IAM

Best Practices for Scenarios_ SSL Content Decryption

Version 12.0.42

Change Log

Date	Change Description
July 27, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

CONTENT

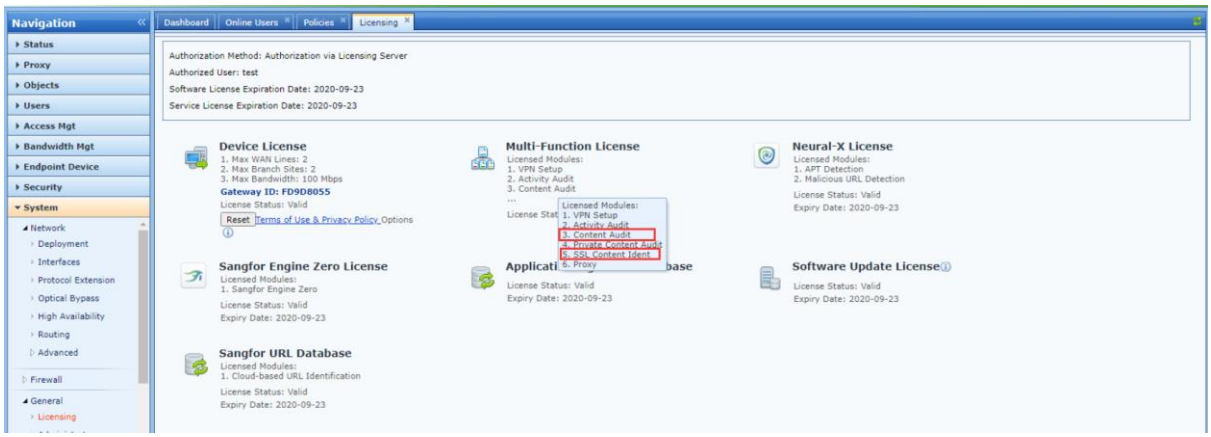
Chapter 1 Scenario 1
Chapter 2 Configuration 1

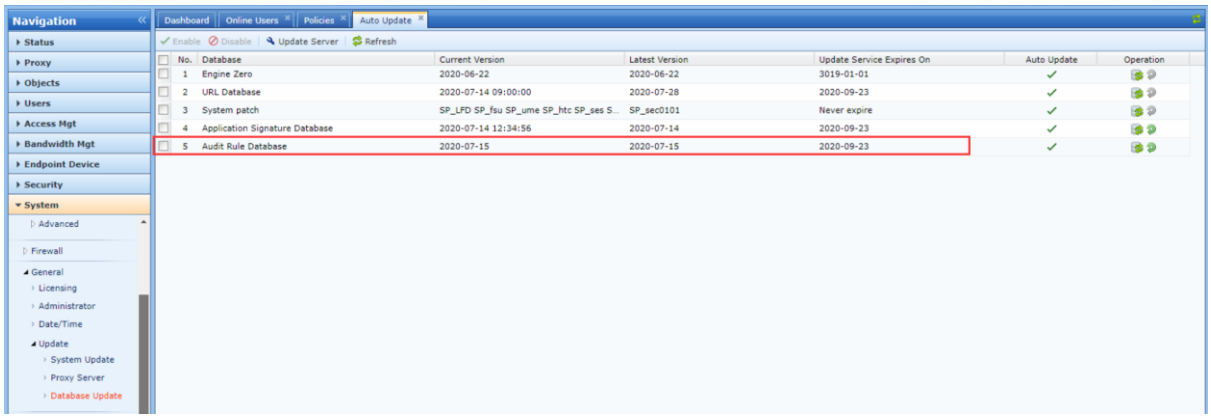
Chapter 1 Scenario

The R&D department of a software company needs to audit the content of emails sent by developers to avoid leakage of code information, so it wants to use IAM to audit users' encrypted content.

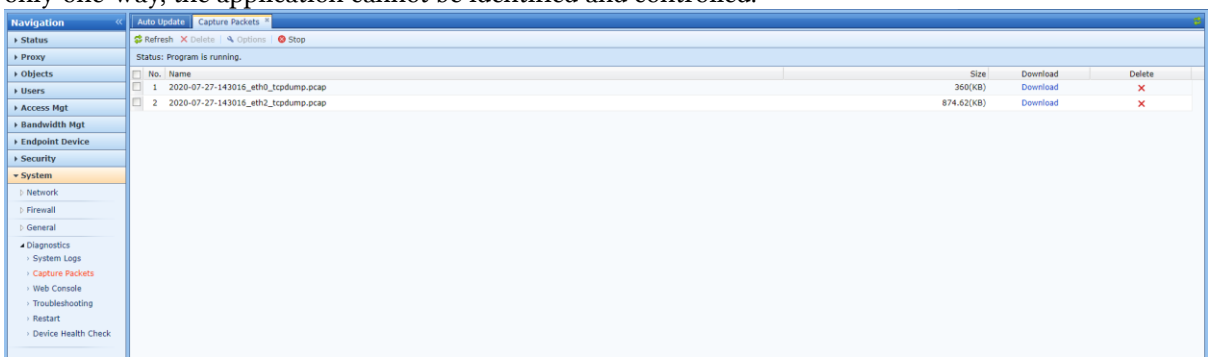
Chapter 2 Configuration

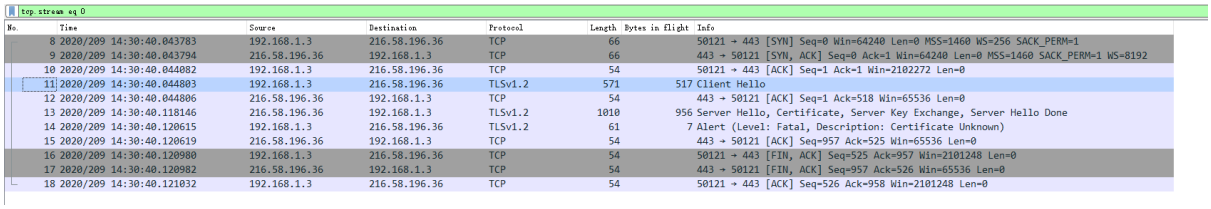
1. Check the authorization and rule base version to ensure that the Multi-Function License contains Content and SSL Content Ident



