IAM

Implementasi yang Direkomendasikan untuk Skenario_ SSL Content Decryption

Versi 12.0.42

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Juli 27, 2020	Rilis Dokumen Versi 12.0.42.
Mei 17, 2021	Dokumen update Versi 12.0.42.

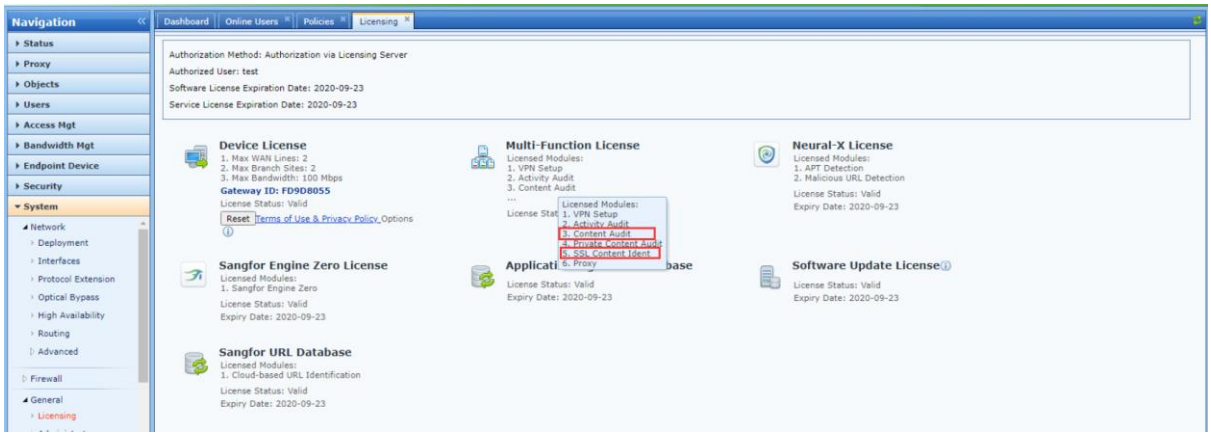
Daftar Isi

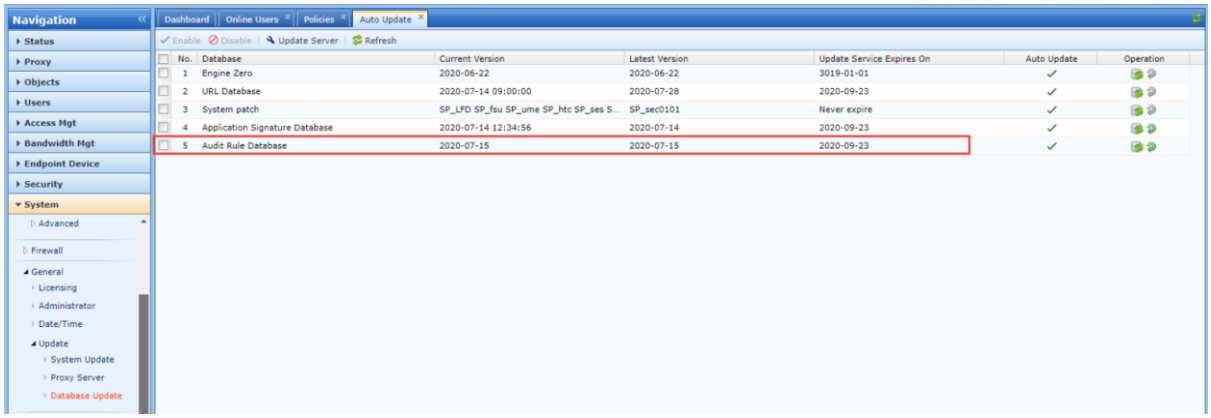
Bab 1 Skenario

Departemen R&D dari perusahaan perangkat lunak perlu audit content email yang dikirim oleh developer untuk menghindari kebocoran informasi kode, jadi hendak menggunakan IAM untuk audit content terenkripsi pengguna.

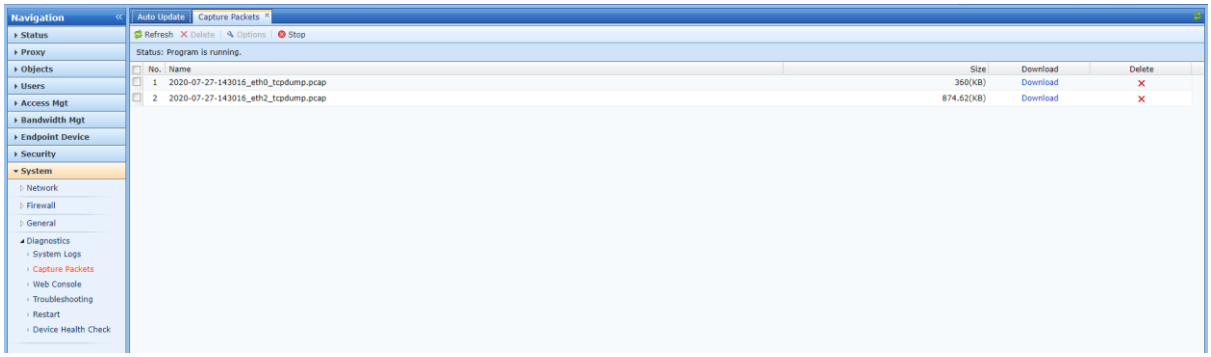
Bab 2 Konfigurasi

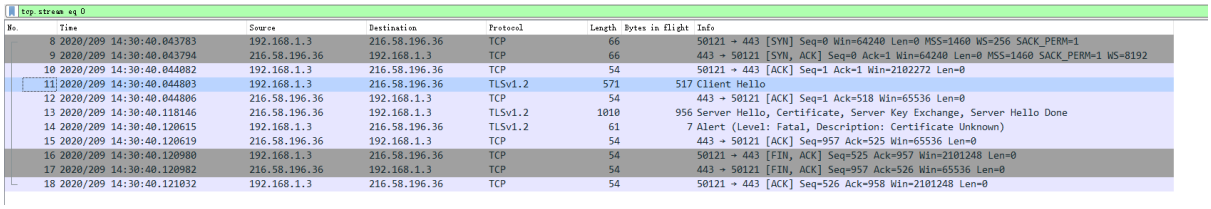
1. Periksa authorization dan rule basis versi untuk memastikan bahwa Multi-Function License berisi Content dan SSL Content Ident



