SANGFOR

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.

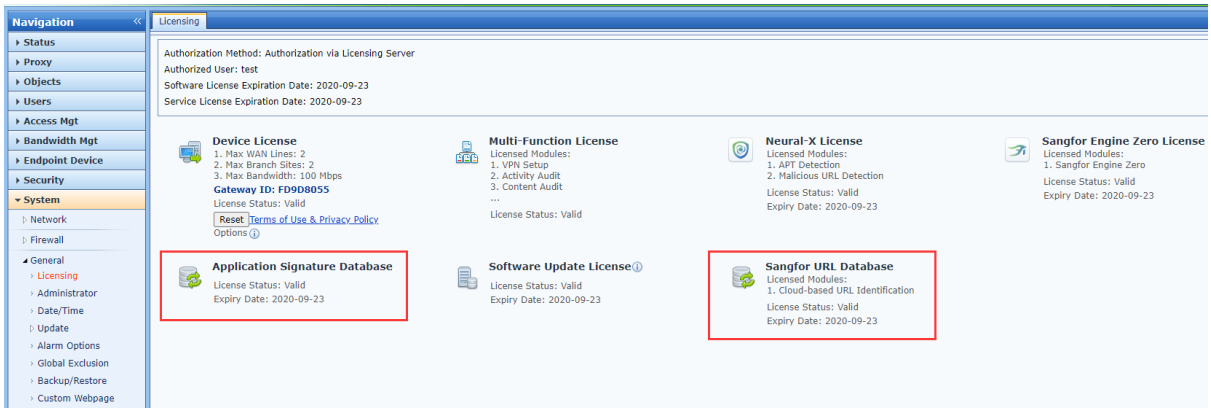
CONTENT

Chapter 1 Scenario

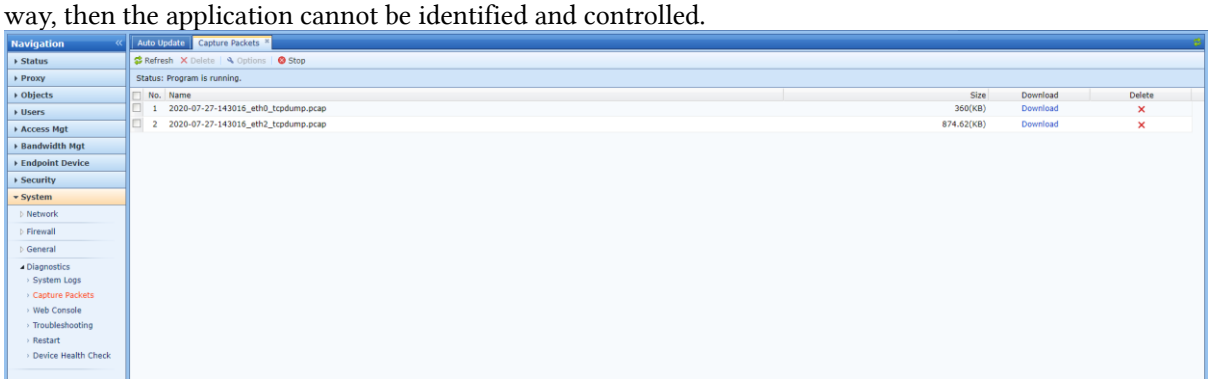
The R&D department of a software company has strict control over intranet users and needs to prohibit users from accessing Facebook during working hours. In addition, in order to ensure information security, users are prohibited from using Gmail to send files, and IAM can be used for behavior control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

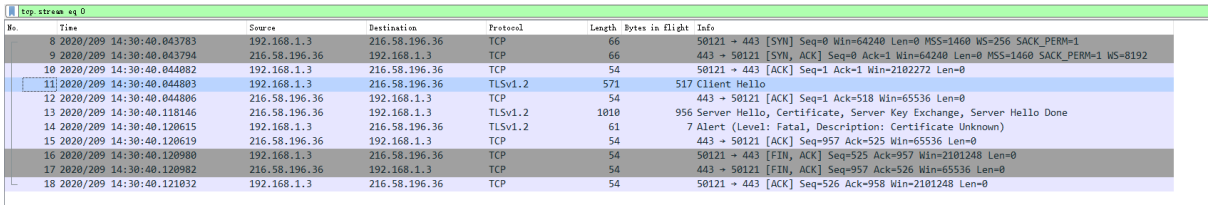
Chapter 2 Configuration

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.