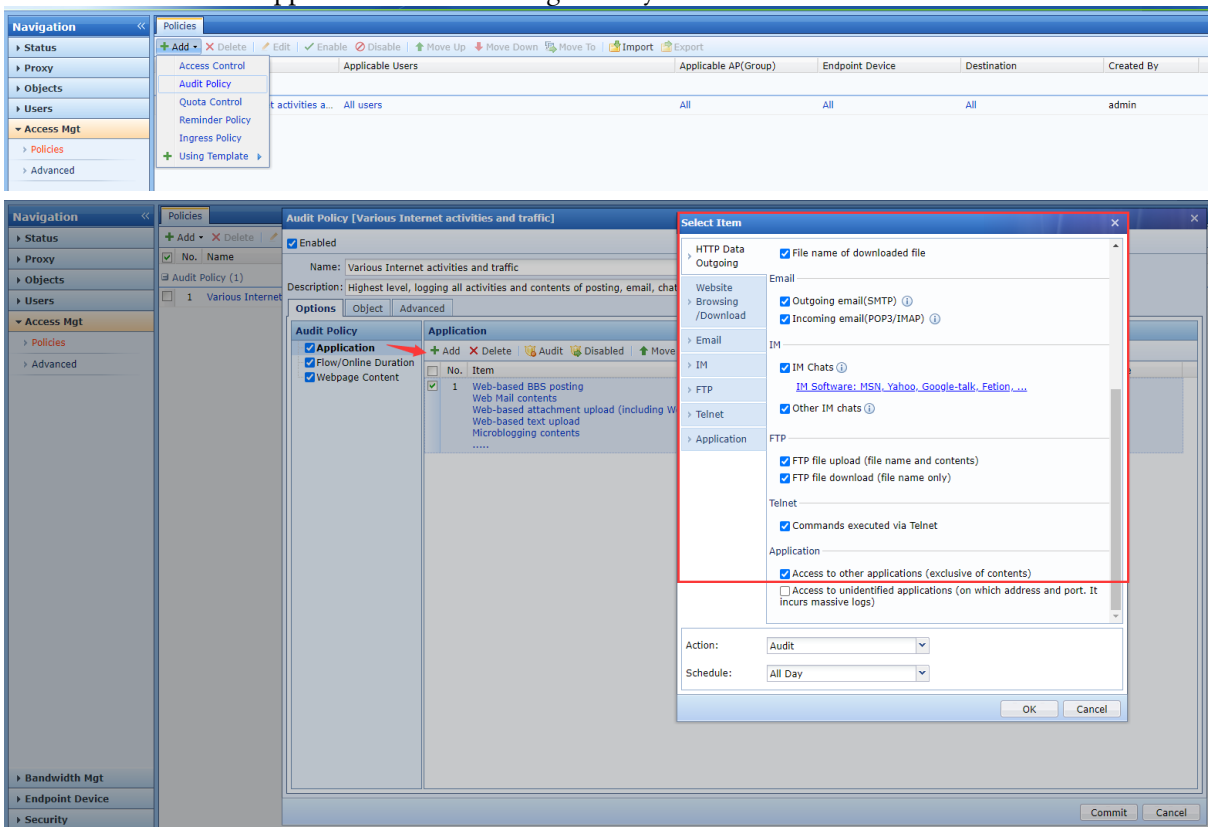


2. Make sure that the network traffic passes through the IAM device in both directions. If the traffic is only one-way, the application cannot be identified and controlled.

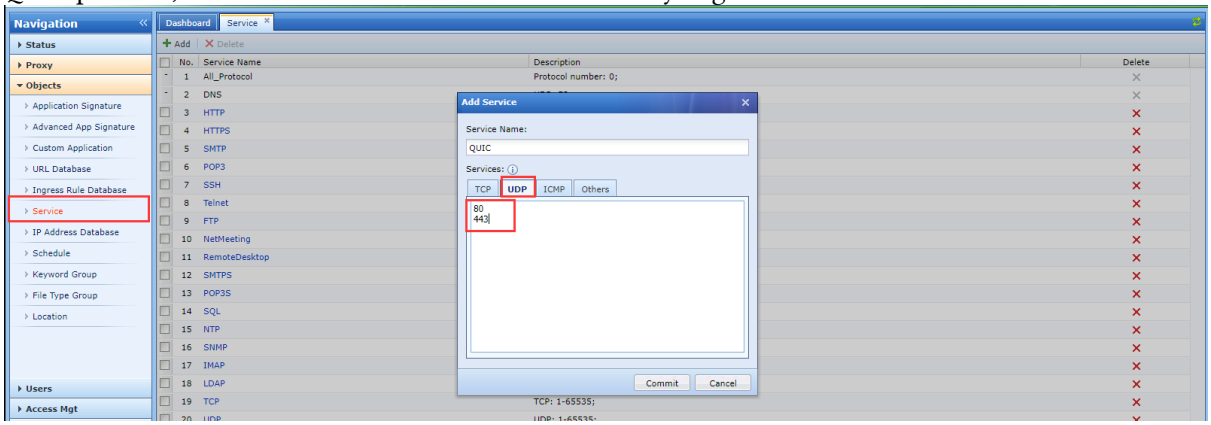


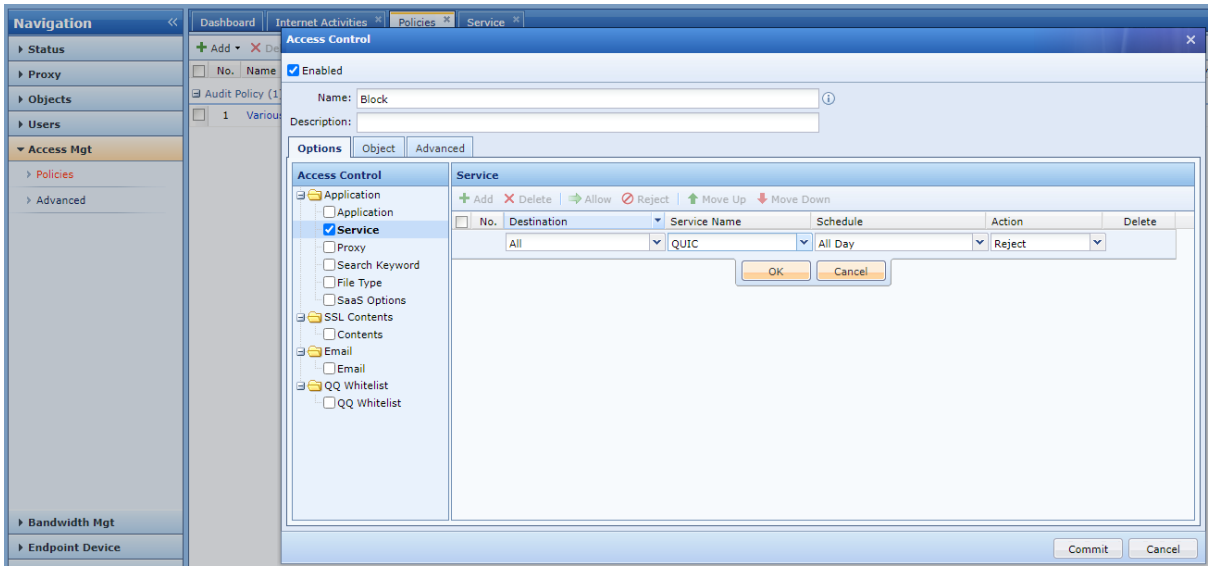


3. Configure the audit policy, because the application often contains multiple rules, it is necessary to check which rules the application traffic is recognized by the IAM database.

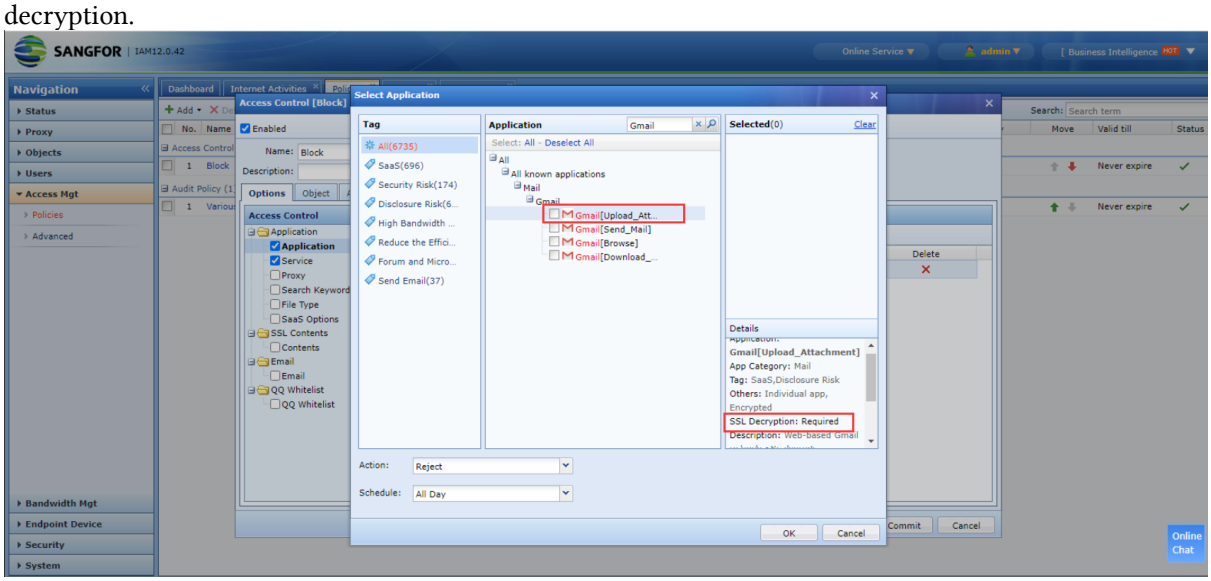


4. Now many websites and browsers use the QUIC protocol to transmit data, and the data encrypted by the QUIC protocol cannot be controlled, so the QUIC protocol needs to be disabled. After disabling the QUIC protocol, the website and browser will automatically negotiate the use of HTTPS to transmit data.