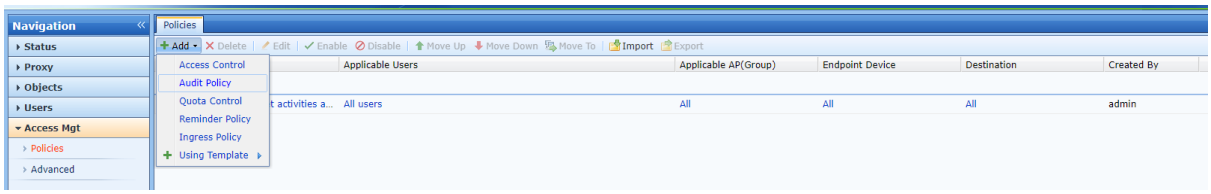


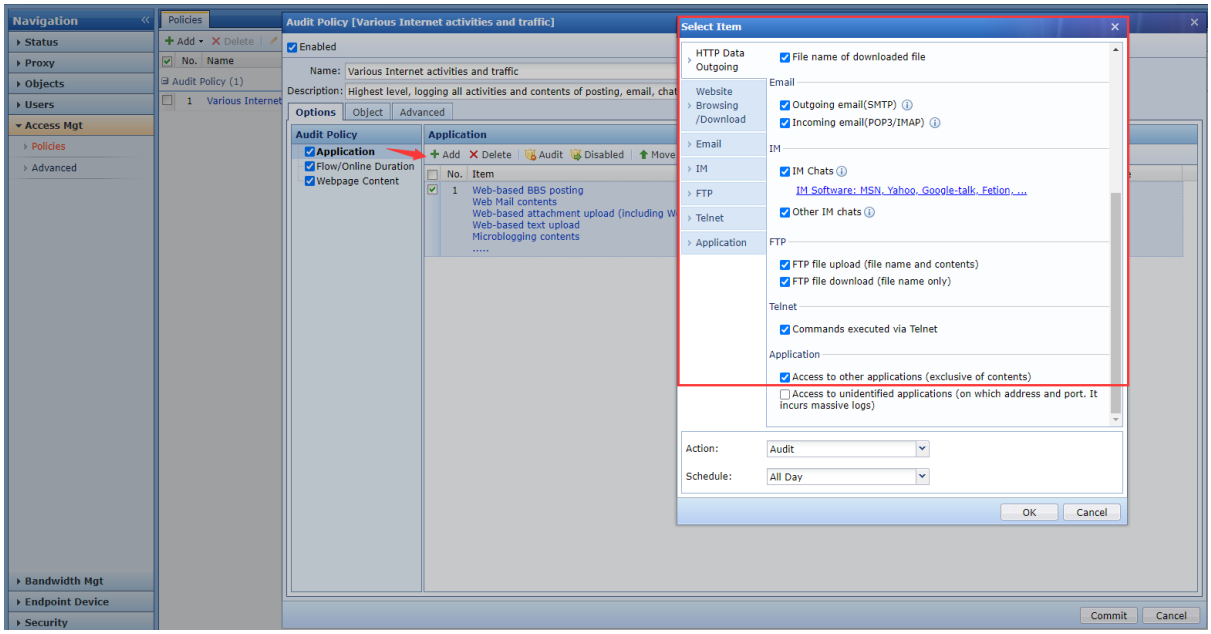
2. Pastikan bahwa traffic network melewati perangkat IAM di kedua arah. Jika traffic hanya satu arah, aplikasi tidak dapat diidentifikasi dan dikontrol.



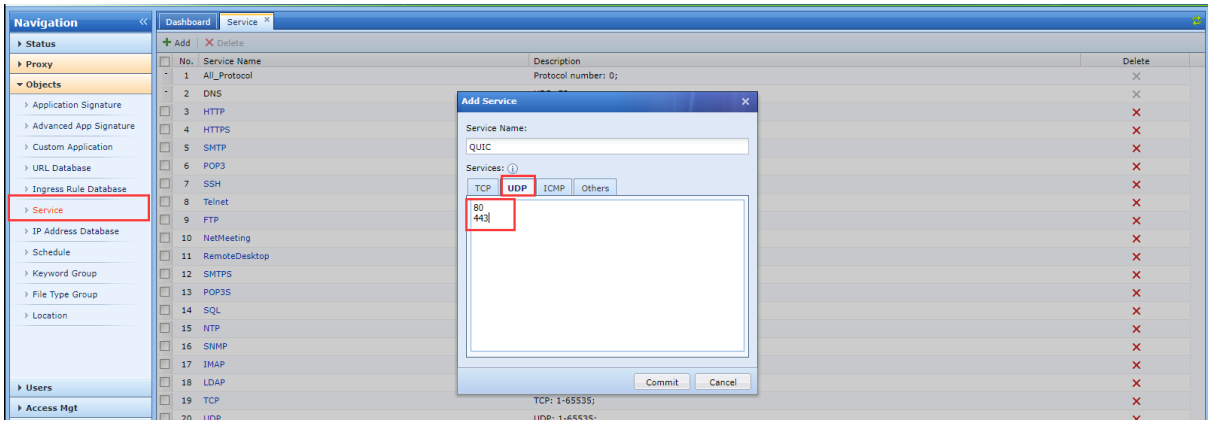


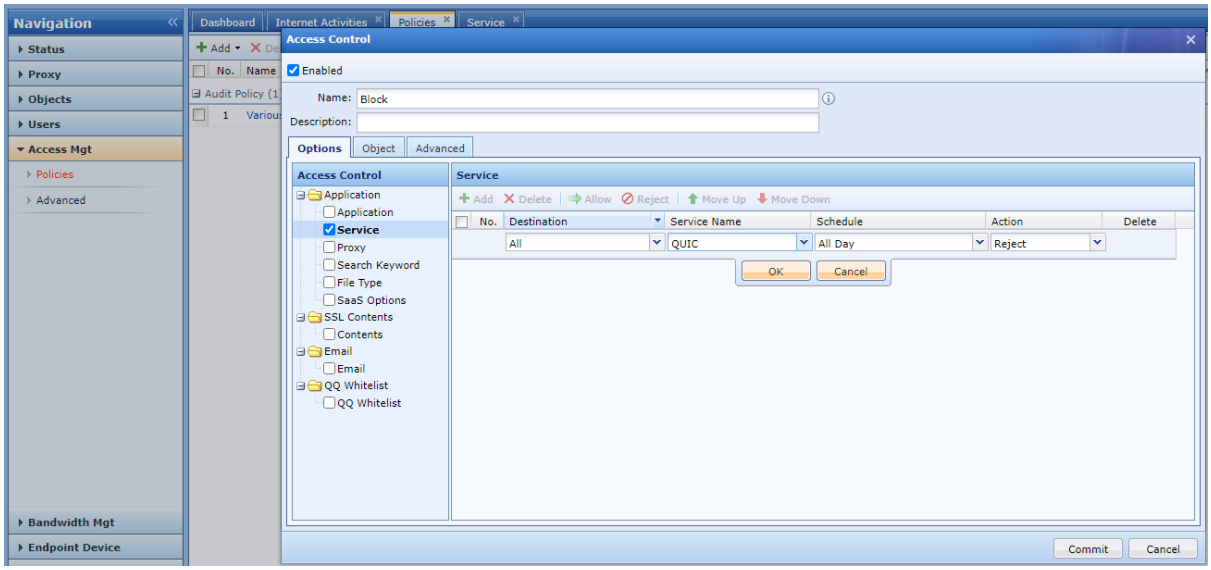
3. Konfigurasi audit policy, karena aplikasi sering berisi multiple rules, perlu untuk memeriksa rule aplikasi mana yang dikenali oleh IAM database.



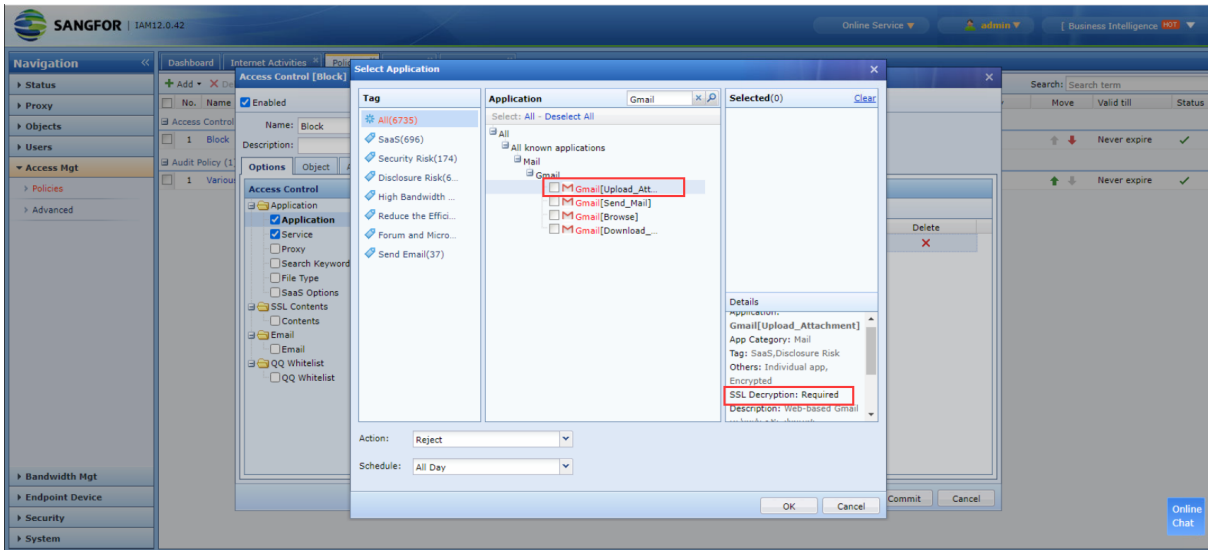


4. Sekarang banyak website dan browser menggunakan protokol QUIC untuk mengirimkan data, dan data yang dienkripsi oleh protokol QUIC tidak dapat dikontrol, jadi protokol QUIC perlu dinonaktifkan. Setelah nonaktifkan protokol QUIC, website dan browser akan secara otomatis negosiasi penggunaan HTTPS untuk mengirimkan data.