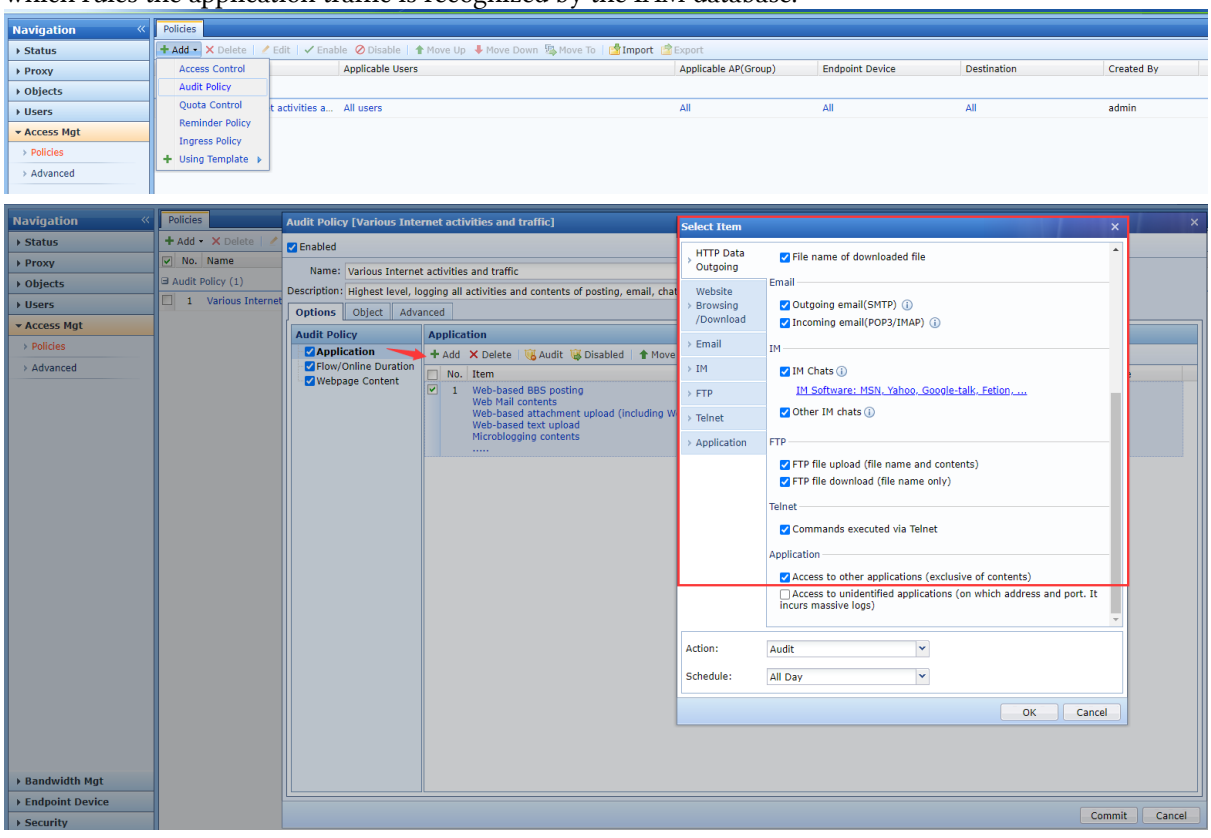


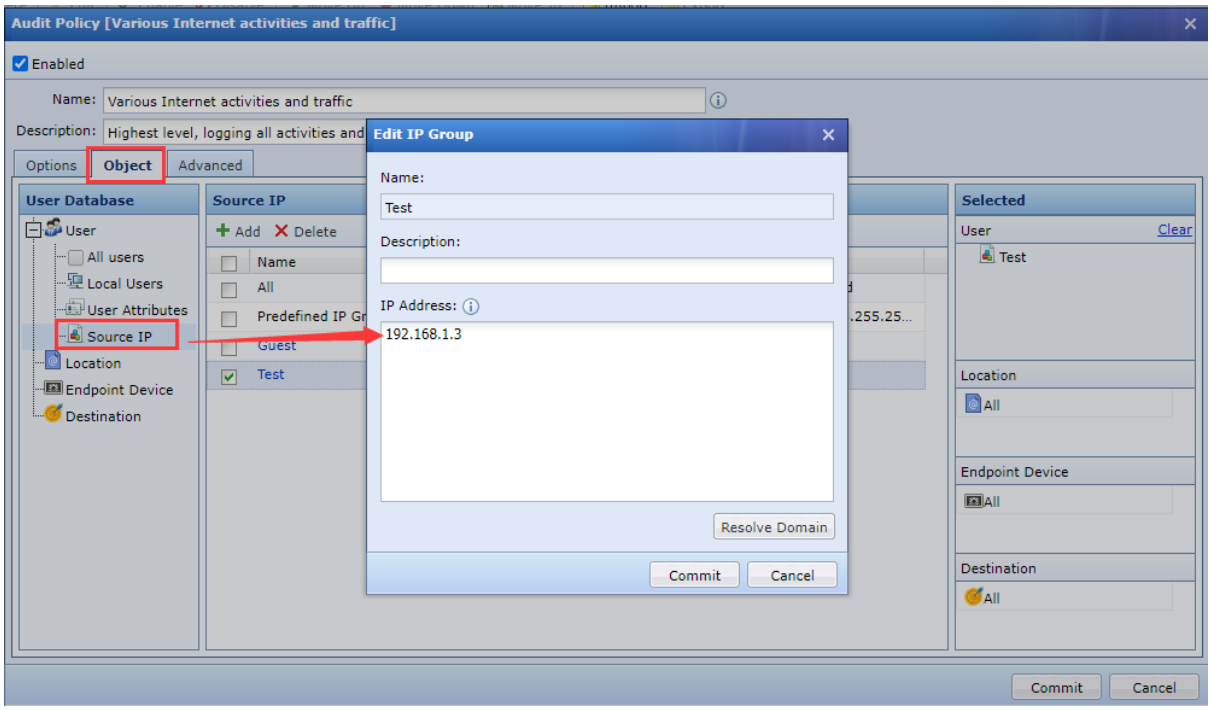
2. Ensure that network traffic passes through the IAM device in both directions. If the traffic is only one-way, then the application cannot be identified and controlled.





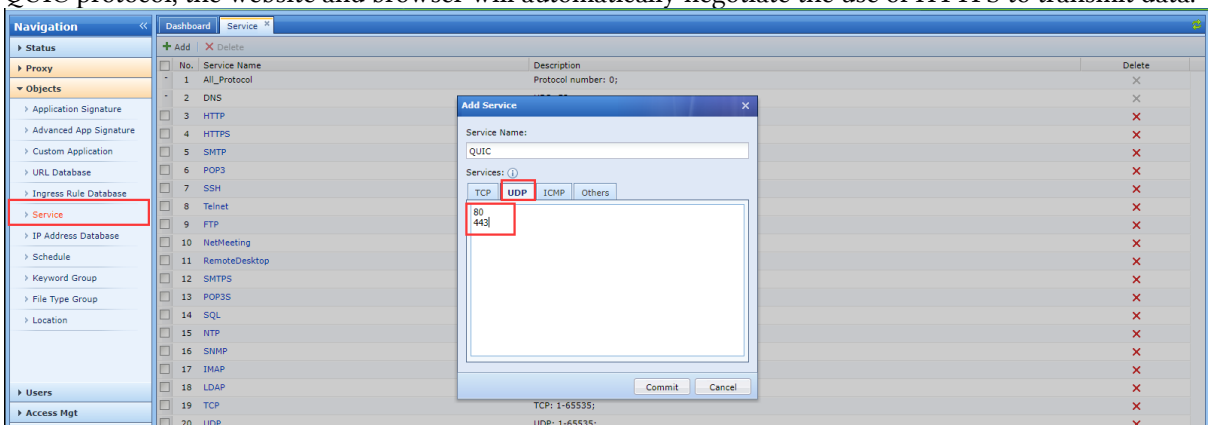
3. Configure audit policies. Actual applications often contain multiple rules. It is necessary to check which rules the application traffic is recognized by the IAM database.

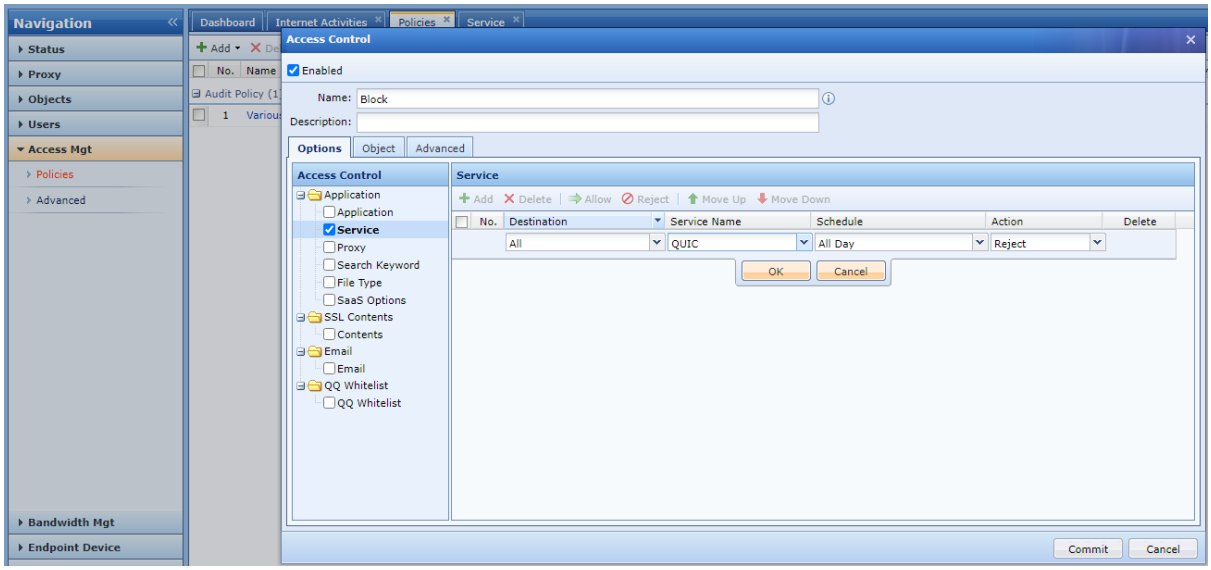




4. Now many websites and browsers use the QUIC protocol to transmit data, and the data encrypted by

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.