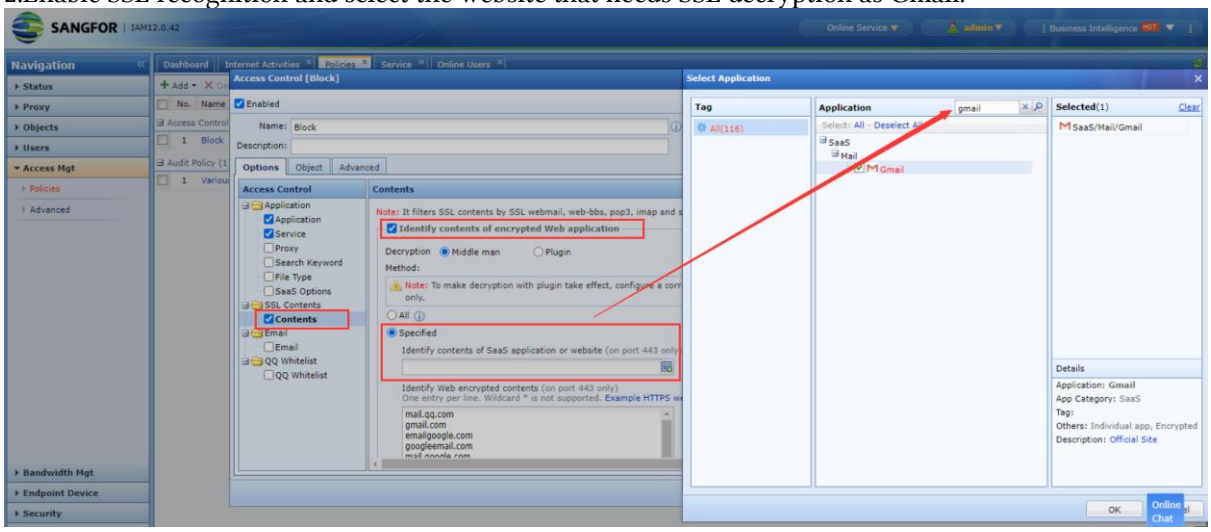




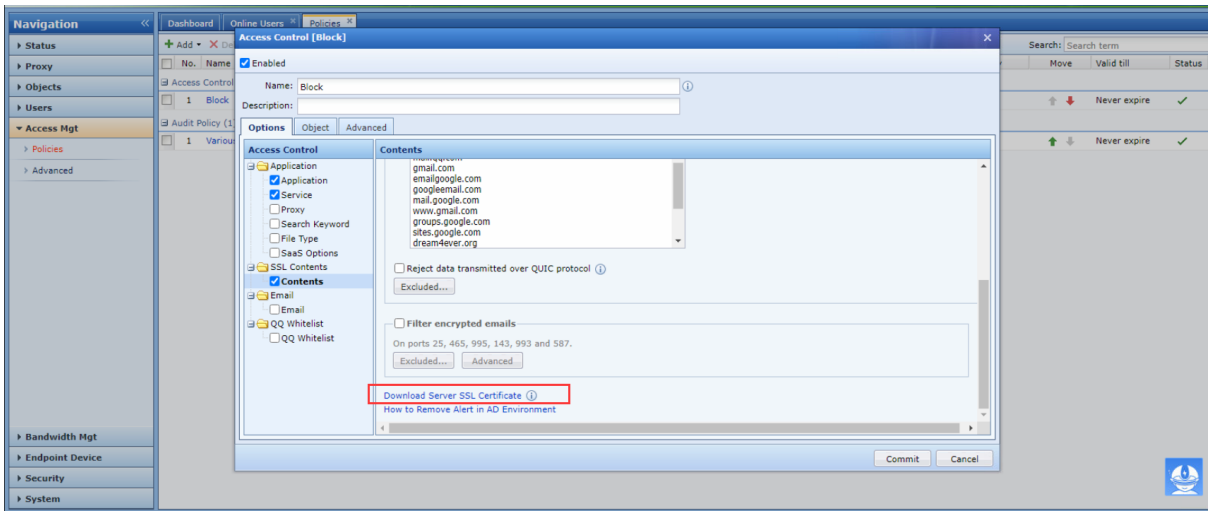
1. If you want to perform more detailed control over the behavior of the https website, such as allowing browsing but not uploading attachments, then you need to check the description of the database apps to determine whether you need to decrypt the relevant domain name. For example, after querying the description of the database, you can confirm that Gmail uploads attachments need to enable SSL data decryption.

