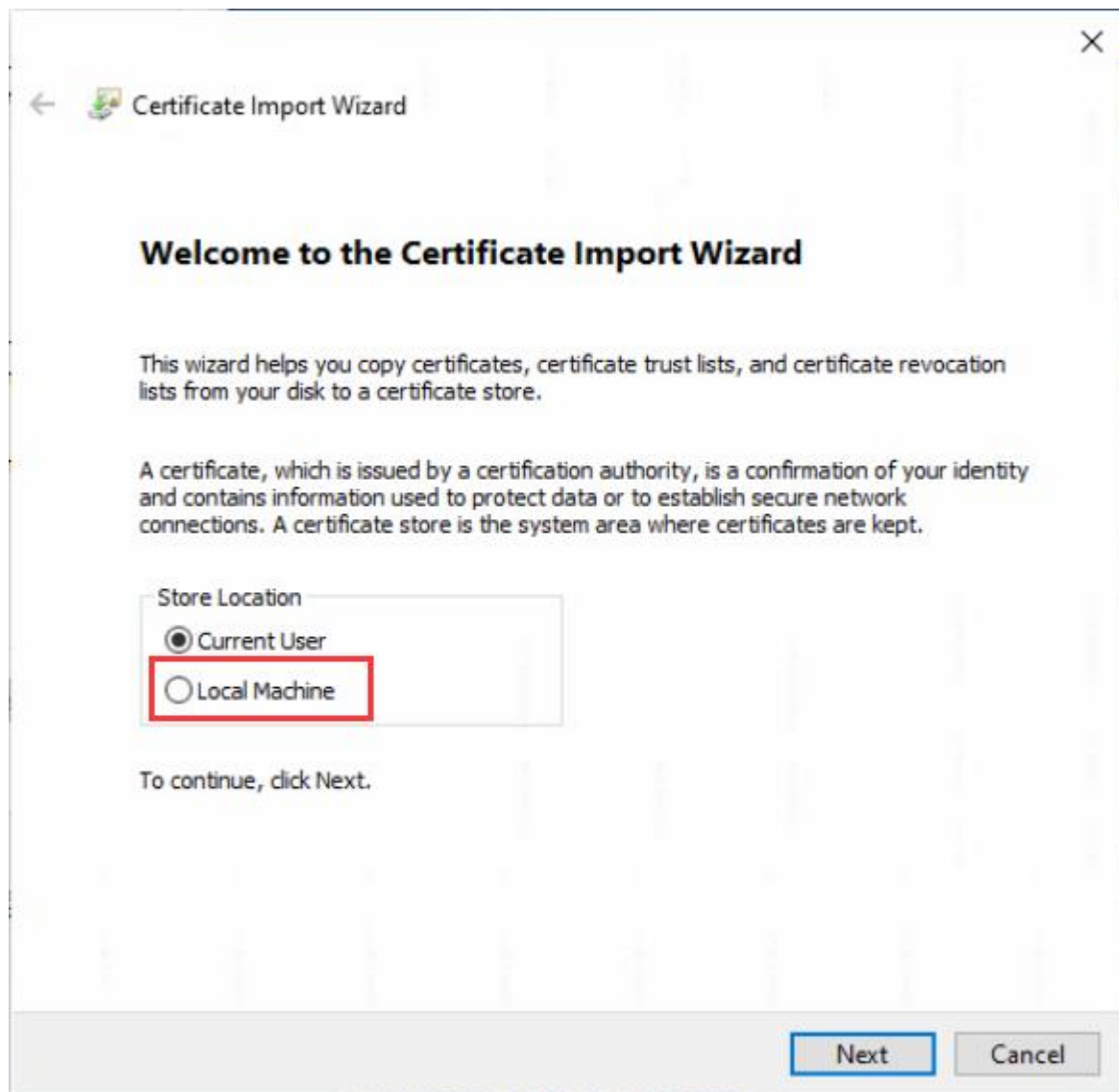
2. Enable SSL recognition and select the website that needs SSL decryption as Gmail.