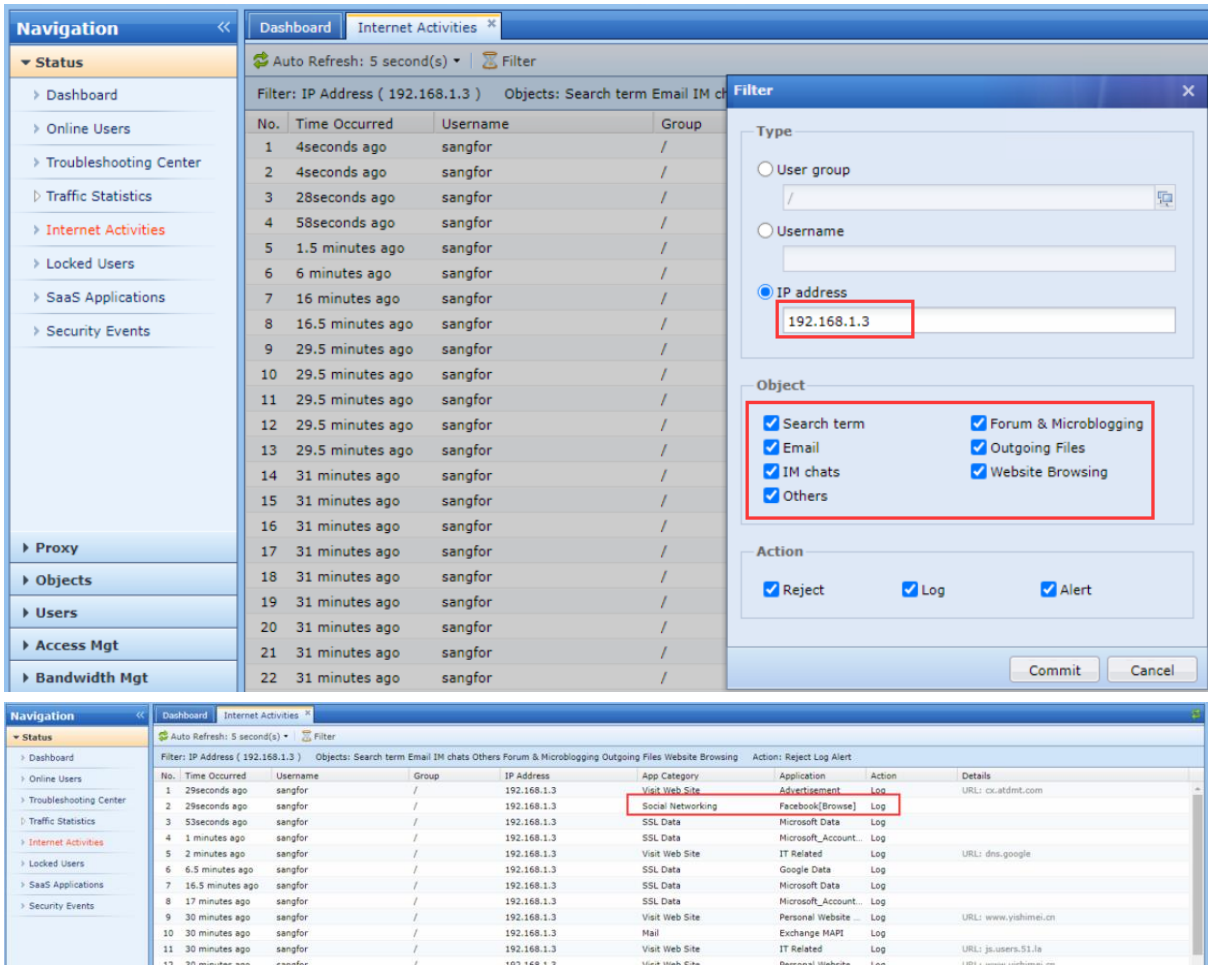




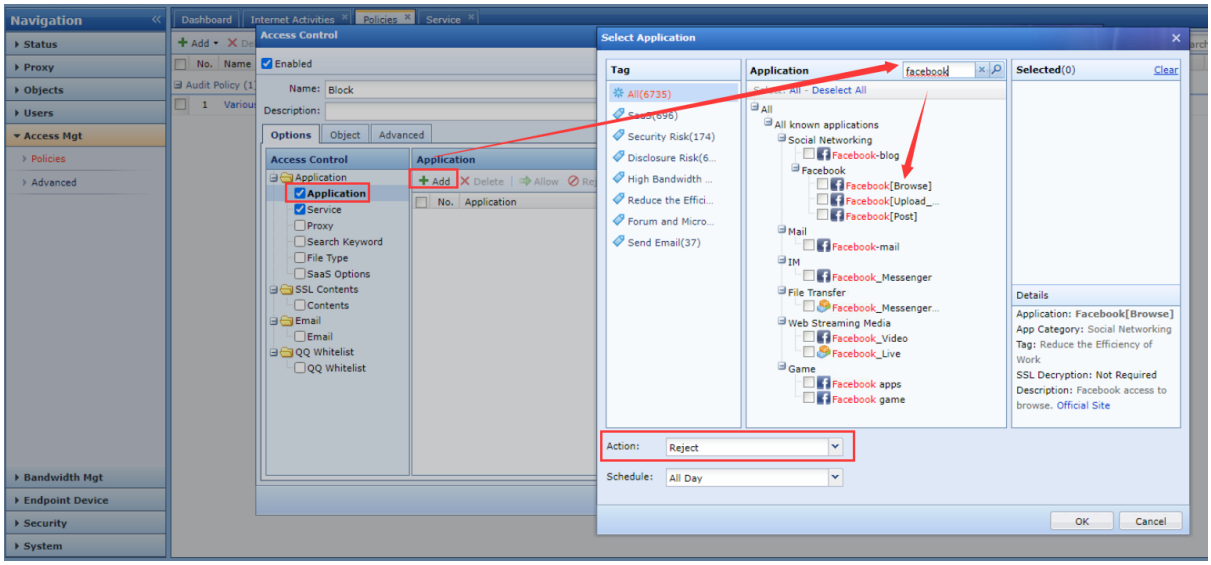
Chapter 3 Configuration

3.1 Block Facebook

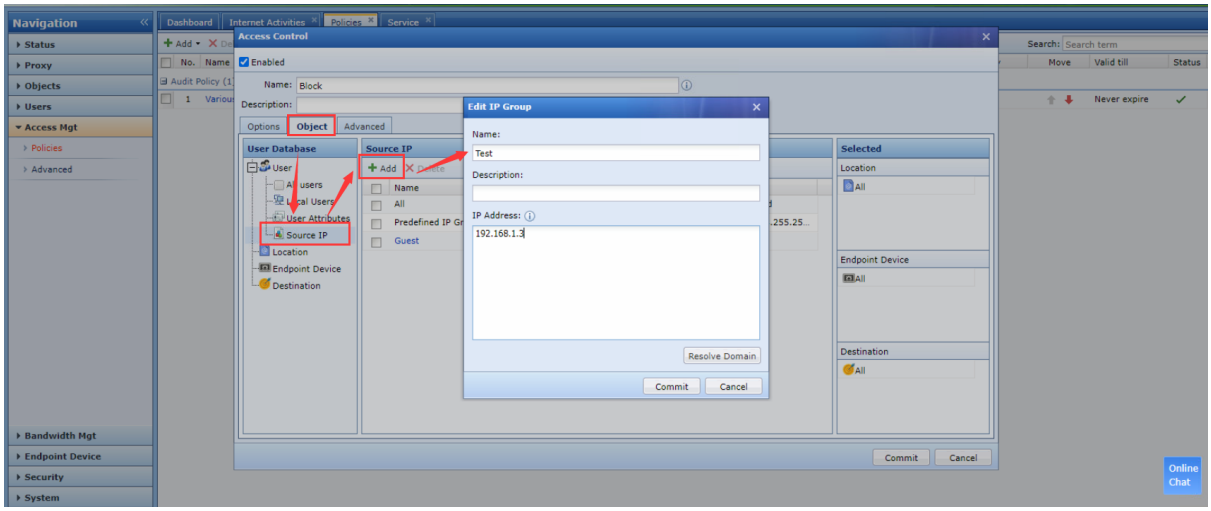
1. Use a browser to access facebook.com, and check which