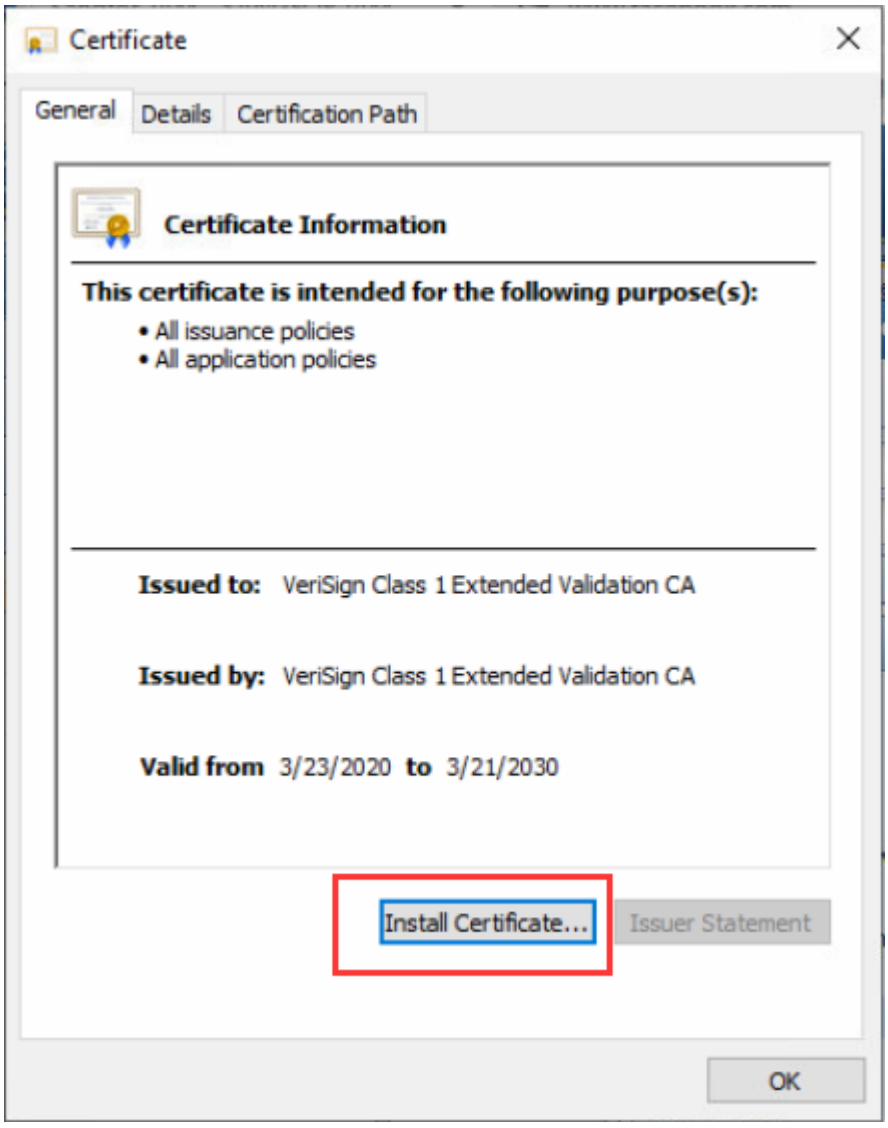


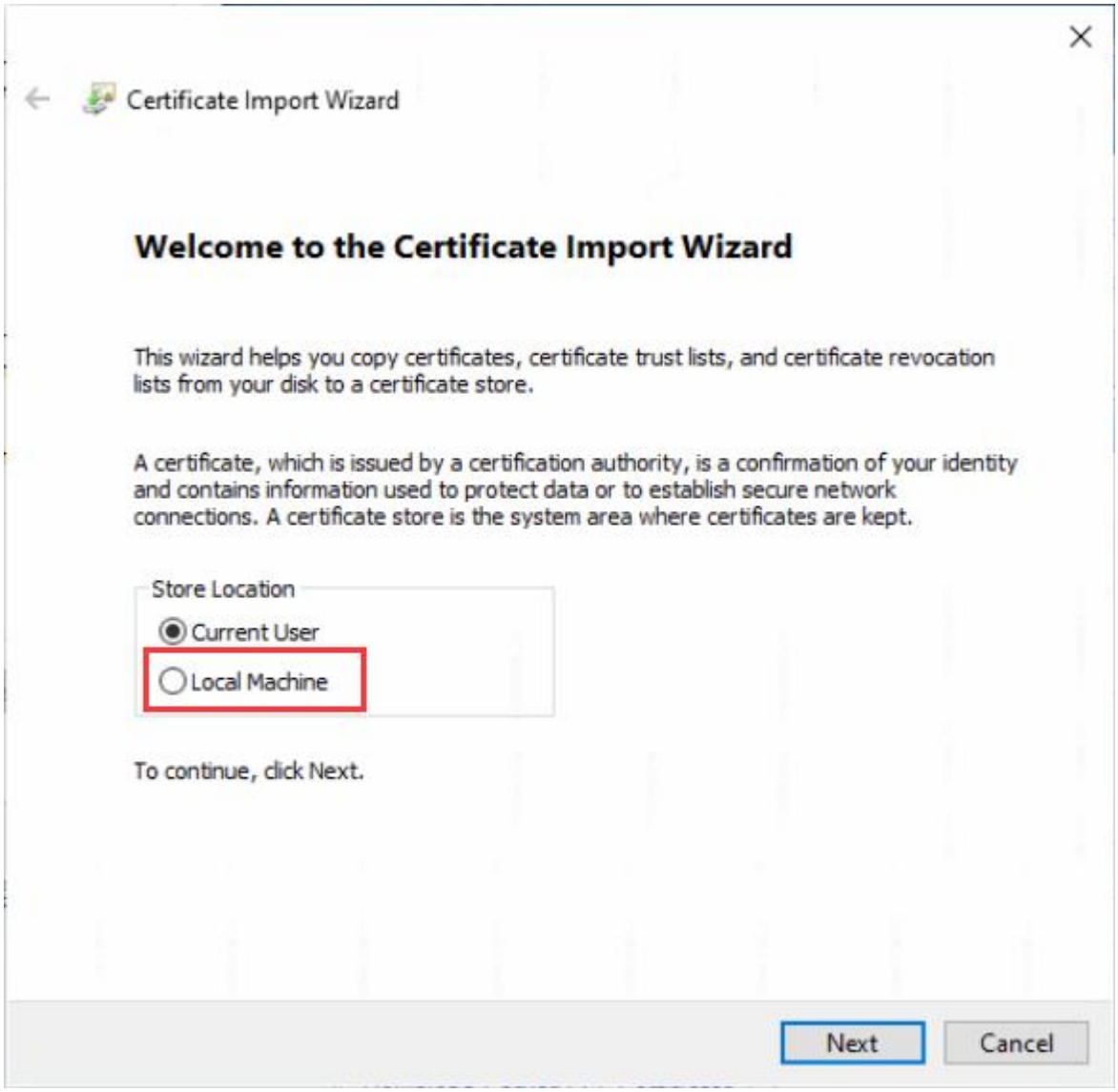
2.Enable SSL recognition and select the website that needs SSL decryption as Gmail.