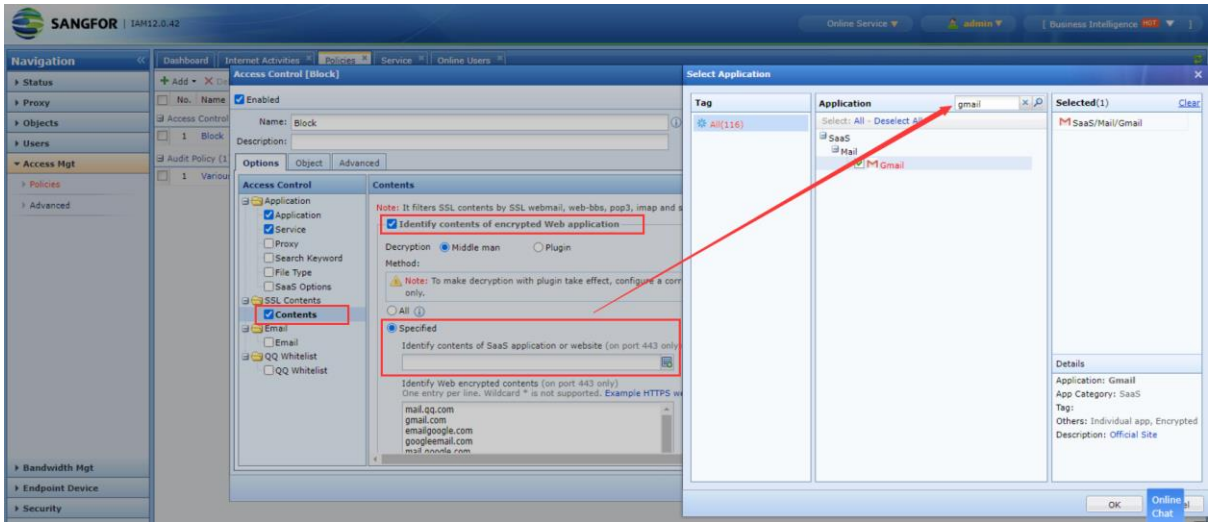




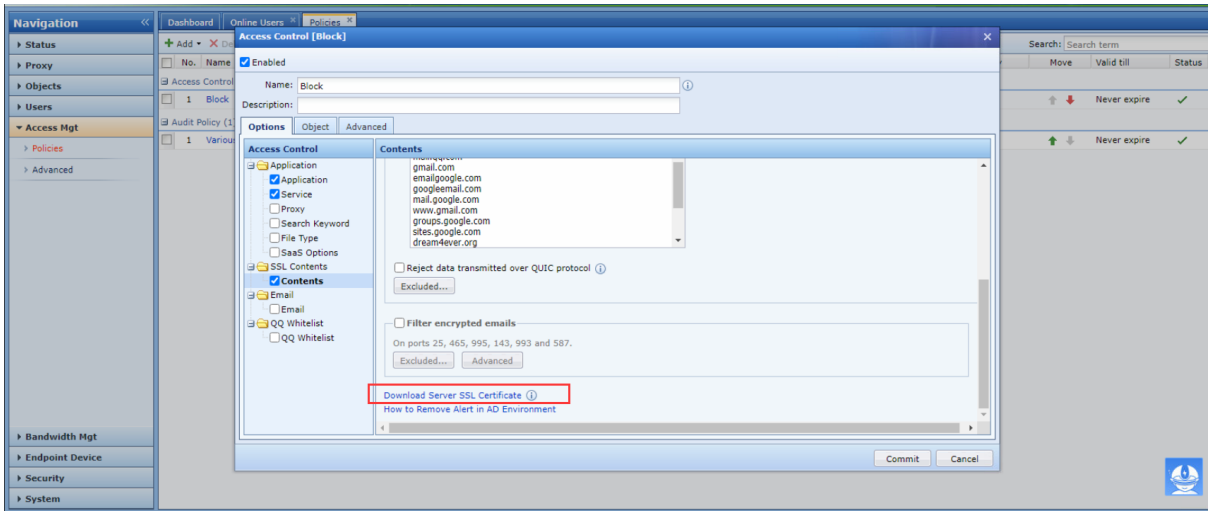
1. Jika Anda ingin melakukan kontrol yang lebih detail atas tindakan dari website https, seperti mengizinkan browsing tetapi tidak upload attachment, kemudian Anda perlu memeriksa deskripsi database apps untuk menentukan apakah Anda perlu decrypt domain name yang relevan. Misalnya, setelah query deskripsi database, Anda dapat konfirmasi bahwa Gmail upload attachment perlu mengaktifkan SSL data decryption.