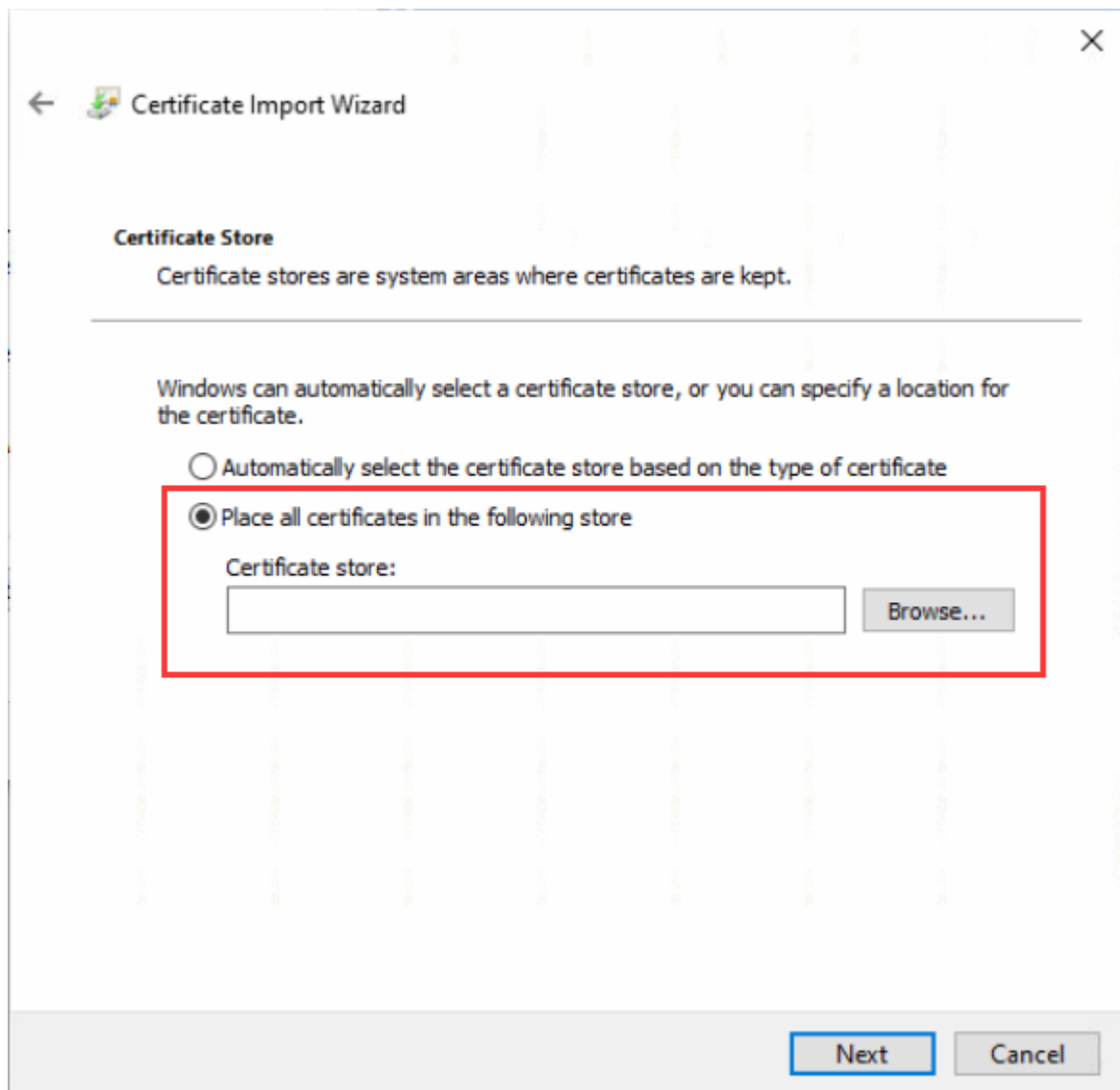


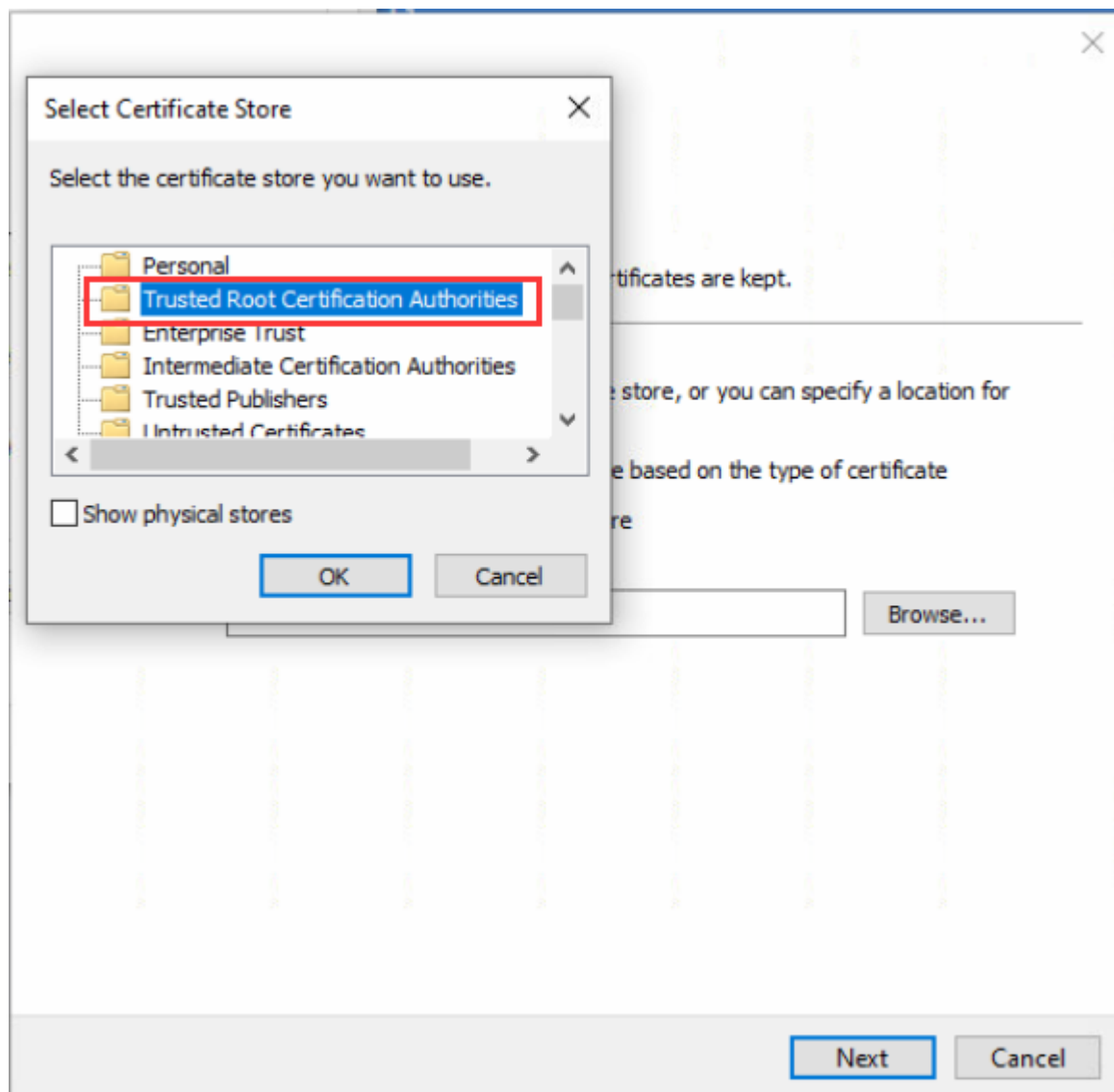
3. Download the root certificate recognized by SSL from the IAM device and import it into the system.