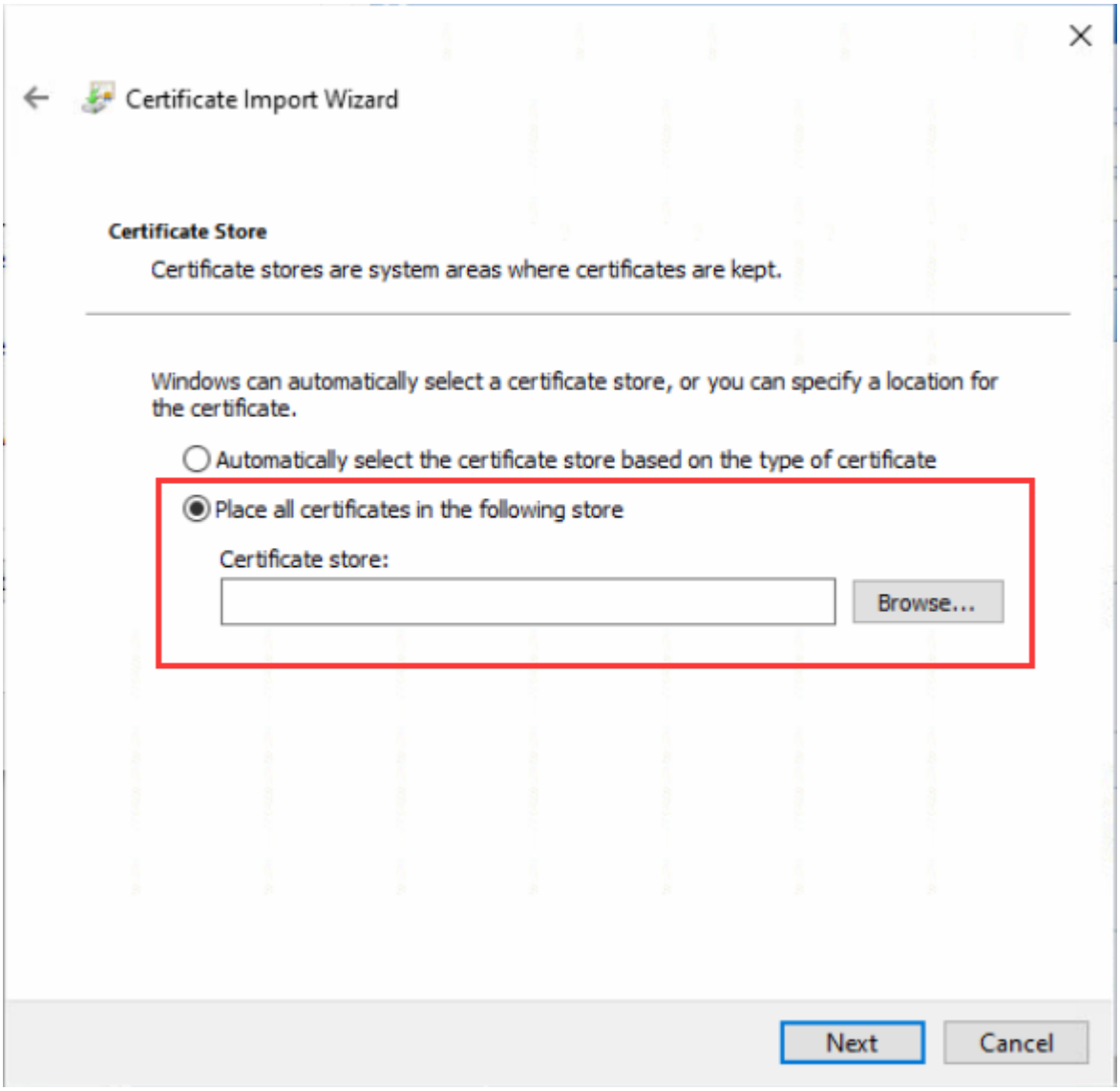


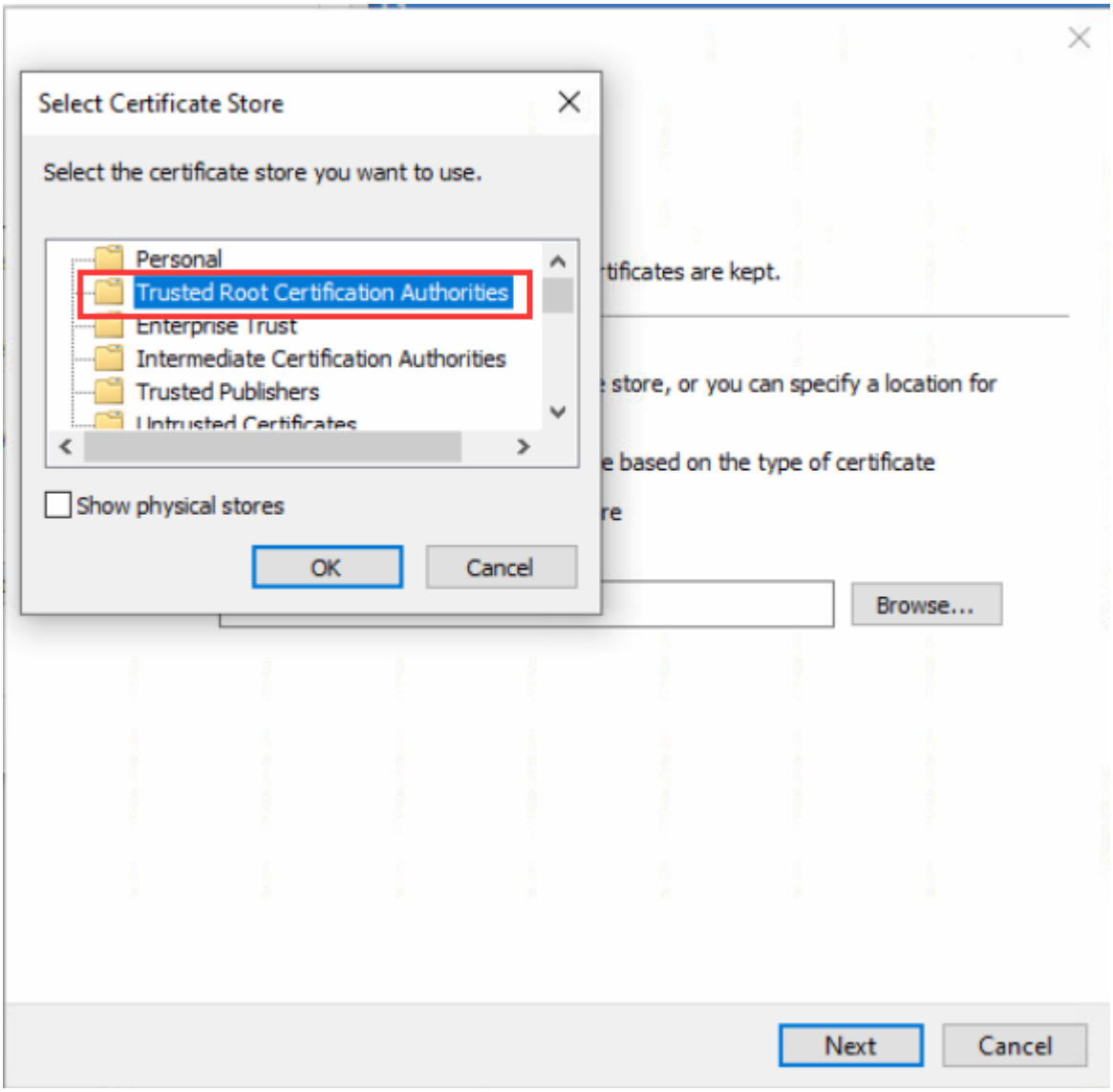
3. Download the root certificate recognized by SSL from the IAM device and import it into the system.