rules Facebook traffic has been recognized in Internet Activities.



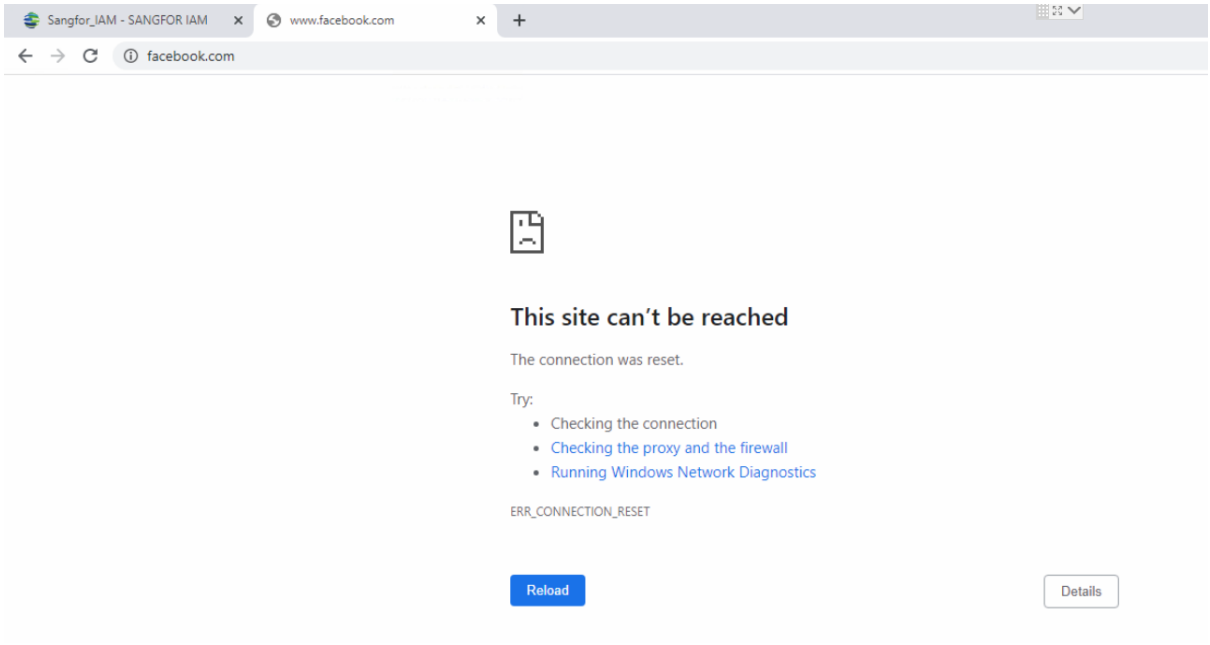
2. Add the corresponding Facebook[Broswe] rule in the application control policy, and select the action as reject.