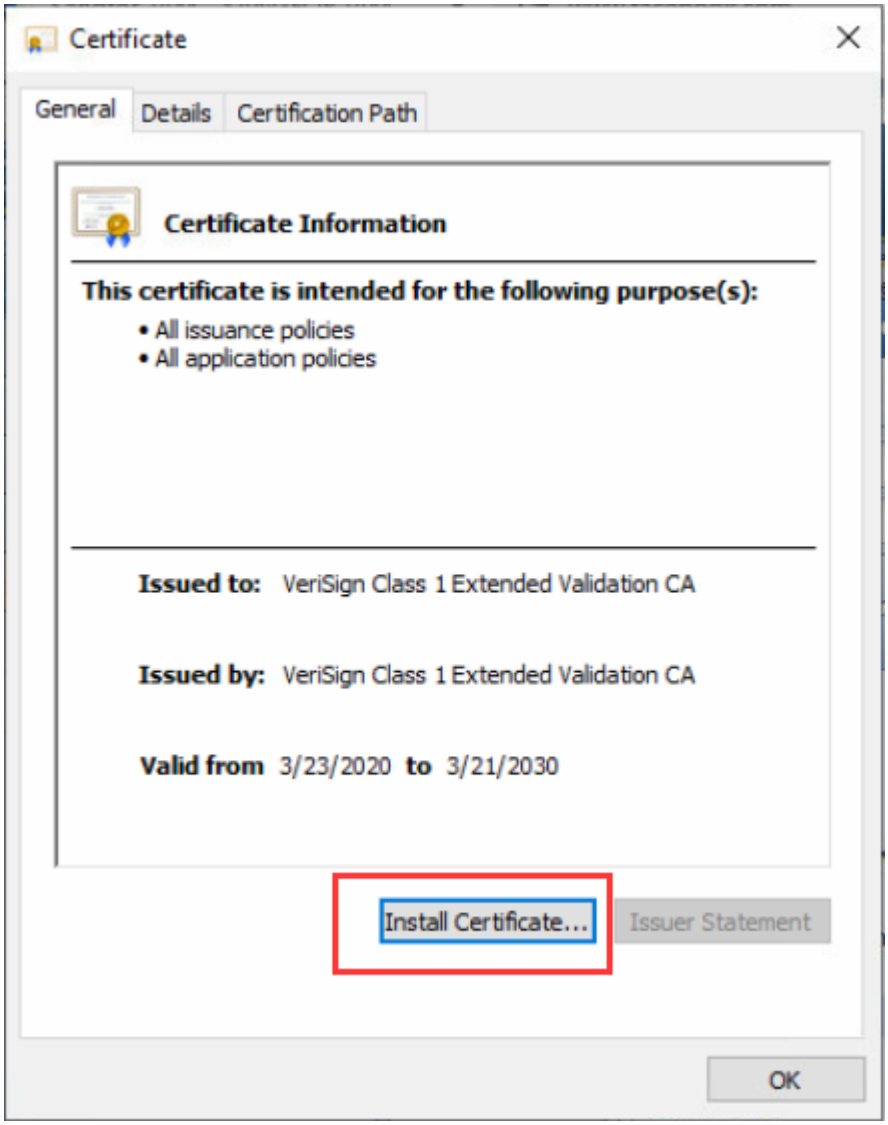


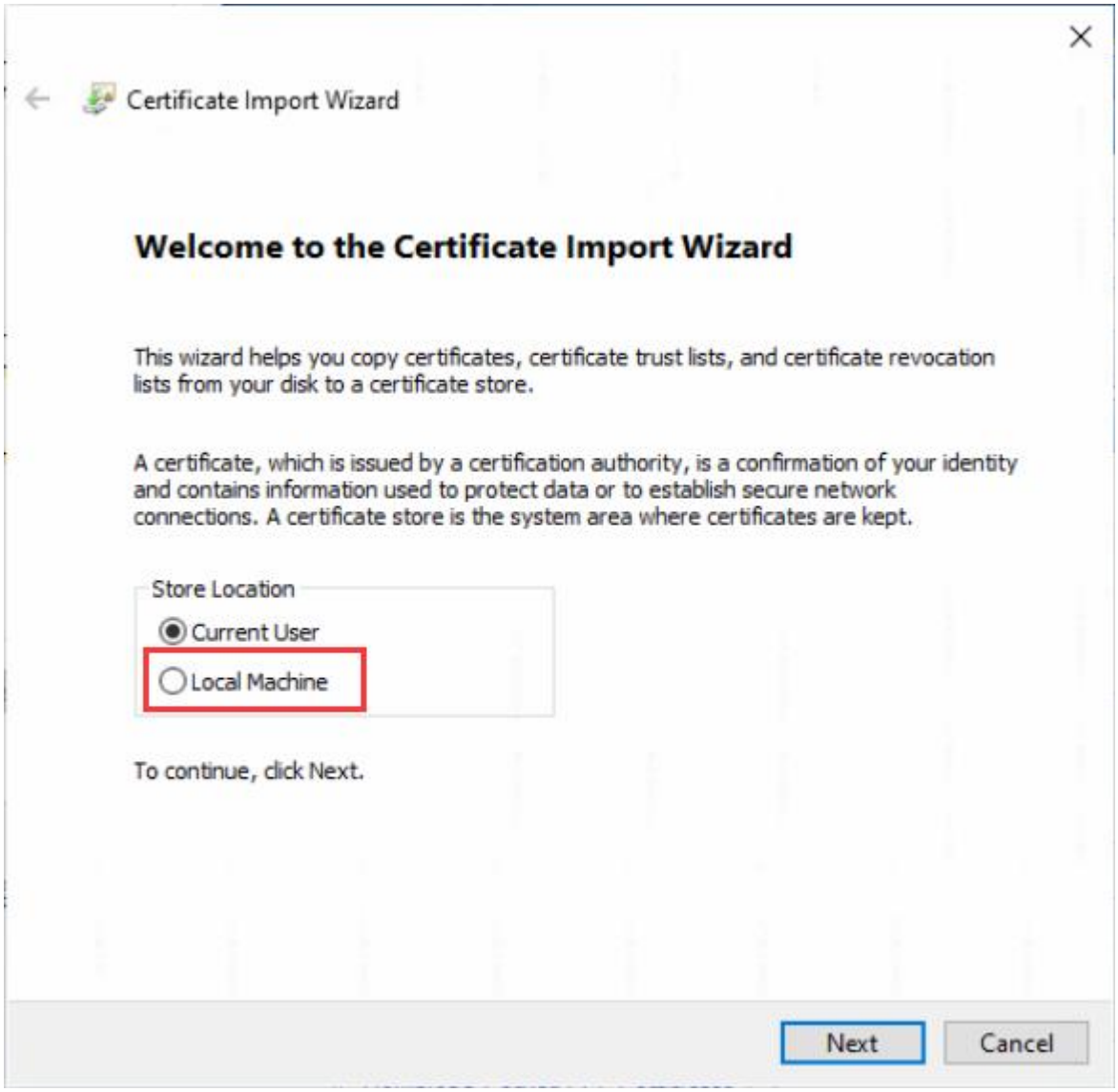
2.Aktifkan SSL recognition dan pilih website yang memerlukan SSL decryption sebagai Gmail.