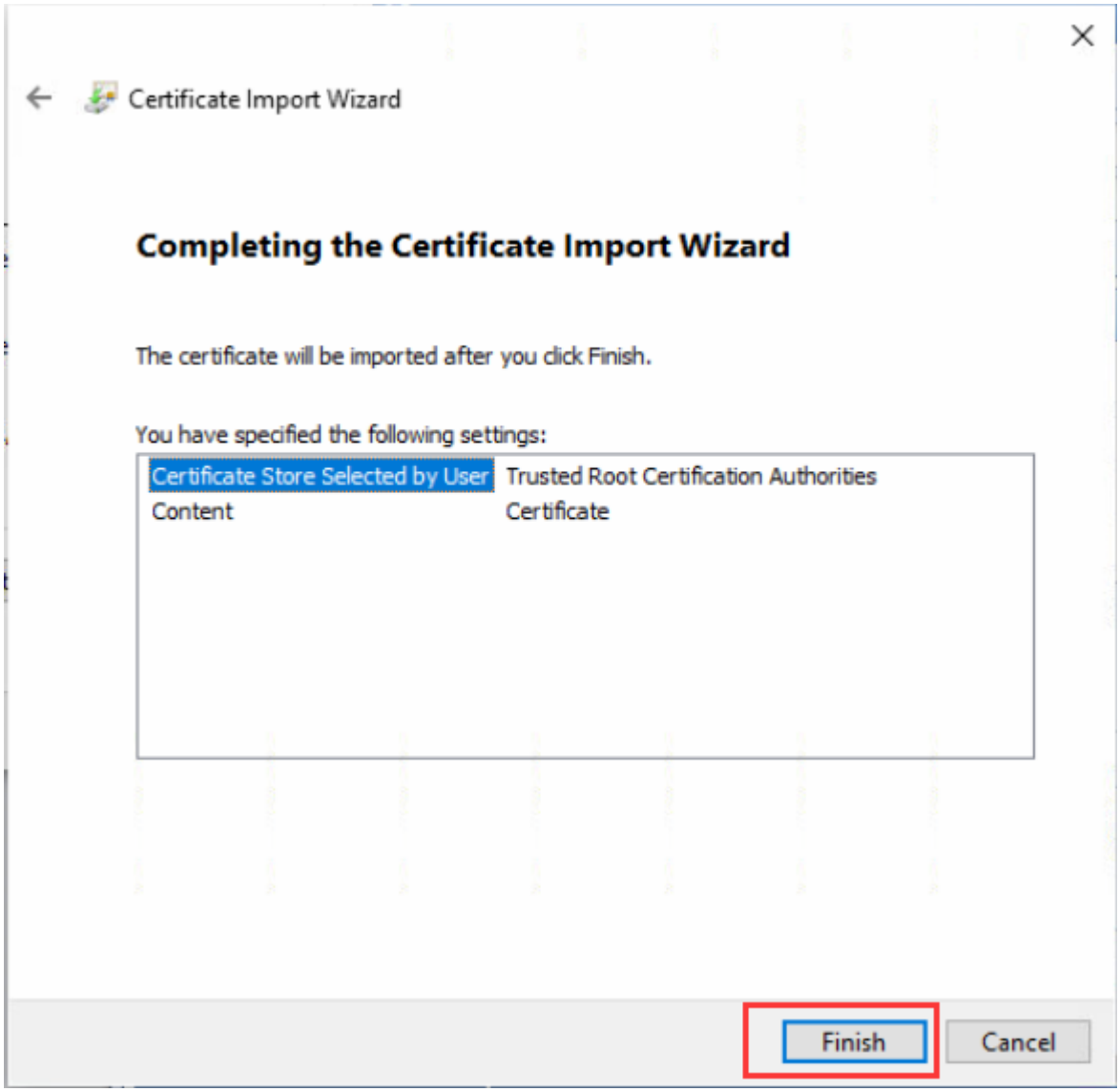




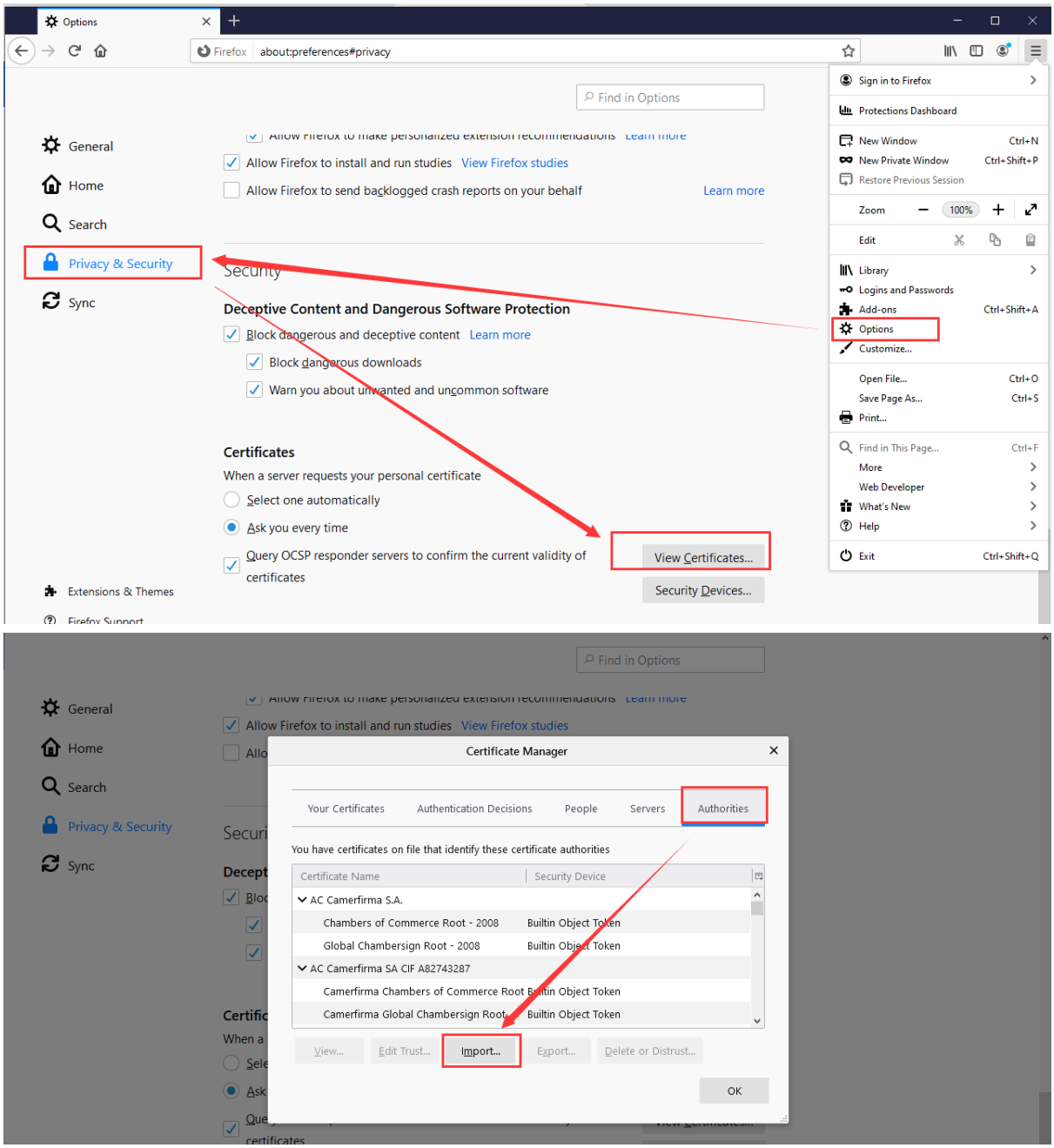

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity 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

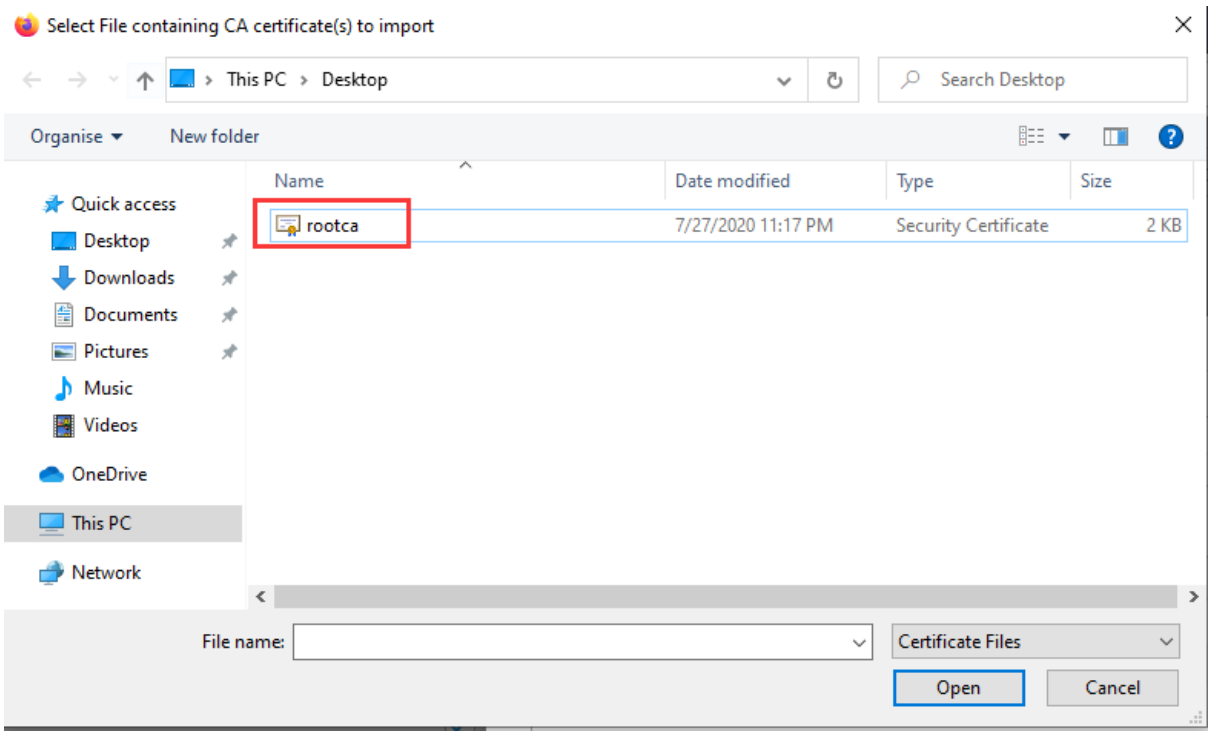

Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Show physical stores
OK
Cancel
tificates are kept.
store, or you can specify a location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

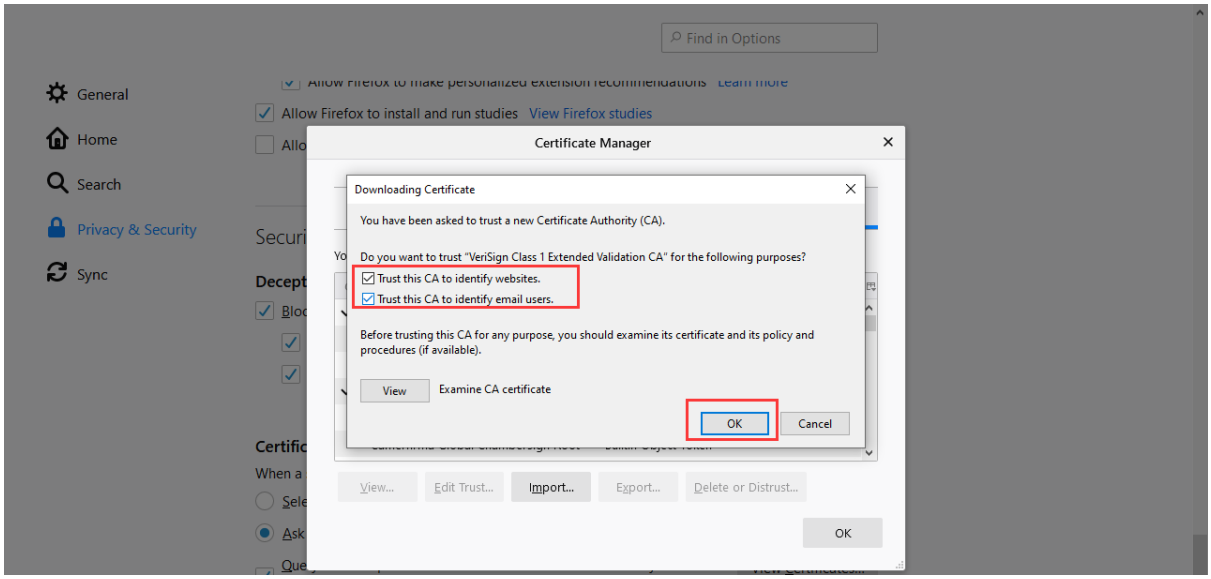


4. IE and Chrome call the built-in certificate of the Windows system, and the Firefox browser does not call the built-in certificate of the Windows system and needs to be imported separately.