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

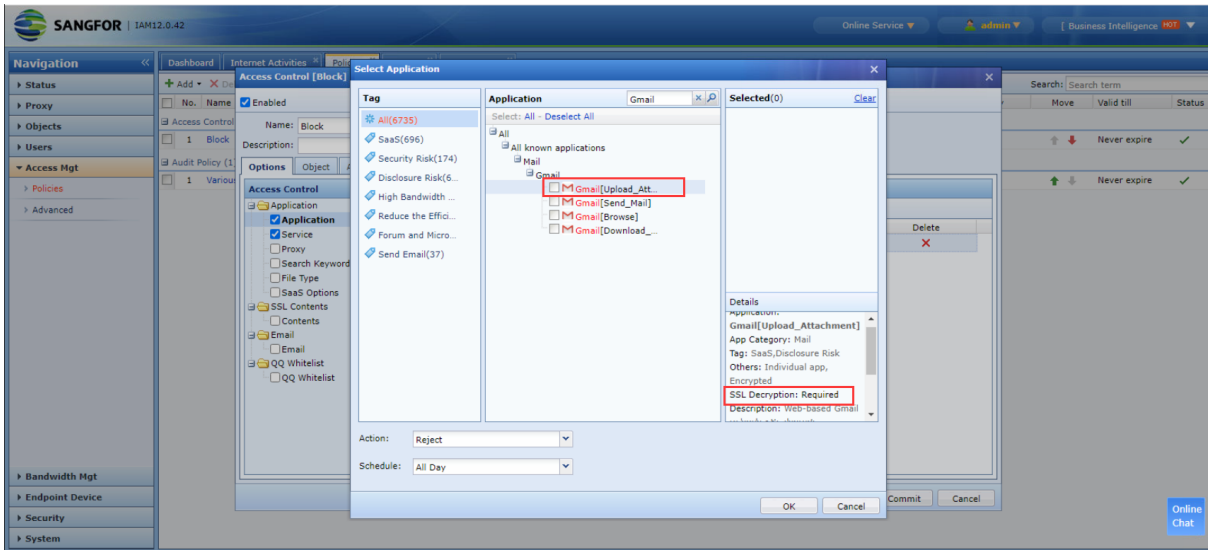


4. Access Facebook again, you can see that Facebook is no longer accessible.

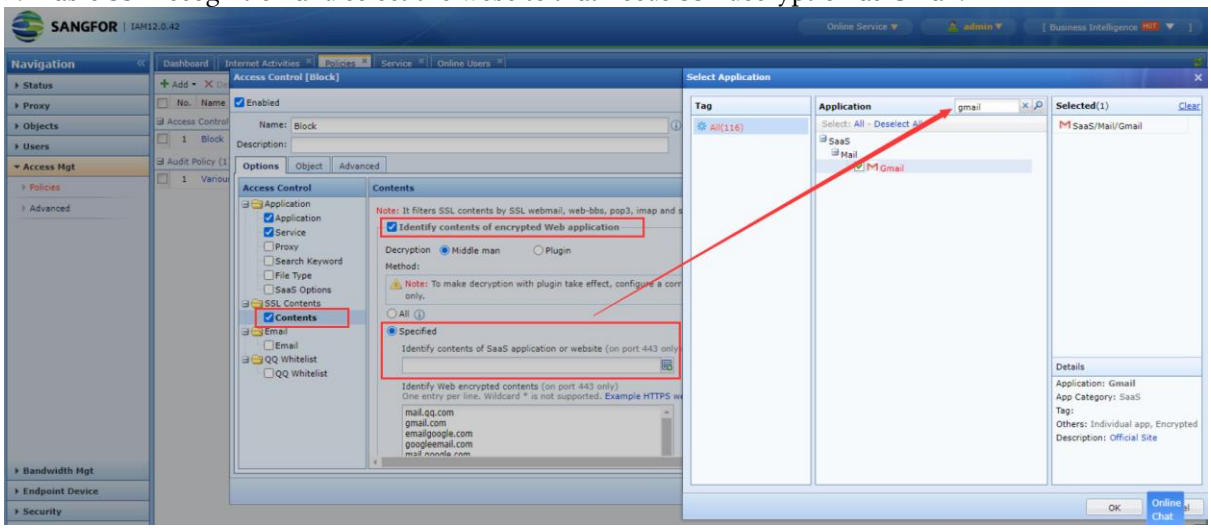


3.2 Block Gmail Outgoing Attachments

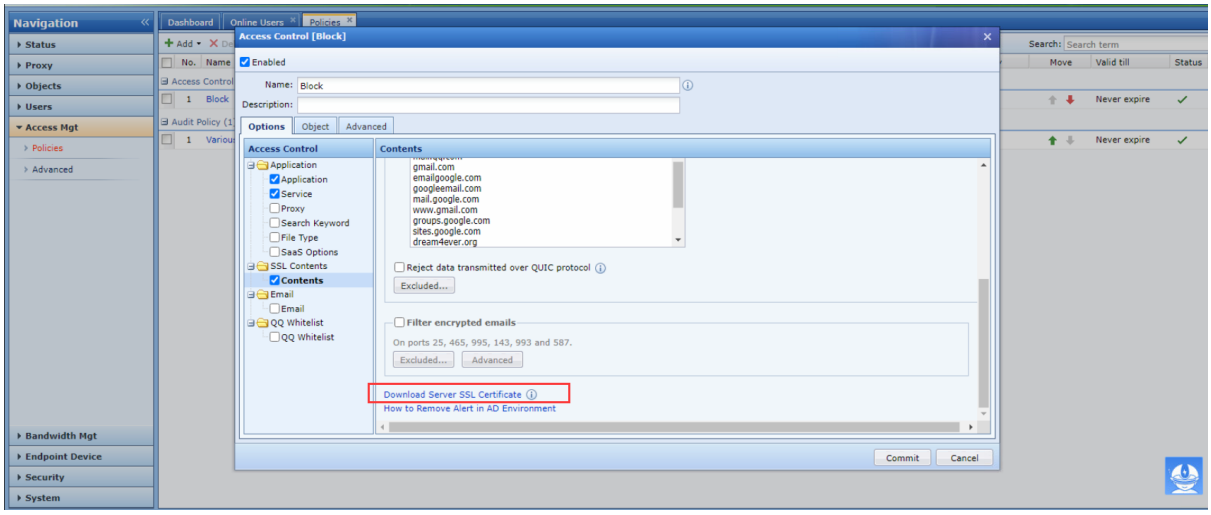
1. If you want to perform more detailed control on the behavior of the https website, such as allowing browsing but not uploading attachments, then you need to check the IAM rule description to determine whether you need to decrypt the traffic of the relevant domain name. For example, after querying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