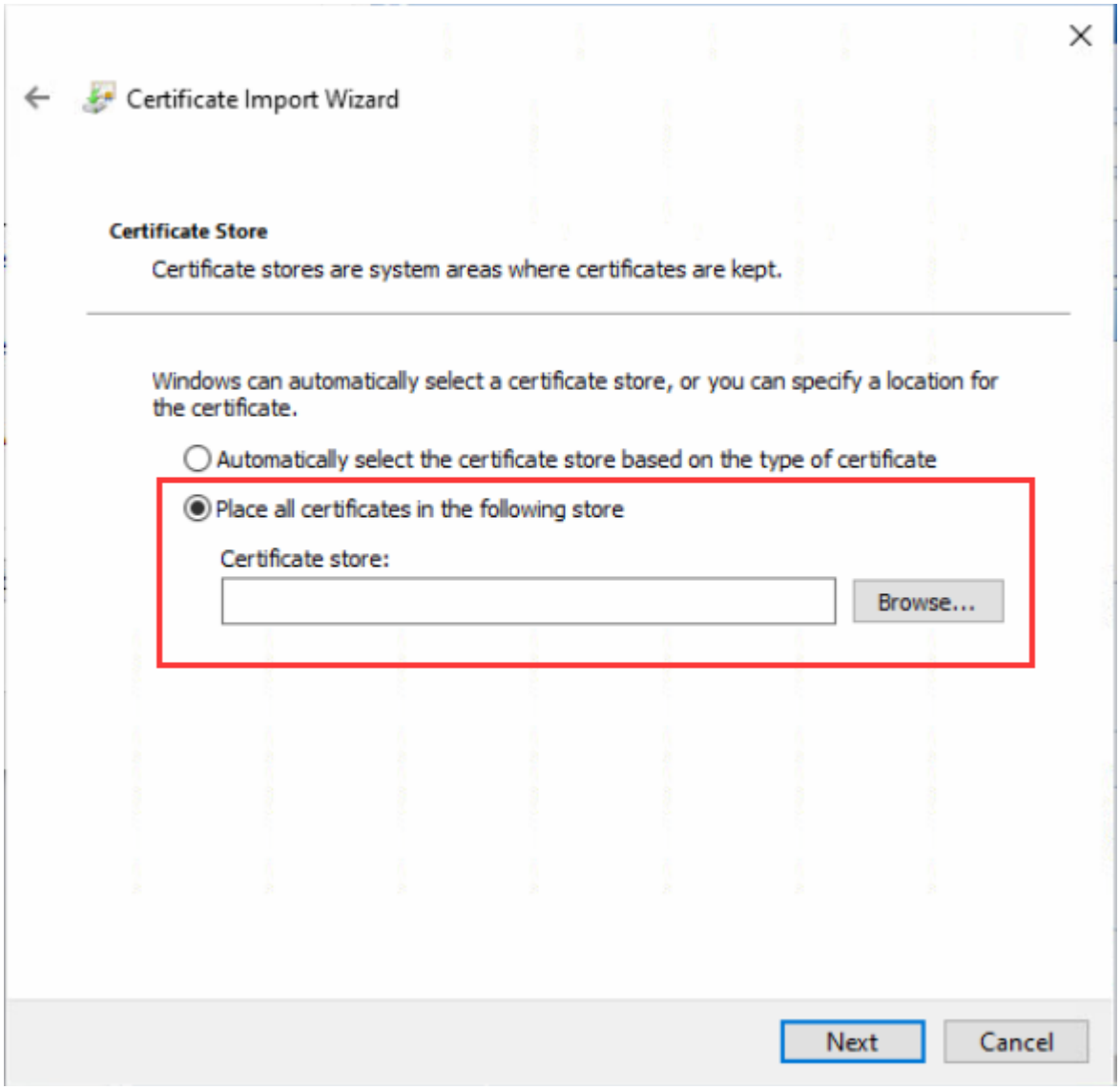


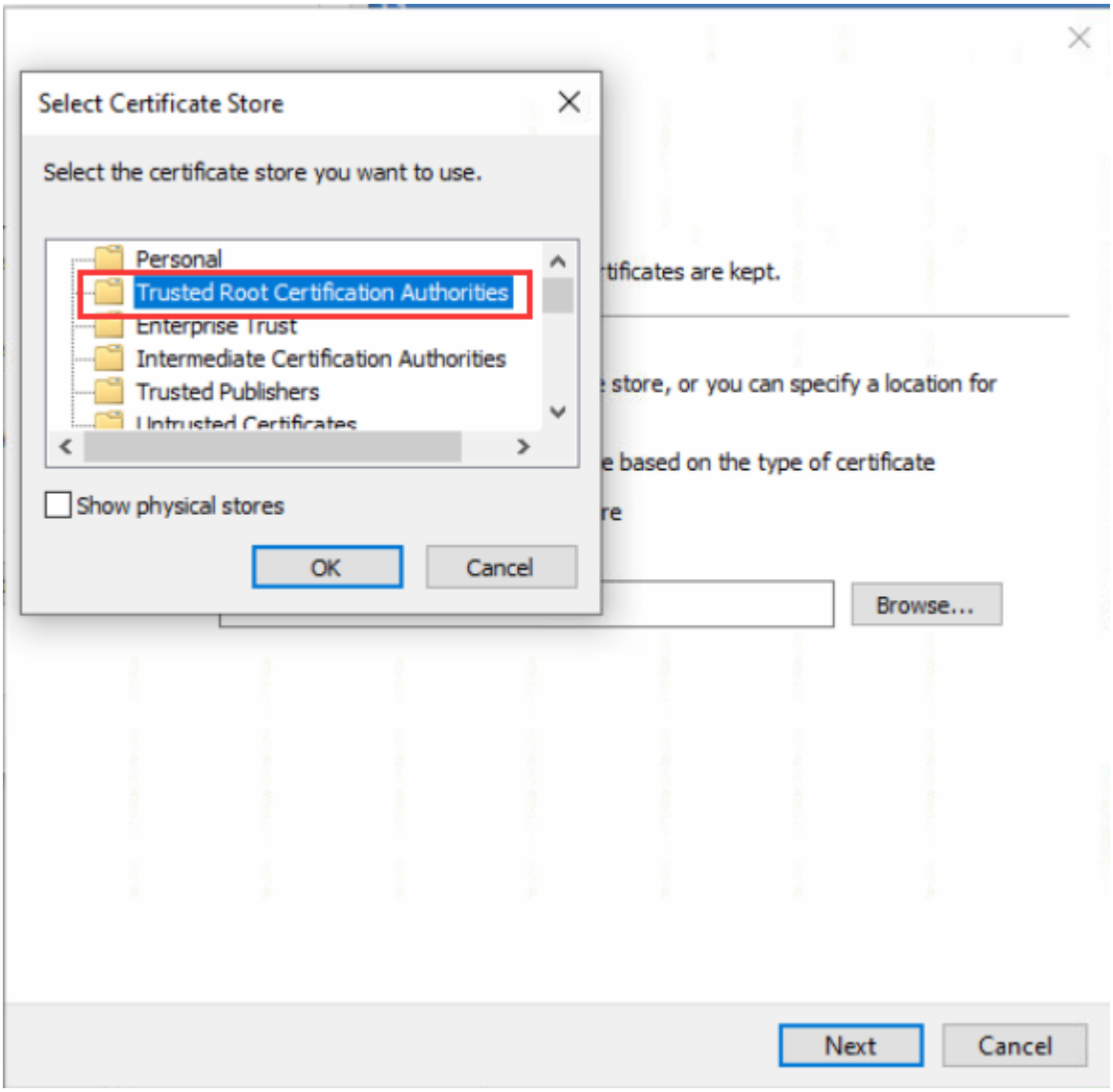
3. Download root certificate yang dikenali oleh SSL dari perangkat IAM dan import ke dalam sistem.

