SANGFOR

IAM

SSL Content Identification Troubleshooting Guide

Version 12.0.18

Change Log

Date	Change Description
April 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Background 1
Chapter 2 Common troubleshooting methods for SSL content identification 1
1 Check if the device can access the Internet 1
2 Check if the SSL proxy is successful 1
Chapter 3 Advanced troubleshooting 3
1 Confirm whether the Multi-Function License has Private Content Audit 3
2 Check if the root certificate is imported to the appropriate path 3
3 Check if the IP address or domain name is added to Global Exclusion 4
4 Check the network topology 5
5 Reject HSTS Network Protocol 5

Chapter 1 Background

Many websites are encrypted during the online process, such as webmail or web BBS; many email clients also support encrypted transmission. The IAM device enables auditing and filtering of encrypted content by enabling the ssl content identification function.

Chapter 2 Common troubleshooting methods for SSL content identification

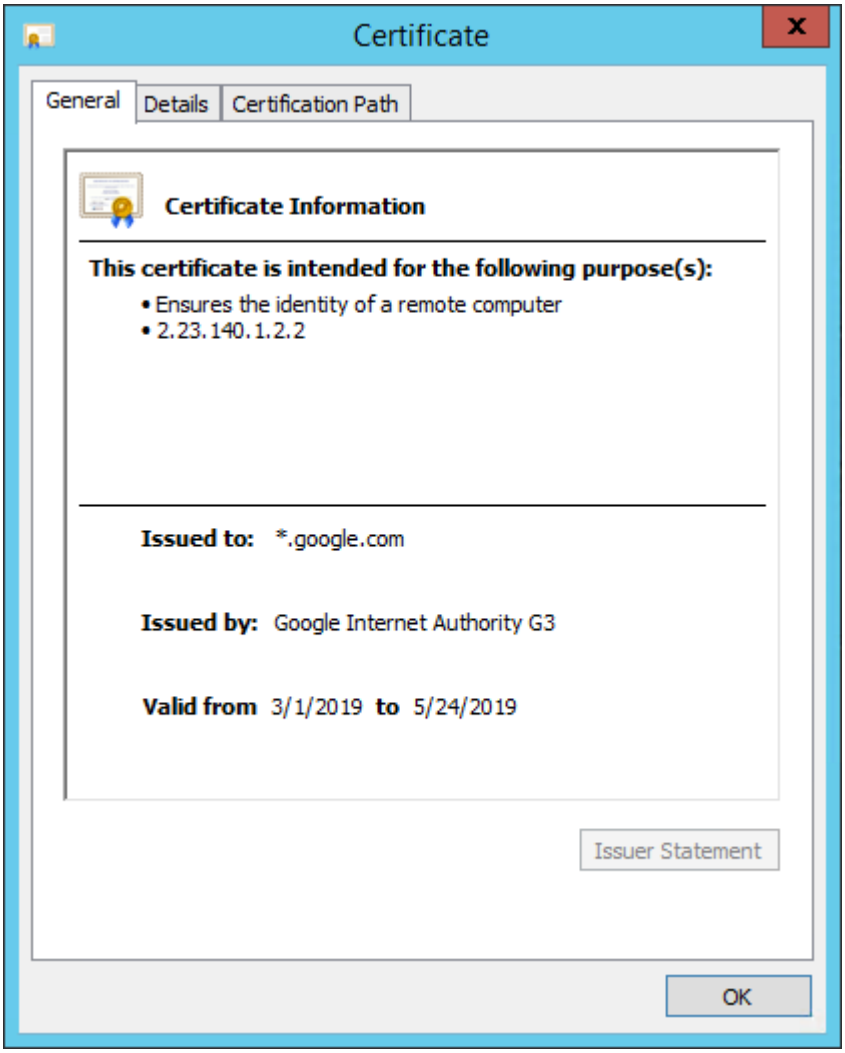
1 Check if the device can access the Internet

In the routing mode, SSL content identification is implemented by the device program proxy, so it is necessary to ensure that the device itself can be authenticated by SSL content recognition.