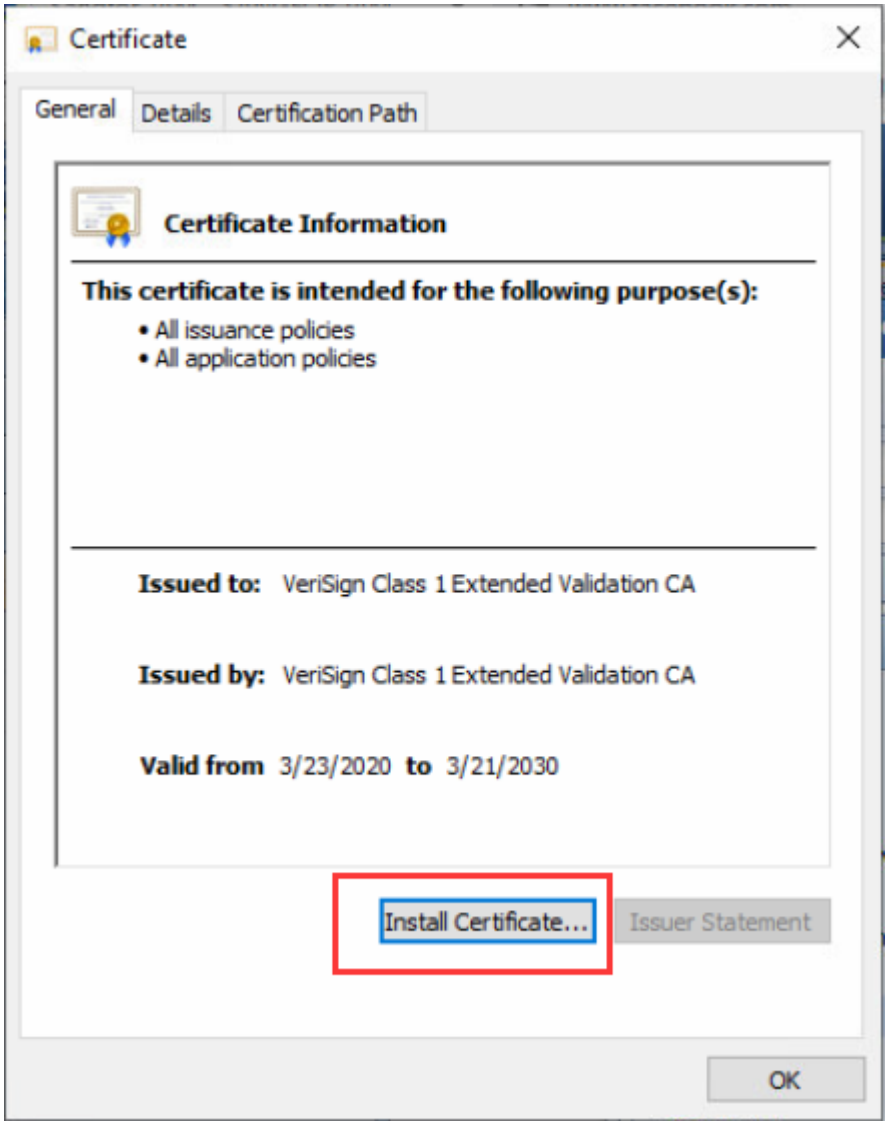


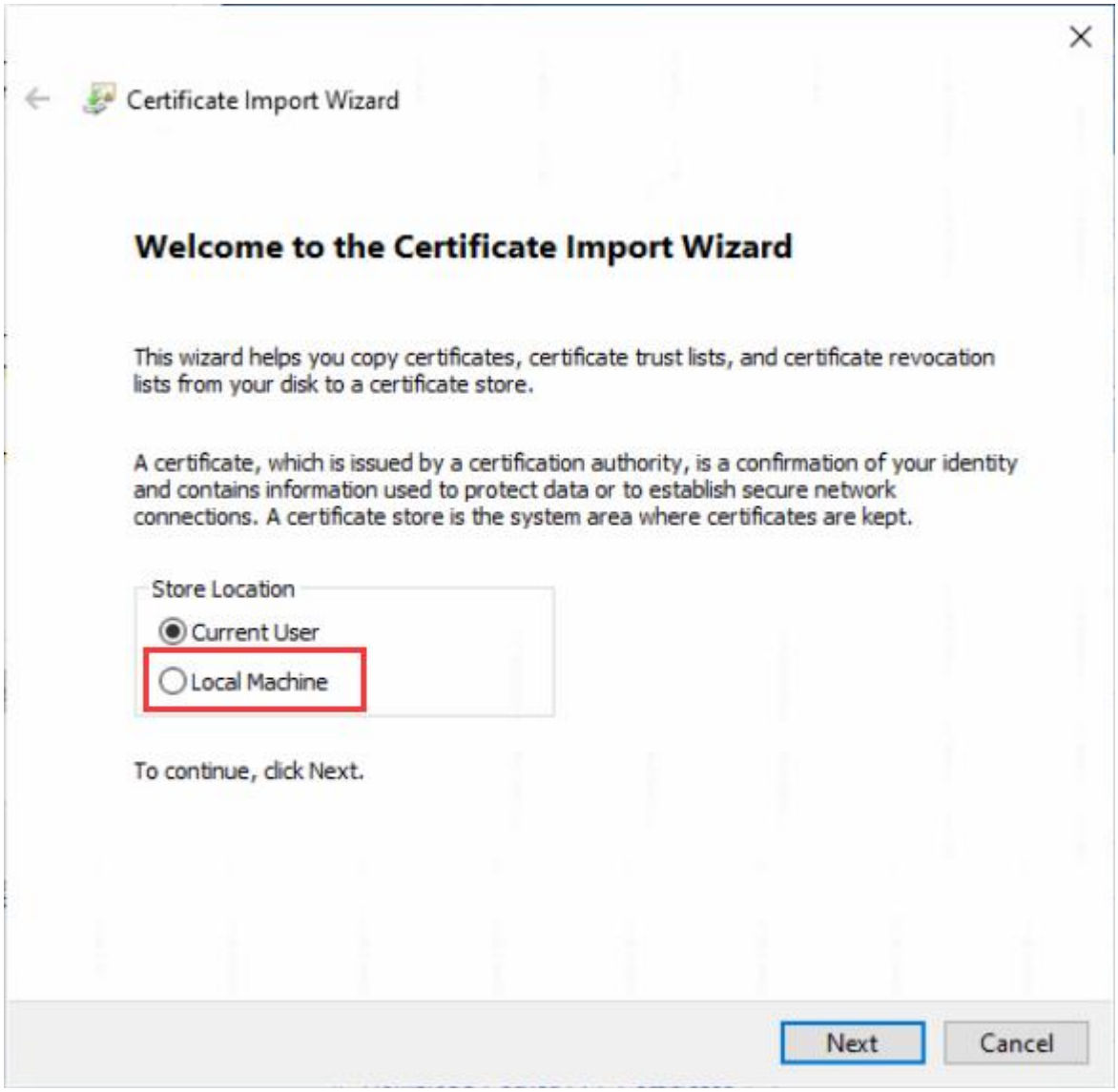
2.Enable SSL recognition and select the website that needs SSL decryption as Gmail.