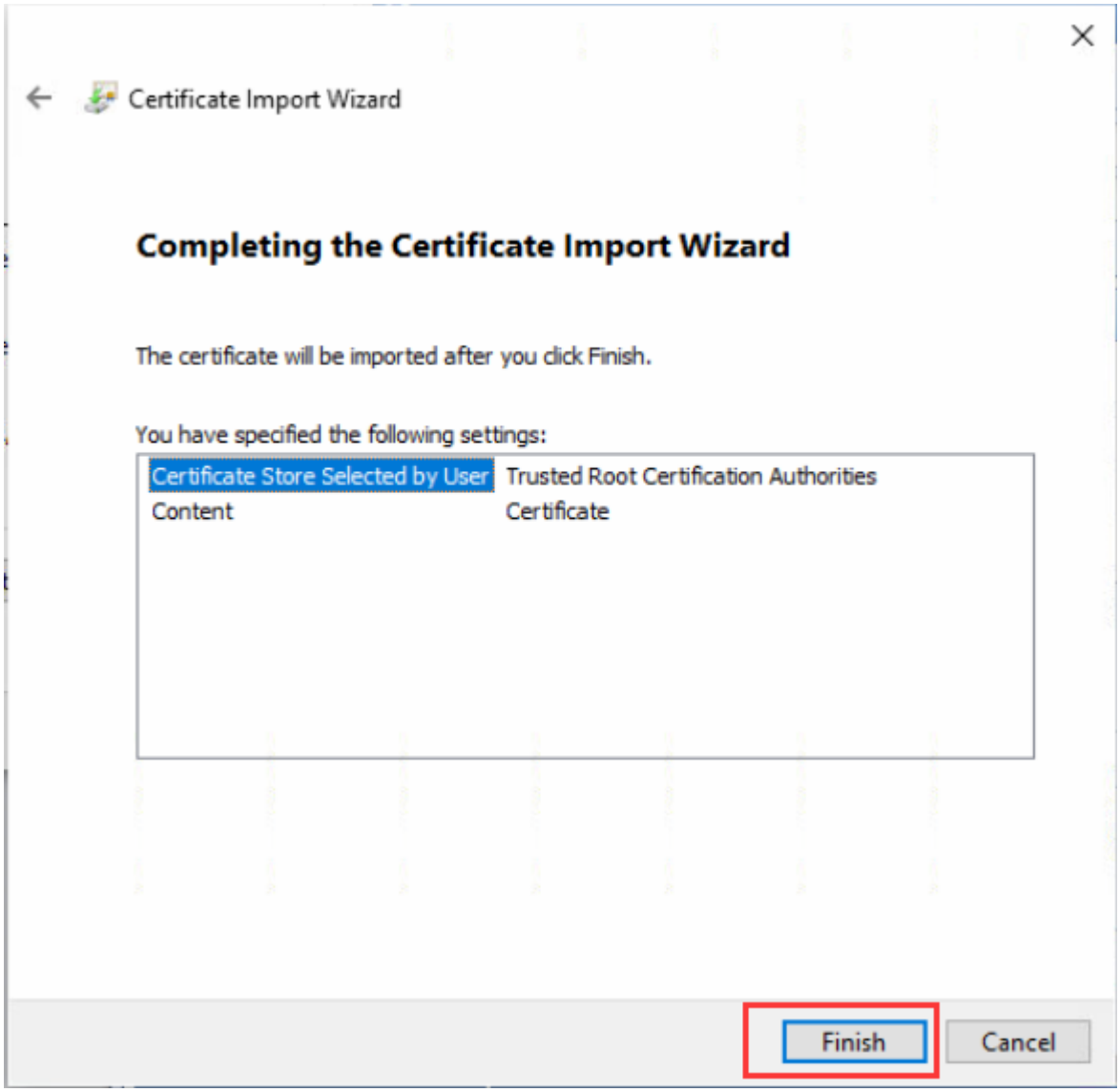



Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: VeriSign Class 1 Extended Validation CA
Issued by: VeriSign Class 1 Extended Validation CA
Valid from 3/23/2020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

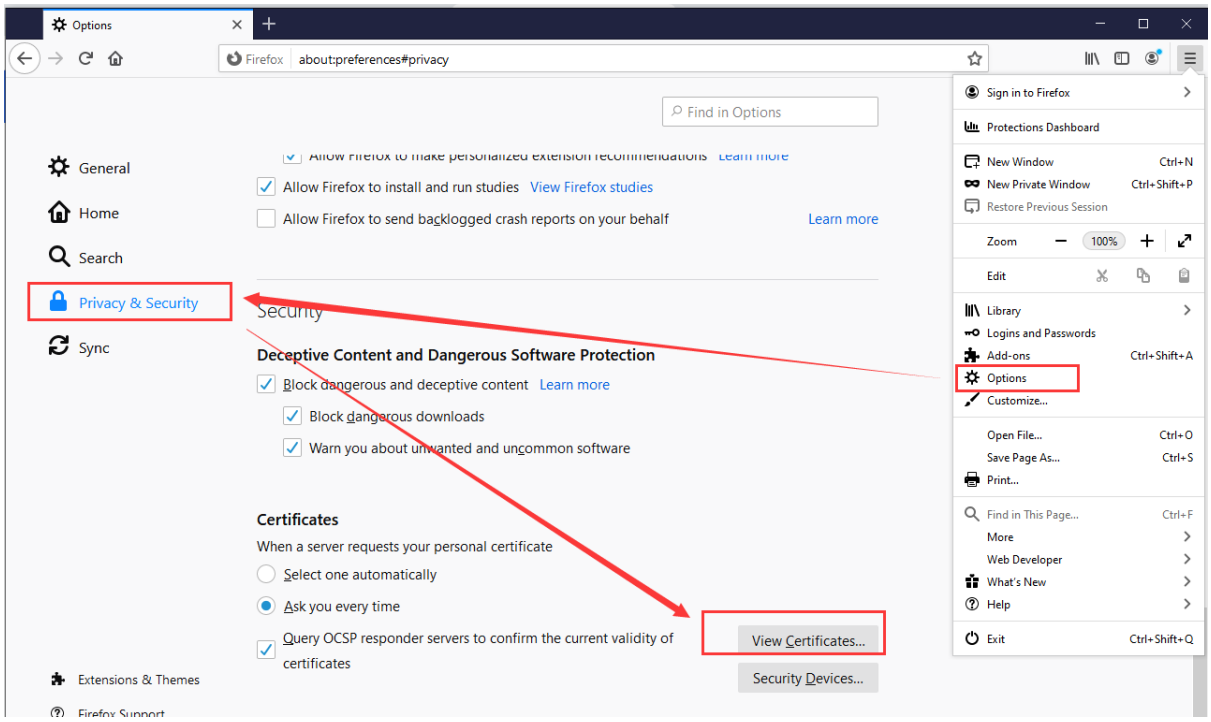

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity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

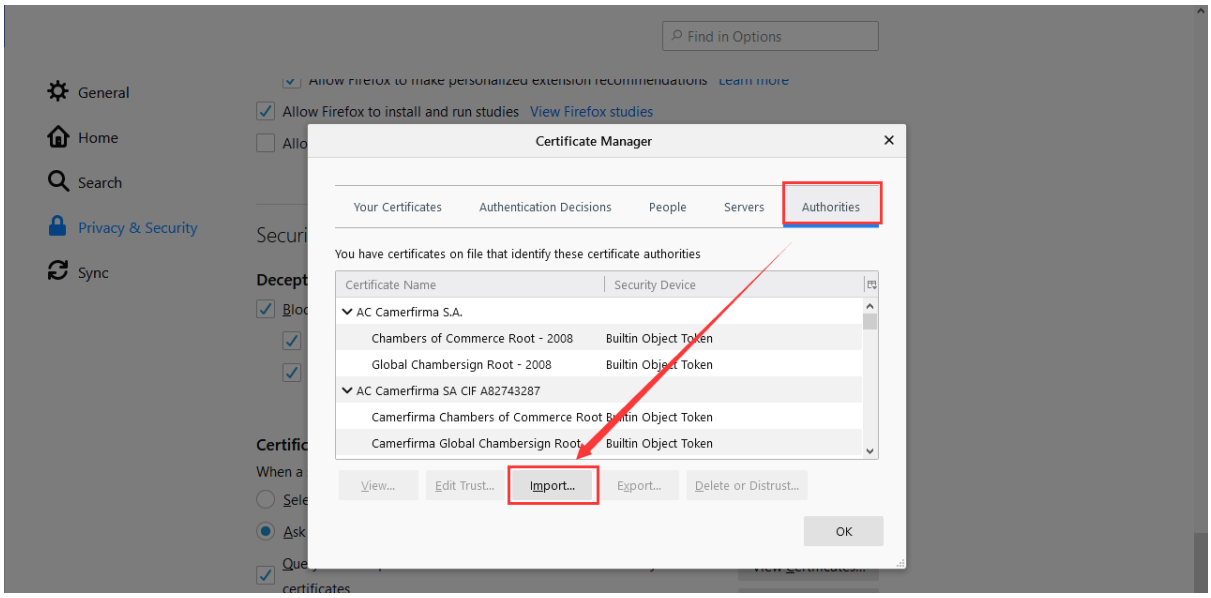

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates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