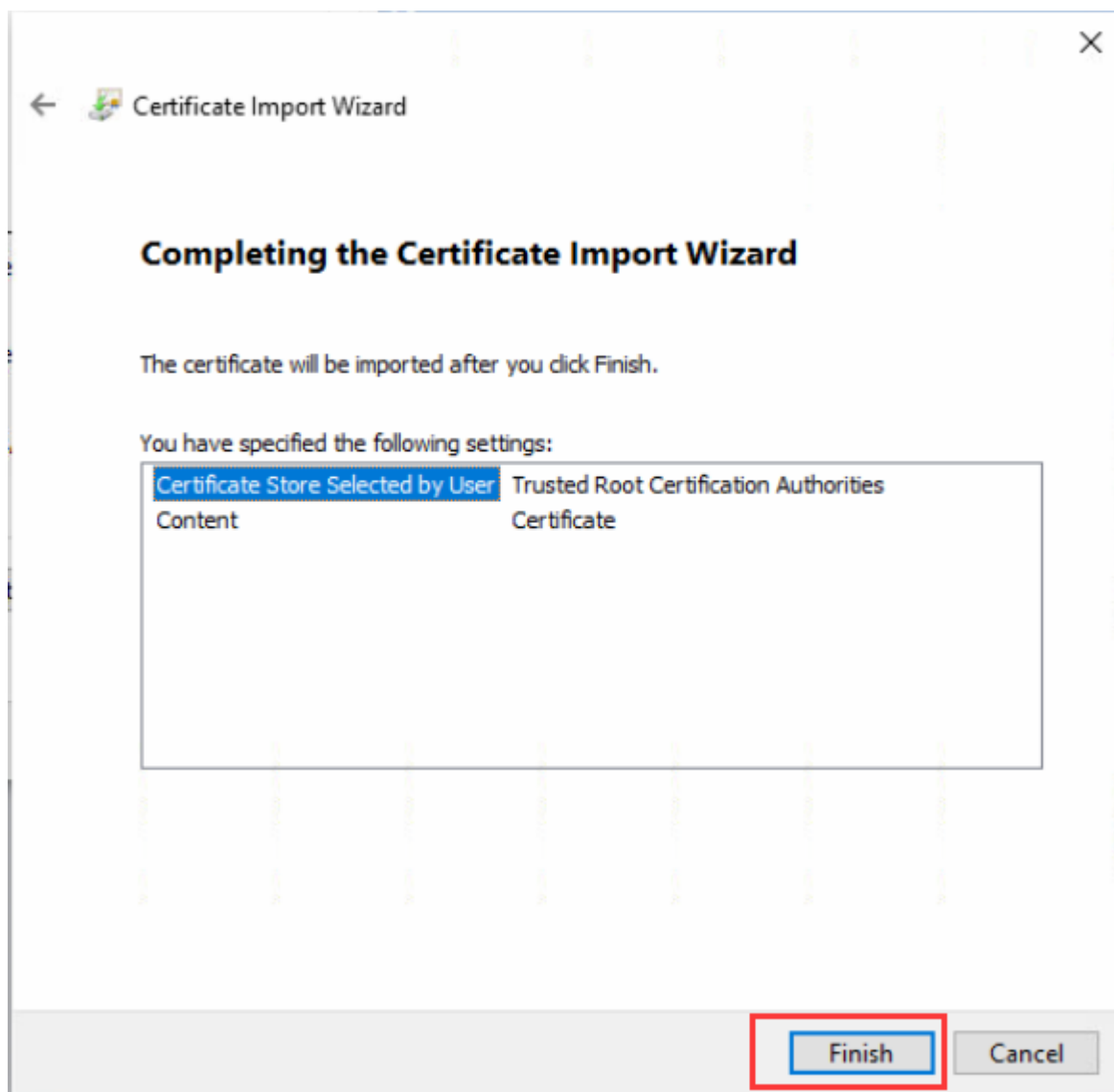




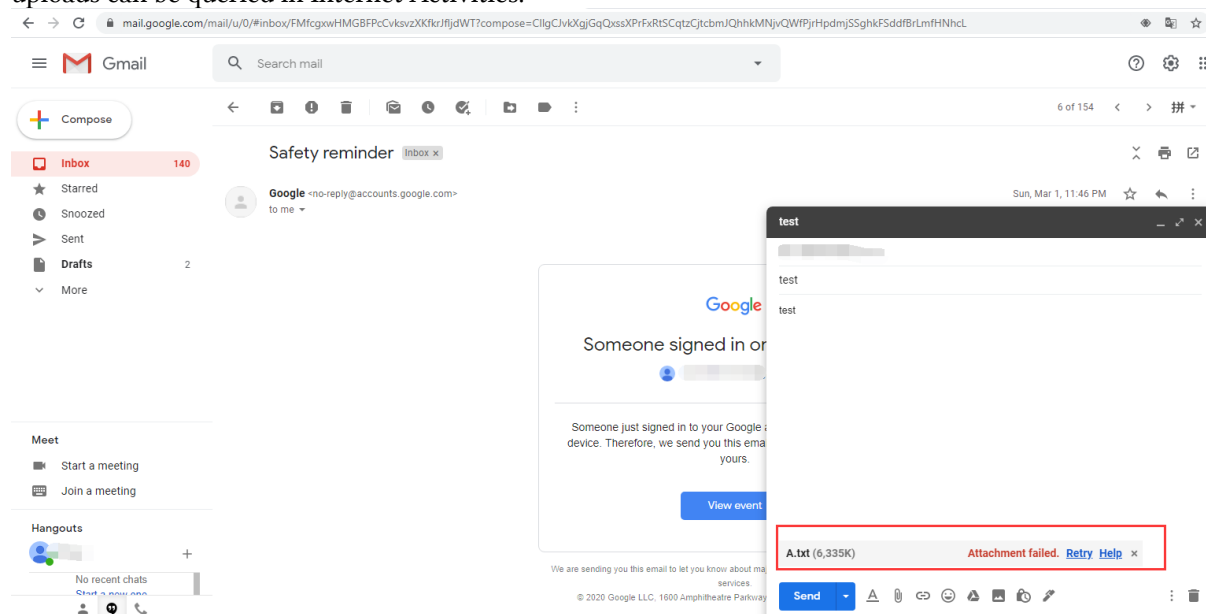








3. It shows that Gmail has been unable to upload attachments, and the log of rejecting attachment uploads can be queried in Internet Activities.



Navigation		Dashboard Online Users Policies Internet Activities								
Status		Auto Refresh: 5 second(s) Filter								
Dashboard		Filter: Group (/) Objects: Search term Email IM chats Forum & Microblogging Outgoing Files Website Browsing Action: Reject Log Alert								
Online Users		No.	Time Occurred	Username	Group	IP Address	App Category	Application	Action	Details
Troubleshooting Center		1	1.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Log	URL: mail.google.com
Traffic Statistics		2	1.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Search Engine	Reject	URL: googlemail.google.com
Internet Activities		3	2 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Upload_Att.	Reject	
Locked Users		4	2 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Reject	URL: mail.google.com
SaaS Applications		5	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
Security Events		6	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		7	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		8	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
		9	6 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com