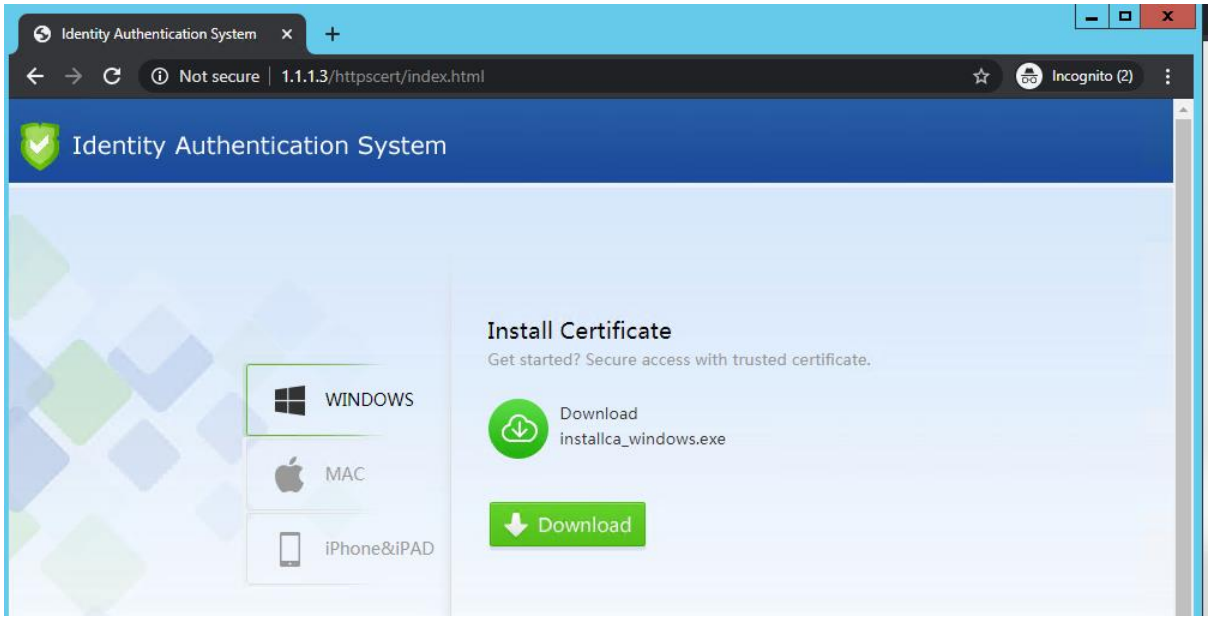

Options
Firefox about:preferences#privacy
Find in Options
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Allow Firefox to install and run studies View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf Learn more
Security
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
When a server requests your personal certificate
Select one automatically
Ask you every time
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
Sign in to Firefox
Protections Dashboard
New Window Ctrl+N
New Private Window Ctrl+Shift+P
Restore Previous Session
Zoom 100%
Edit
Library
Logins and Passwords
Add-ons Ctrl+Shift+A
Options
Customize...
Open File... Ctrl+O
Save Page As... Ctrl+S
Print...
Find in This Page... Ctrl+F
More
Web Developer
What's New
Help
Exit Ctrl+Shift+Q

Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce Root
Builtin Object Token
Camerfirma Global Chambersign Root
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK