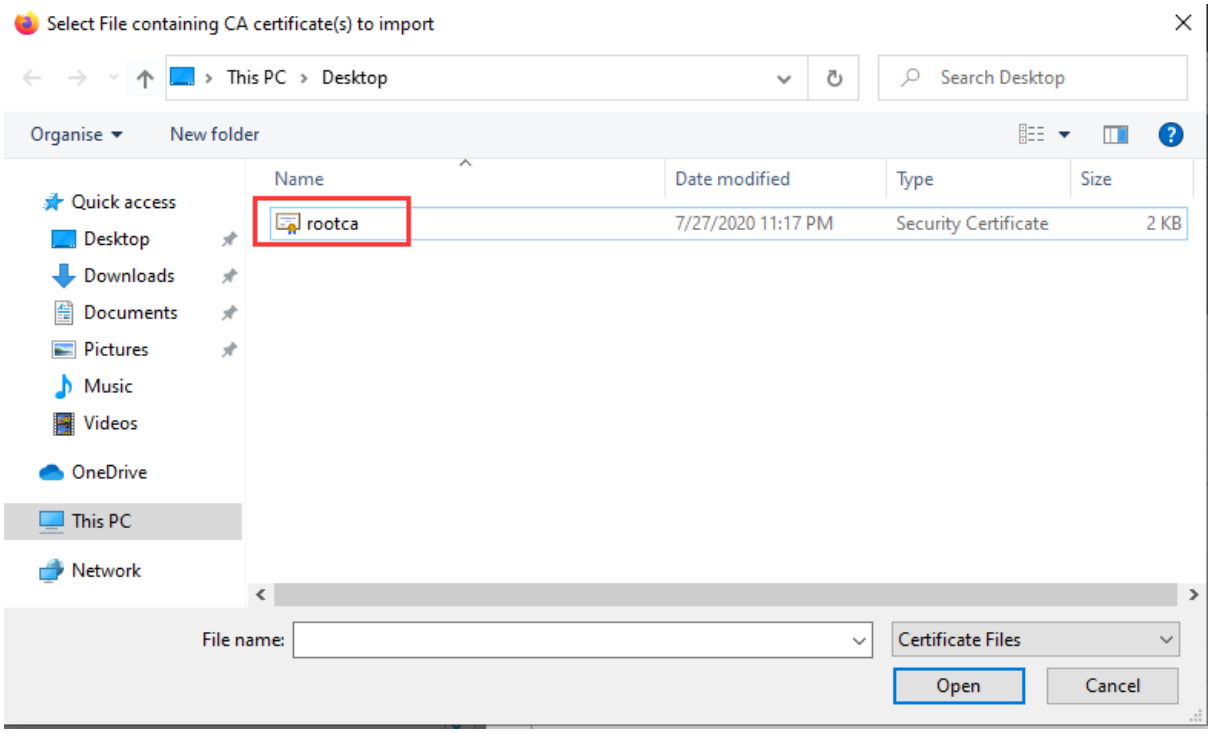

Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Show physical stores
OK
Cancel
tificates are kept.
store, or you can specify a location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

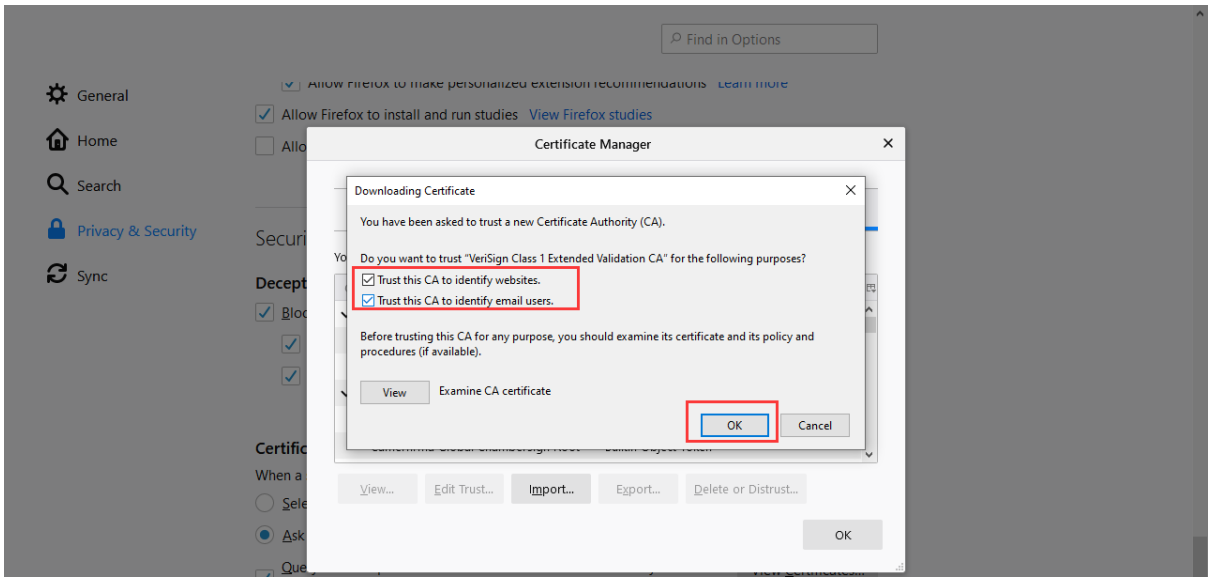


4. IE dan Chrome call certificate bawaan dari sistem Windows, dan Firefox browser tidak call certificate bawaan dari sistem Windows dan perlu diimport secara terpisah.

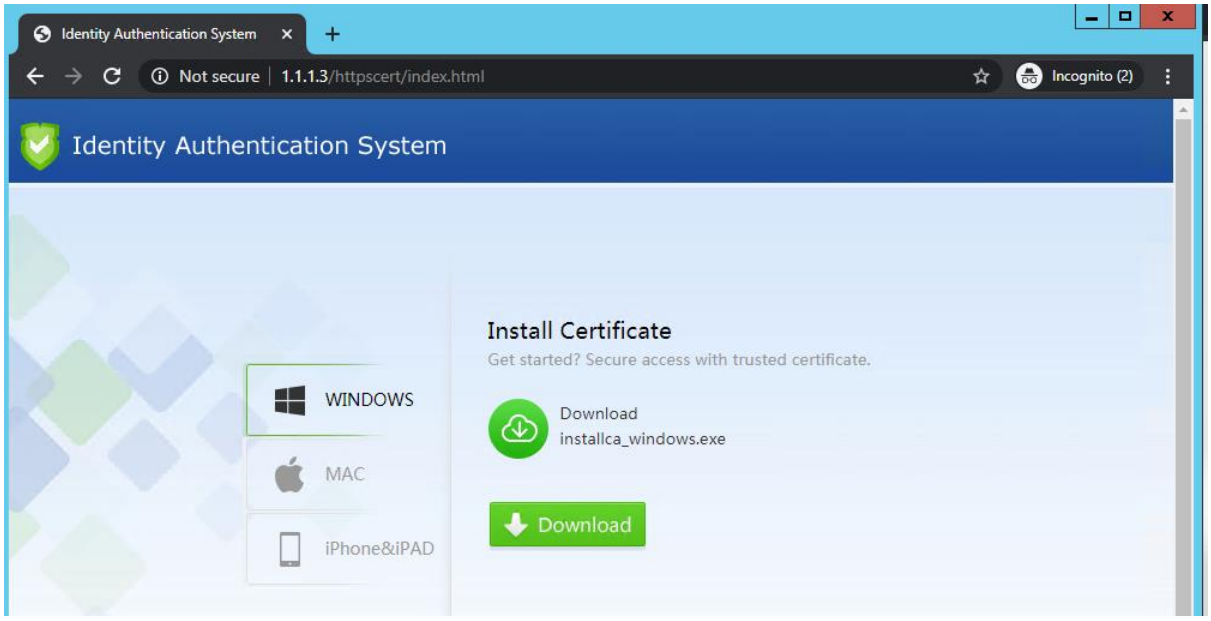

Options
Firefox
about:preferences#privacy
Find in Options
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Allow Firefox to install and run studies
View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf
Learn more
Security
Deceptive Content and Dangerous Software 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
New Private Window
Restore Previous Session
Zoom
100%
Edit
Library
Logins and Passwords
Add-ons
Options
Customize...
Open File...
Save Page As...
Print...
Find in This Page...
More
Web Developer
What's New
Help
Exit