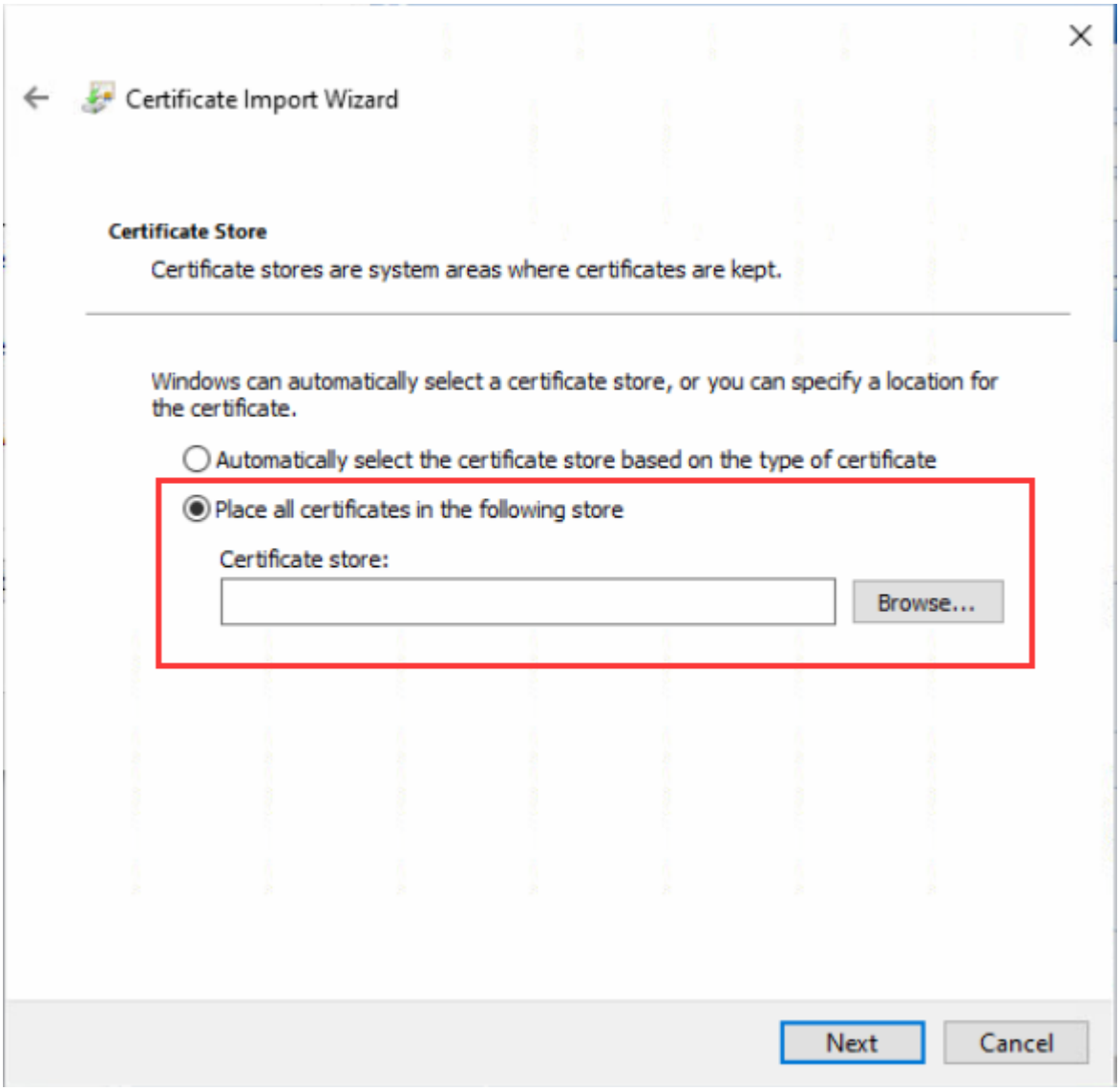


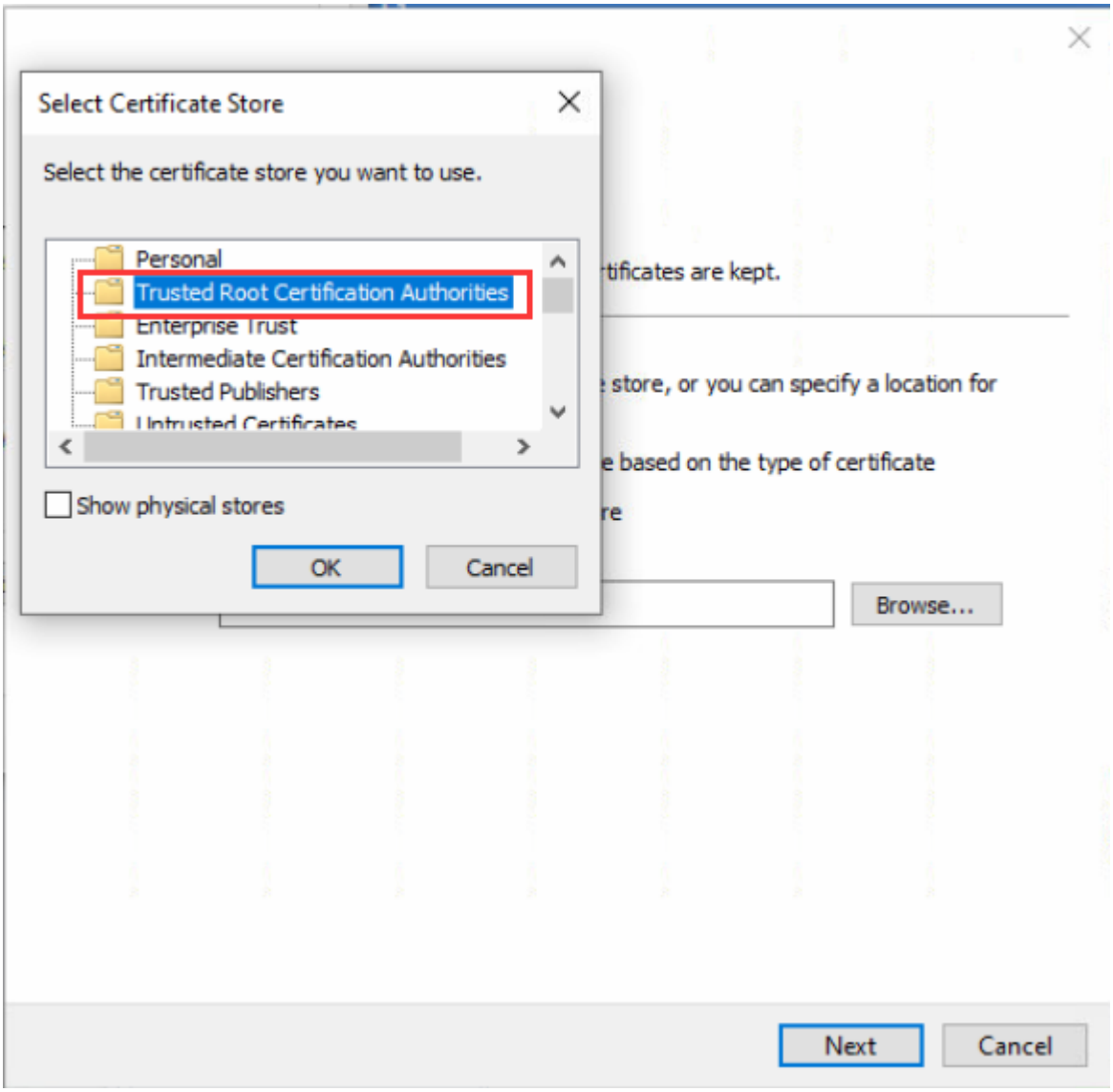
3. Download the root certificate recognized by SSL from the IAM device and import it into the system.