		10	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		11	6 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		12	6.5 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com/mail/u/0?ui=2&ik=687af392f7 Website: mail.google.com
		13	6.5 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com/mail/u/0?ui=2&ik=687af392f7 Website: mail.google.com
		14	6.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
		15	6.5 minutes ago	sangfor	/	192.168.1.3	Visit Web Site	Mailbox(Web)	Log	URL: mail.google.com
Proxy		16	7 minutes ago	sangfor	/	192.168.1.3	Mail	Other Web Mail[P.	Log	URL: mail-ads.google.com
Objects		17	7 minutes ago	sangfor	/	192.168.1.3	Mail	Gmail[Browse]	Log	URL: mail.google.com

Chapter 4 Precaution

1. It is recommended to upload a new file that has not been uploaded. If the file exists on the Google server, it will not be re-uploaded. It will display that the upload is completed within an instant. In this way, the traffic of the uploaded attachment does not actually pass through IAM, so IAM cannot Blocked. To create a brand-new file, you can take the following operations: manually create a txt file, then fill in any fields in it, and keep copying and pasting to make the file size around 5MB.
2. Before selecting the rules in the application control policy, it is recommended to open the audit policy first, then use the application and trigger the relevant application traffic, and then observe which rules the actual application traffic contains in Internet Activities.



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