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

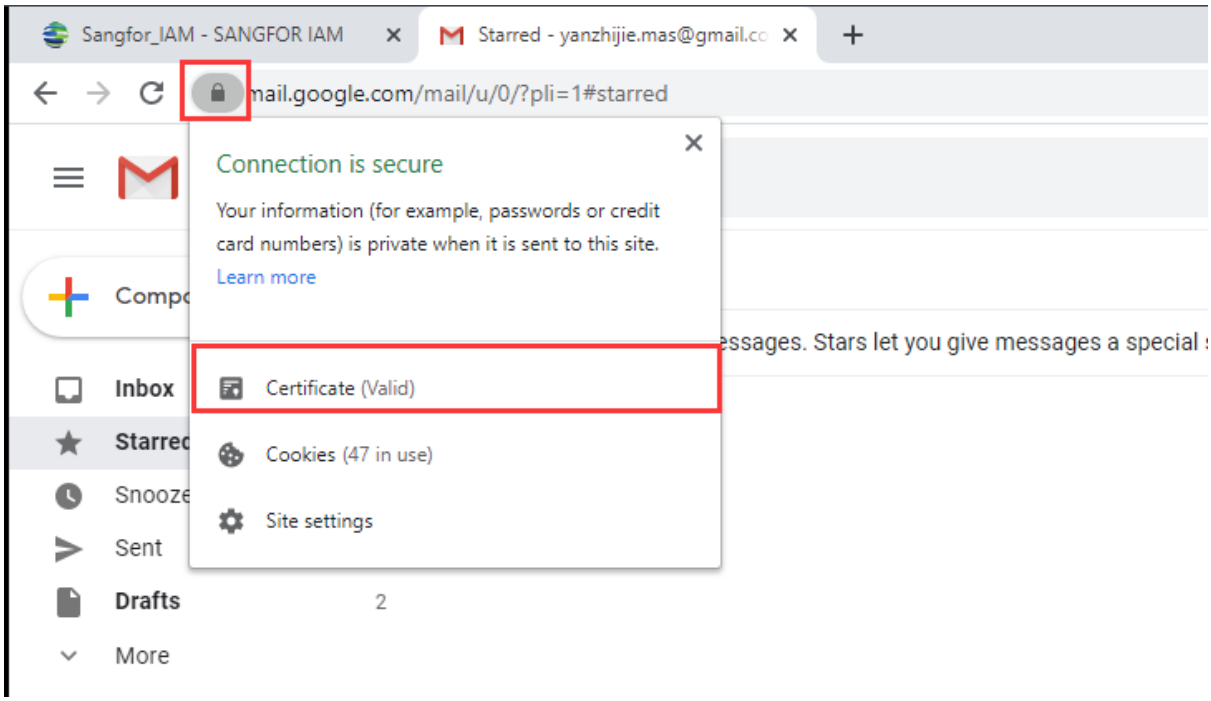


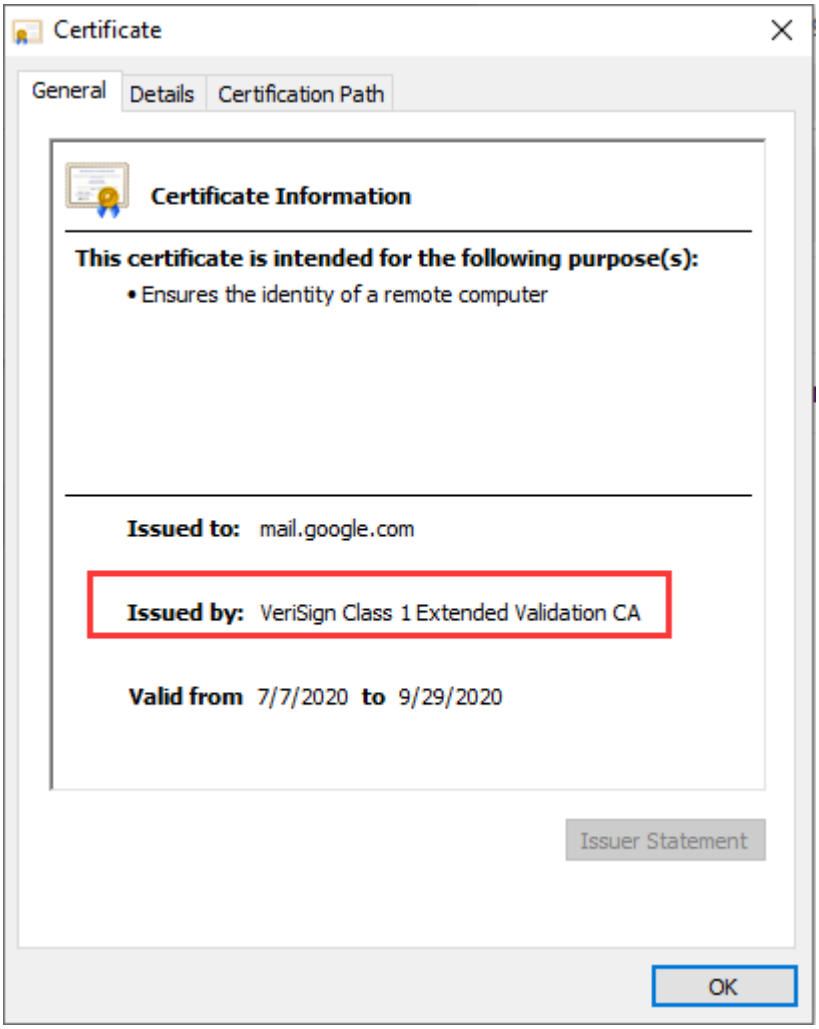


4. Anda juga dapat menggunakan cert installer download dari IAM link.
http://IAMip/httpscert/index.html IP IAM adalah IP IAM apapun yang dapat terkoneksi dari PC ke IAM.
misalnya: http://1.1.1.3/httpscert/index.html

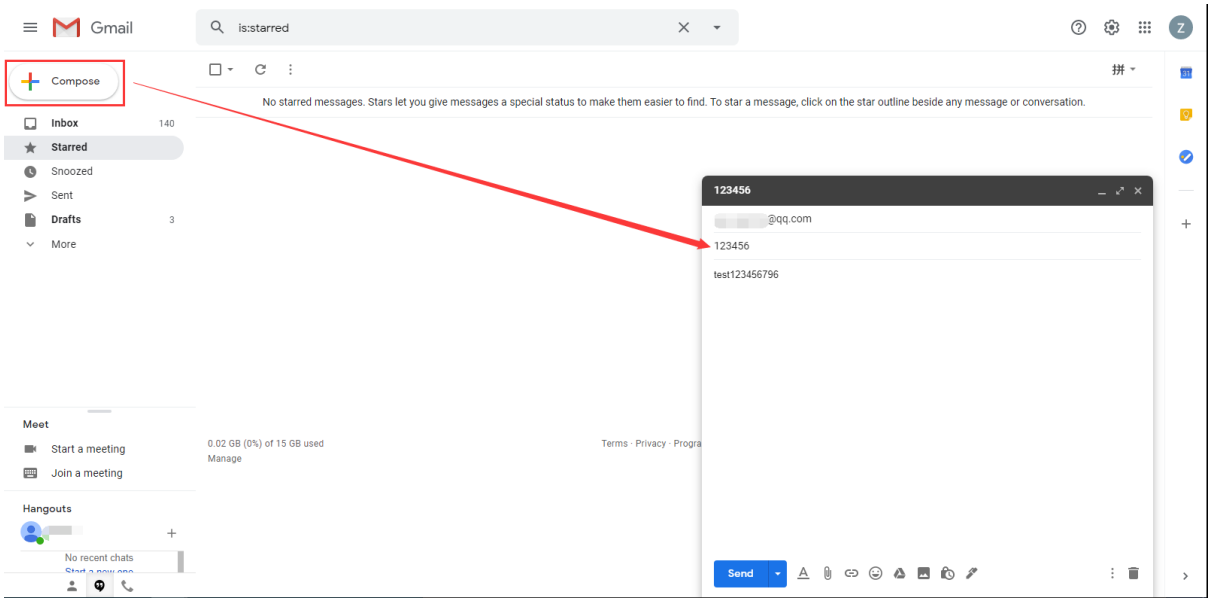


5. Periksa apakah certificate yang digunakan untuk mengakses website "VeriSign Class 1 Extended Validation CA", jika benar, berarti SSL decryption berhasil.





5. Gunakan Gmail untuk mengirim mail, Anda bisa mendapatkan judul dan body content dari mail.



SSL Content Decryption