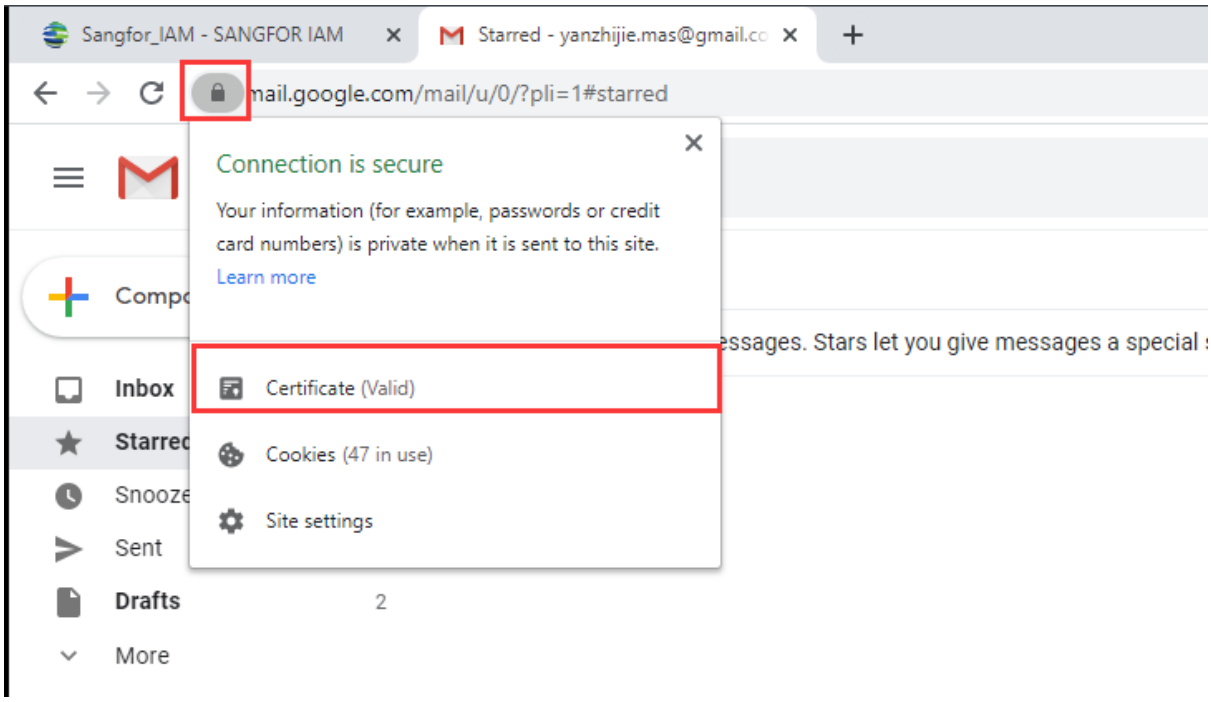


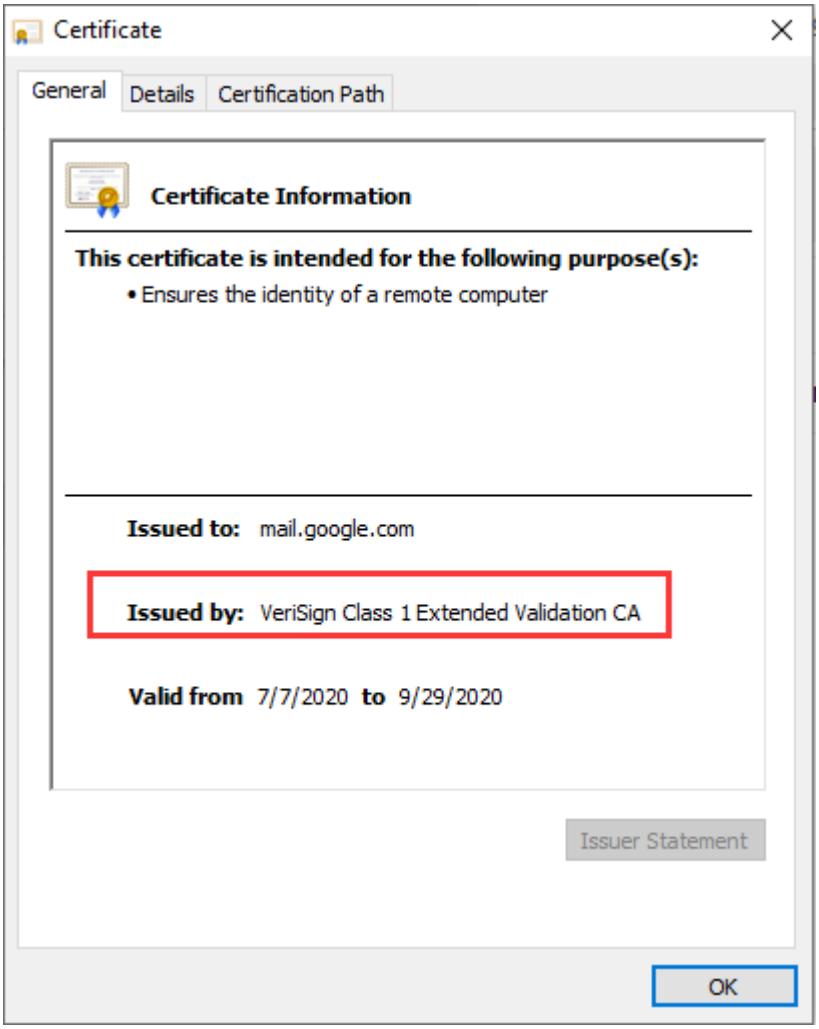


4. You may also use the cert installer download from IAM's link.
http://IAMip/httpscert/index.html IAM's ip is any IAM ip that can connect from PC to IAM.
For example: http://1.1.1.3/httpscert/index.html

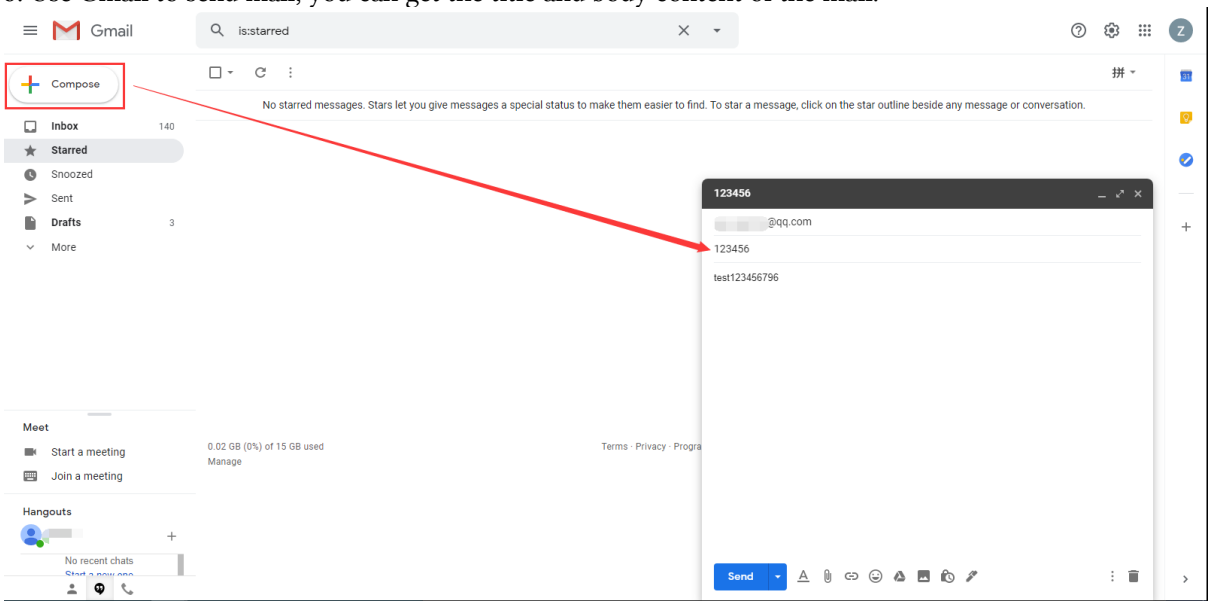


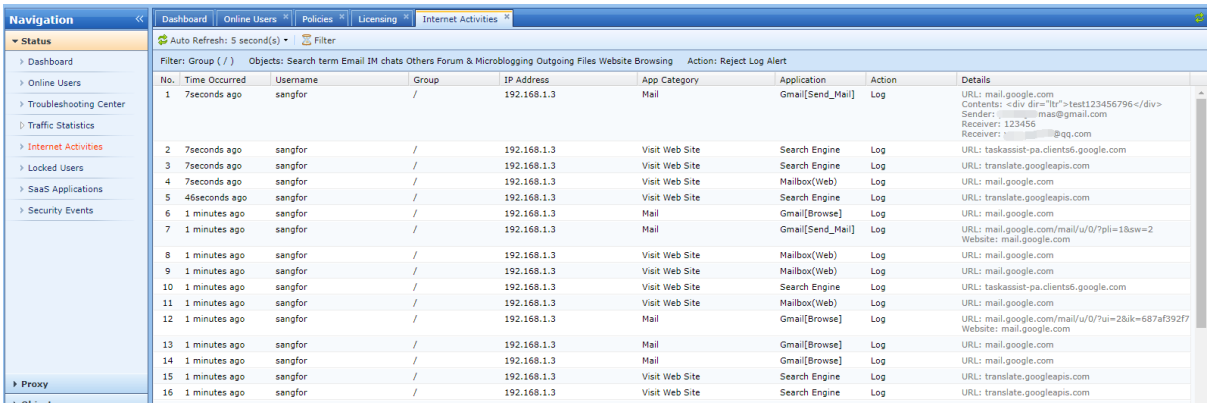
5. Check whether the certificate used to access the website is "VeriSign Class 1 Extended Validation CA", if it is, it means that the SSL decryption is successful.





5. Use Gmail to send mail, you can get the title and body content of the mail.




Navigation
Status
Dashboard
Online Users
Troubleshooting Center
Traffic Statistics
Internet Activities
Locked Users
SaaS Applications
Security Events
Proxy
Dashboard
Online Users
Policies
Licensing
Internet Activities
Auto Refresh: 5 second(s)
Filter
Filter: Group (/)
Objects: Search term Email IM chats Others Forum & Microblogging Outgoing Files Website Browsing
Action: Reject Log Alert
No. Time Occurred Username Group IP Address App Category Application Action Details
1 7seconds ago sangfor / 192.168.1.3 Mail Gmail[Send_Mail] Log URL: mail.google.com Contents: test123456796 Sender: mas@gmail.com Receiver: 123456 Receiver: @qq.com
2 7seconds ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: taskassist-pa.clients6.google.com
3 7seconds ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: translate.googleapis.com
4 7seconds ago sangfor / 192.168.1.3 Visit Web Site Mailbox(Web) Log URL: mail.google.com
5 46seconds ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: translate.googleapis.com
6 1 minutes ago sangfor / 192.168.1.3 Mail Gmail[Browse] Log URL: mail.google.com
7 1 minutes ago sangfor / 192.168.1.3 Mail Gmail[Send_Mail] Log URL: mail.google.com/mail/u/0/?pli=1&sw=2 Website: mail.google.com
8 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Mailbox(Web) Log URL: mail.google.com
9 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Mailbox(Web) Log URL: mail.google.com
10 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: taskassist-pa.clients6.google.com
11 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Mailbox(Web) Log URL: mail.google.com
12 1 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 1 minutes ago sangfor / 192.168.1.3 Mail Gmail[Browse] Log URL: mail.google.com
14 1 minutes ago sangfor / 192.168.1.3 Mail Gmail[Browse] Log URL: mail.google.com
15 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: translate.googleapis.com
16 1 minutes ago sangfor / 192.168.1.3 Visit Web Site Search Engine Log URL: translate.googleapis.com