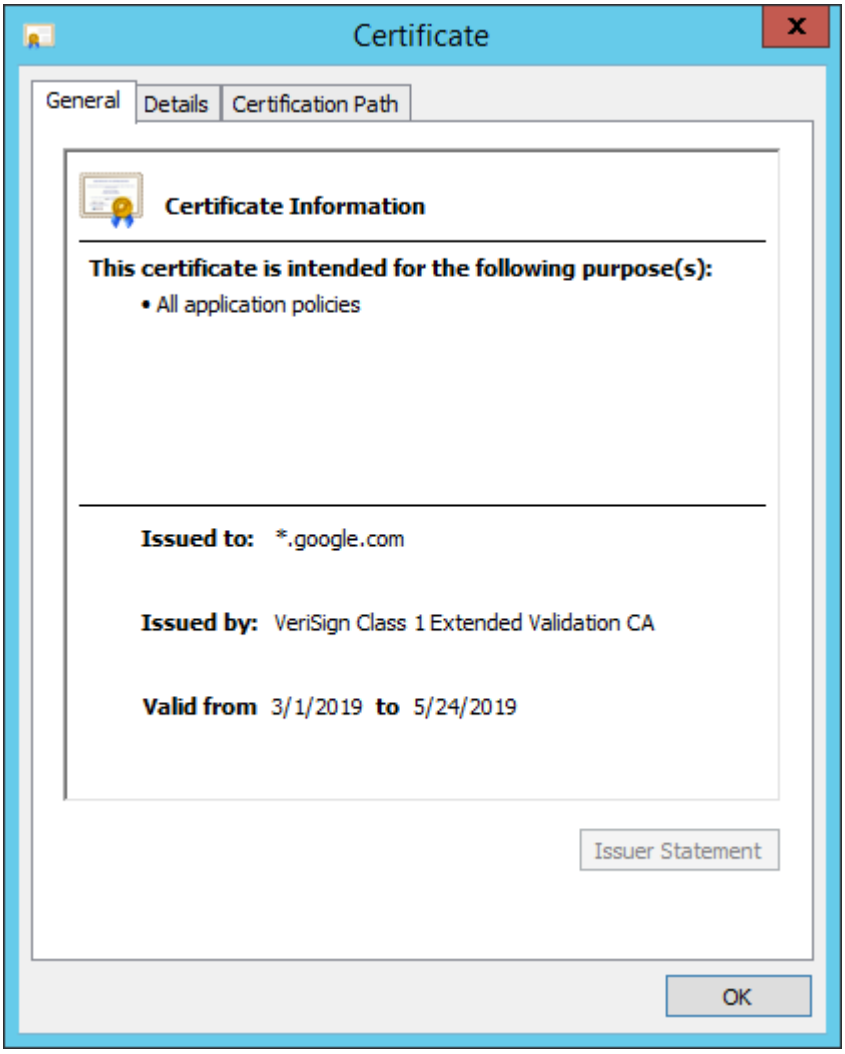
2 Check if the SSL proxy is successful

Confirm that there is no SSL proxy success, you can compare the certificate issuer name after the PC accesses the corresponding website.

Before successful agent:

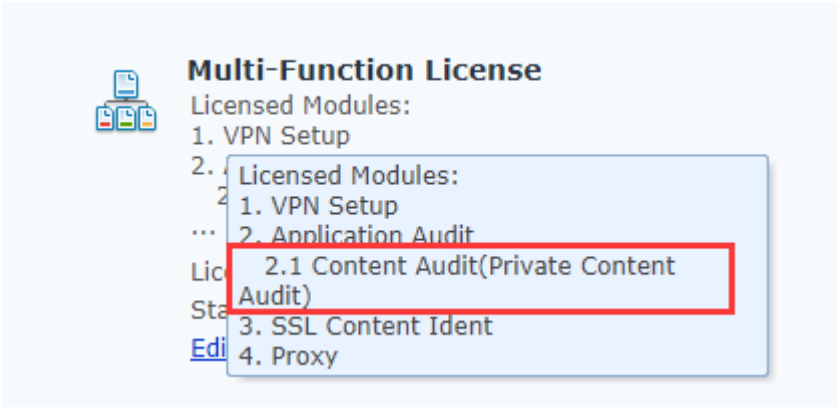


After successful agent:



Chapter 3 Advanced troubleshooting

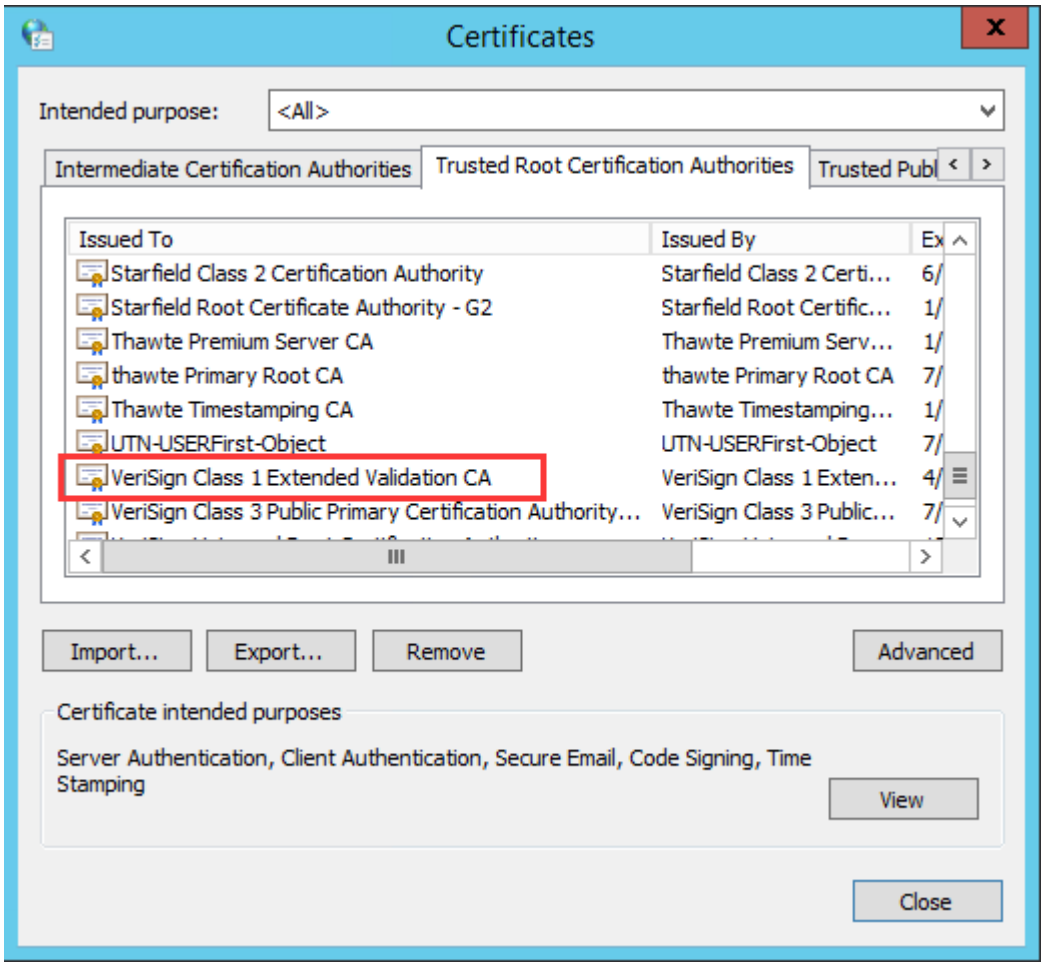
1 Confirm whether the Multi-Function License has Private Content Audit