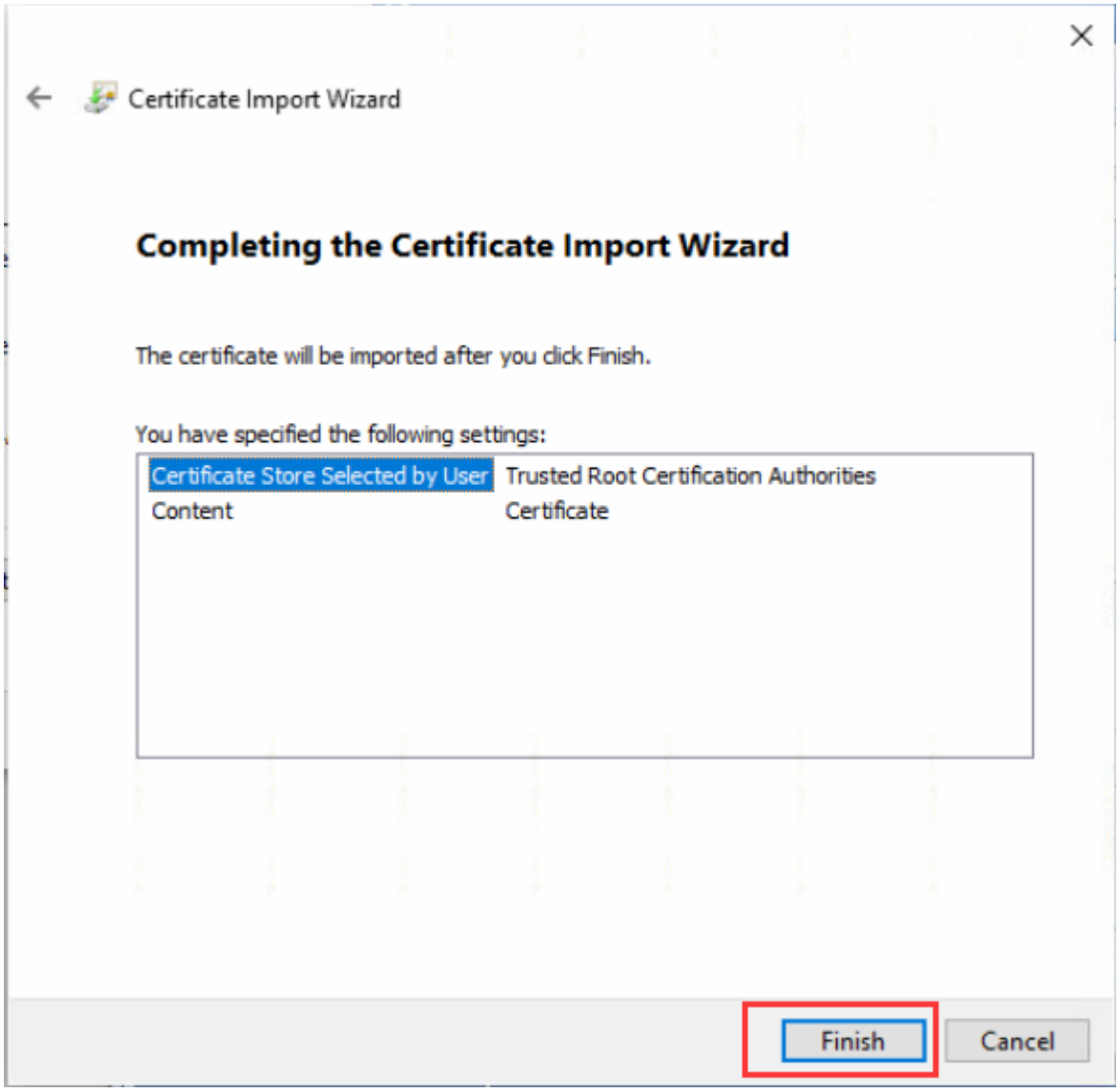



Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: VeriSign Class 1 Extended Validation CA
Issued by: VeriSign Class 1 Extended Validation CA
Valid from 3/23/2020 to 3/21/2030
Install Certificate...
Issuer Statement
OK

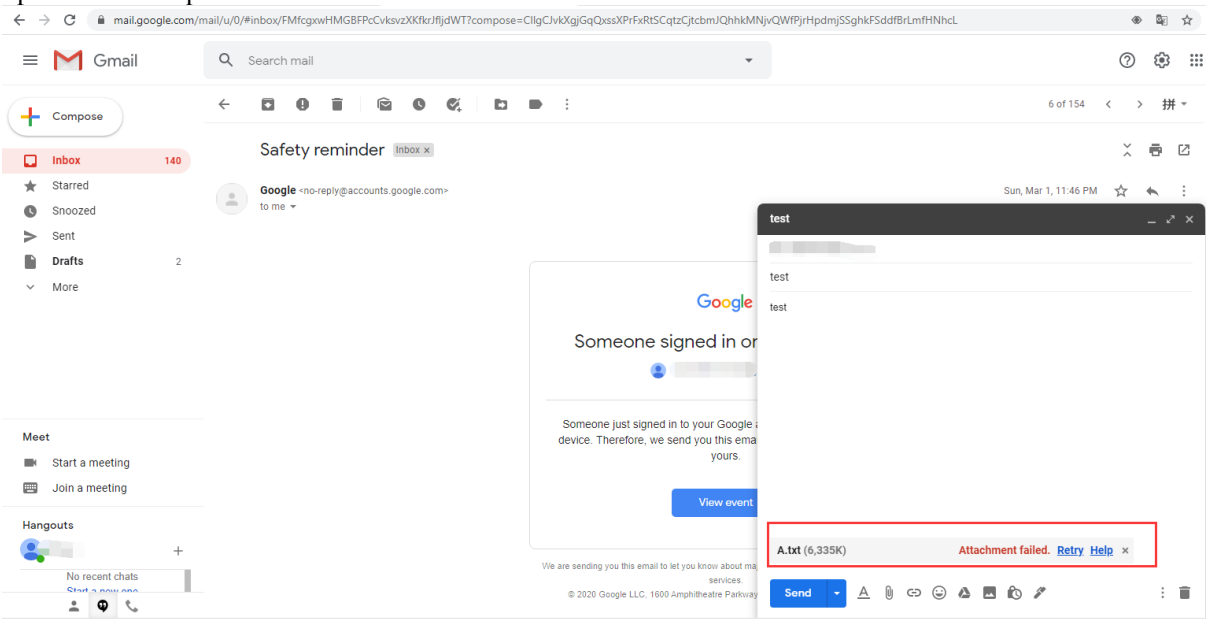

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

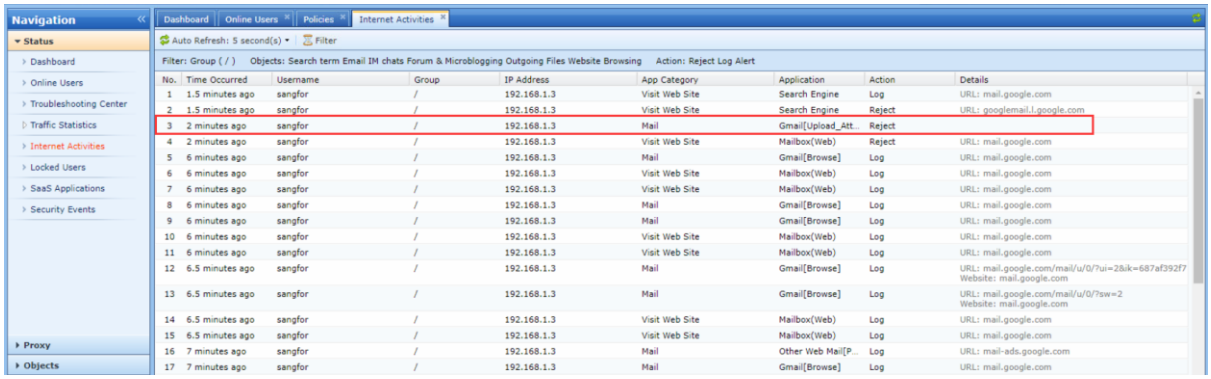

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Next
Cancel


Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Show physical stores
OK
Cancel
tificates are kept.
store, or you can specify a location for
e based on the type of certificate
re
Browse...
Next
Cancel



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





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.