2 Check if the root certificate is imported to the

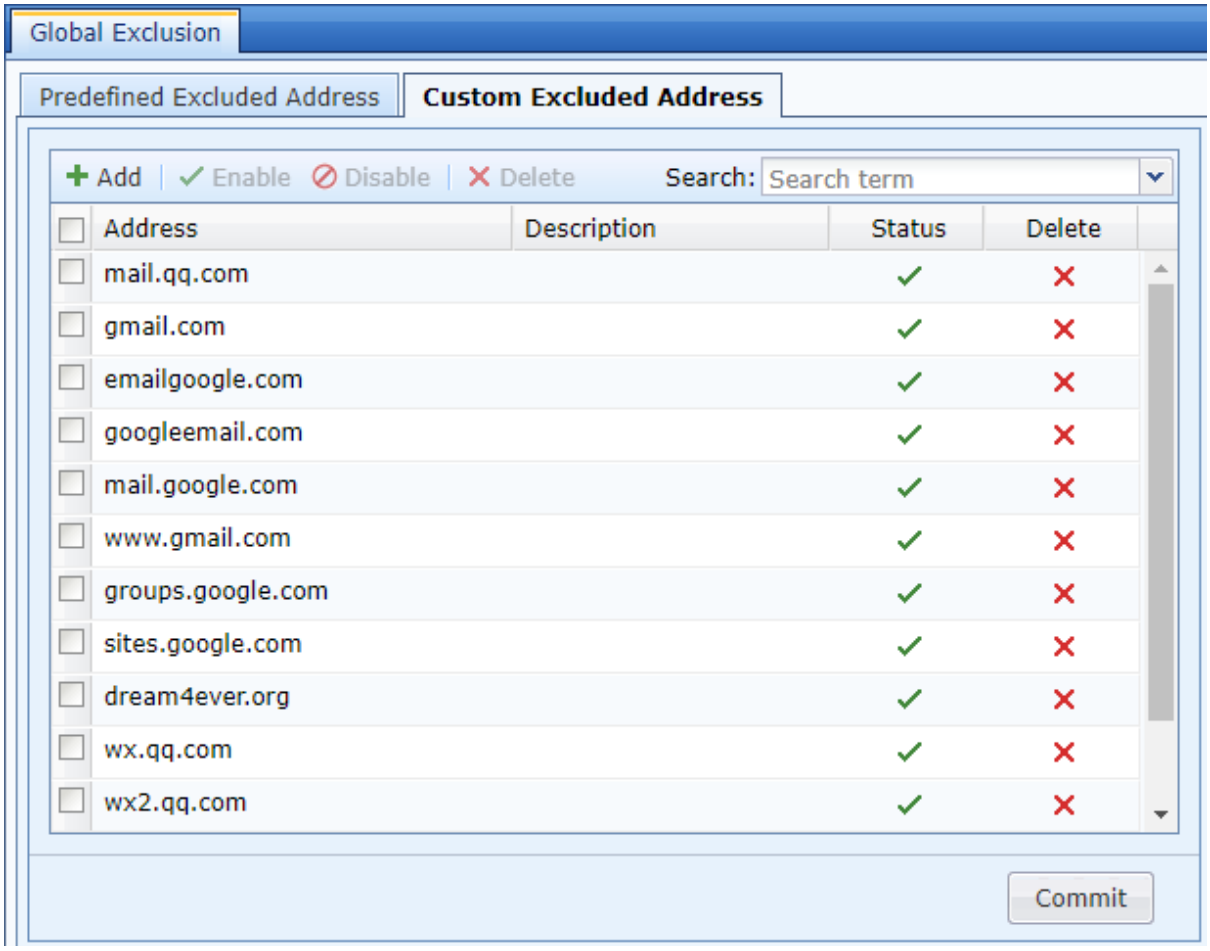
appropriate path

Check if the certificate is imported to a trusted root certification authority.



3 Check if the IP address or domain name is added to Global Exclusion

If the address is added to Global Exclusion, by default, the address or domain name will not be identified by SSL content.

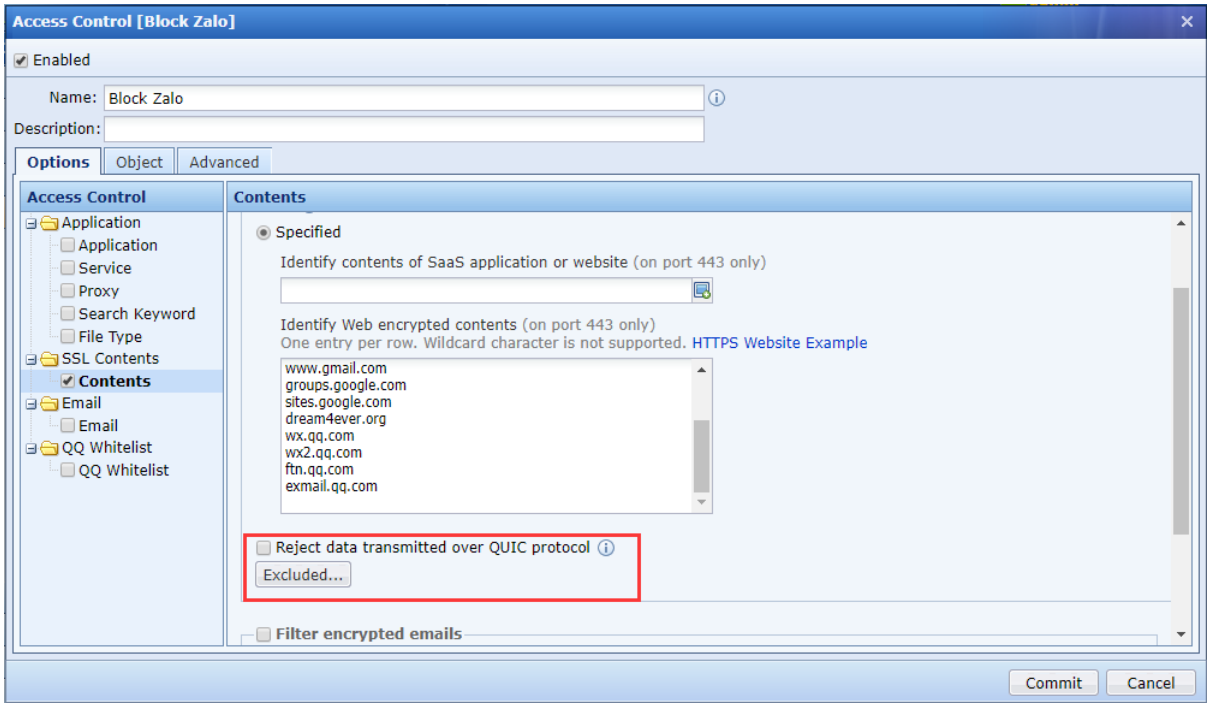


4 Check the network topology

If the device is deployed in the bridge mode between the proxy server and the PC, the SSL content recognition function does not take effect.

5 Reject HSTS Network Protocol

Some websites use the HSTS protocol, which causes SSL content identification to not take effect, so the HSTS protocol needs to be disabled.



At the same time, you can manually define HSTS network services and disable them.