Grandstream Networks, Inc.

GCC6000 Series -
SSL Proxy Guide

GCC6000 Series - SSL Proxy Guide

Introduction

The GCC convergence devices come with an embedded SSL proxy that can be used to encrypt and decrypt data passing between the clients (the connected devices), and the server (the GCC router module), this traffic is encrypted and can only pass through devices that have a CA certificate installed. The CA certificate installed confirms the authenticity of the connected device and allows it to receive HTTPS traffic from the GCC network.

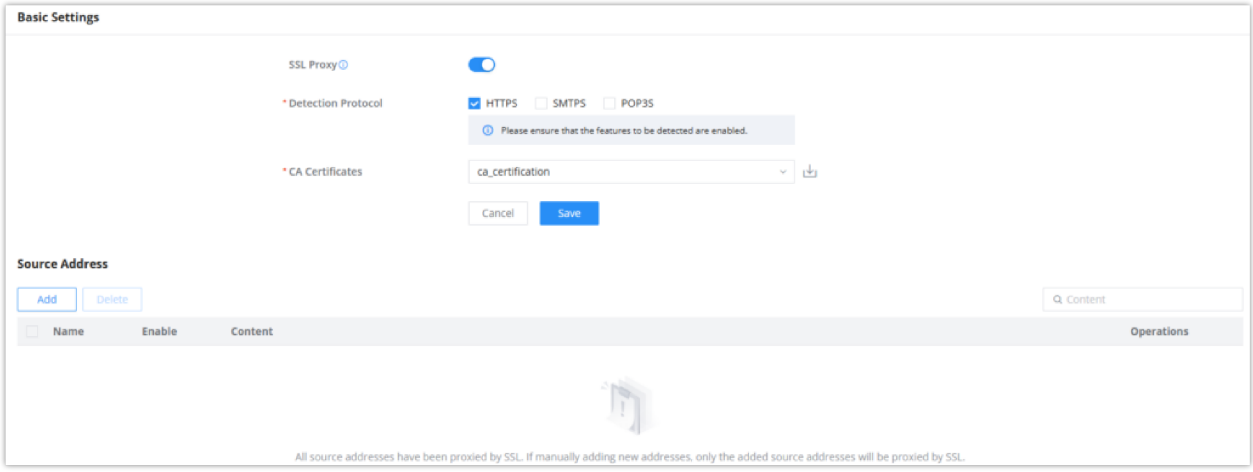
The SSL proxy is used by the GCC device to inspect packets that contain encrypted traffic (HTTPS traffic), which is utilized by tools such as anti-malware, and the content security tools, such as web filtering, and application filtering.

In this guide, we will walk through the steps needed to configure a GCC convergence device to use an SSL proxy, in addition, we will generate a CA certificate and install it on a trusted machine. With this configured, only devices with the CA certificate installed will be able to access HTTPS-encrypted traffic.

Enabling SSL Proxy

The SSL proxy must be enabled on the GCC convergence device to allow packet inspections for HTTPS traffic, to do that:

1. Navigate to **Firewall Module → SSL proxy → Basic Settings**
2. Enable the SSL proxy by toggling the option below, after enabling the SSL Proxy, end users will see certificate warnings when browsing web pages unless the certificate has been installed on their computers.
3. Select the Detection Protocol for the SSL proxy, if HTTPS is selected, the SSL proxy will inspect the HTTPS packets that are sent to and received from the connected desktops with the certificate installed, you can select the detection to include SMTPS, POP3S packets too.
4. A CA certificate must be selected to authenticate the connected devices, Please refer to the [Create CA certificate] section to learn more about this step.
5. Once the CA certificate is created and uploaded, click the icon to download the .crt file that will be installed on connected endpoints that will be granted access to the Internet through HTTPS traffic.



Enabling SSL Proxy

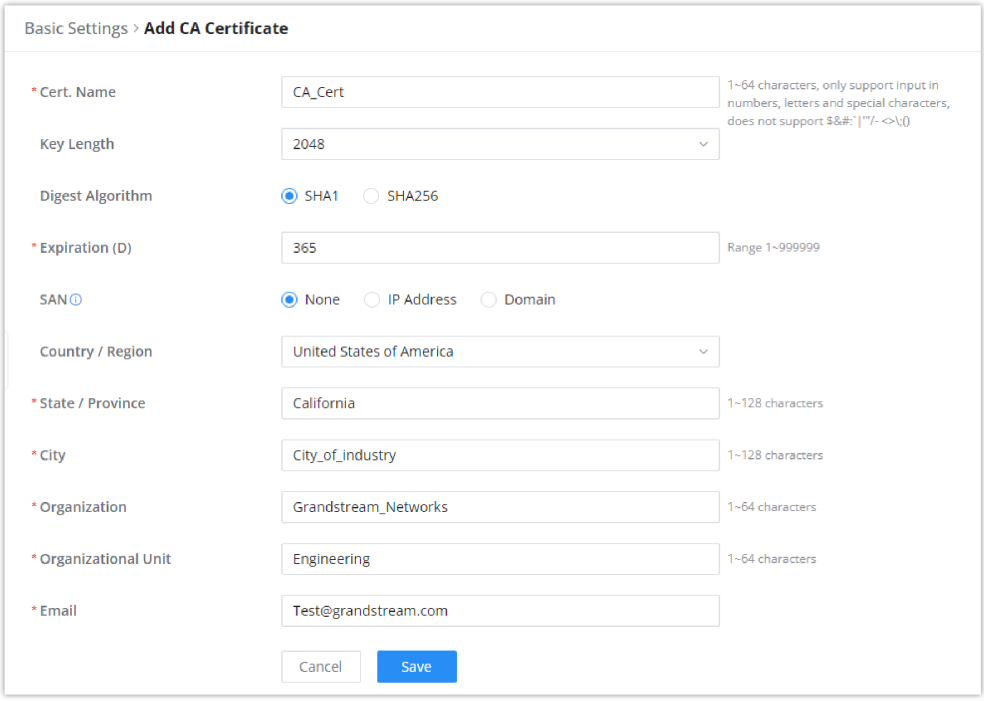
Note

Units without the SSL proxy certificate can still access the internet, but their access will be limited to unencrypted HTTP. However, they can be further restricted from accessing the internet entirely by applying specific inbound firewall rules to block outbound connections.

Creating CA Certificate

To create the CA certificate to be used on the SSL proxy:

- Under **Firewall Module → SSL Proxy → Basic Settings → CA Certificates,** Click the icon Add to add a new certificate
- Define the following parameters:
  1. **Certificate name**: Identifier for the certificate.
  2. **Key length**: Size of the encryption key: 1024, 2048, 4096 bits
  3. **Digest Algorithm**: Hash function for the certificate: SHA1, SHA256
  4. **Expiration**: Validity period of the certificate.
  5. **SAN:** Subject Alternative Name; specific requirements for SSL proxy: None, IP Address, Domain Name
  6. **Country / Region**: Country code of the certificate issuer.
  7. **State / Province**: State or province of the issuer.
  8. **City**: City of the certificate issuer.
  9. **Organization**: Name of the issuing organization.
  10. **Organizational Unit**: Department within the organization.
  11. **Email**: Contact email address.
- Once created it will be automatically added to the list of CA certificates, and can be selected to be used for SSL traffic authentication.



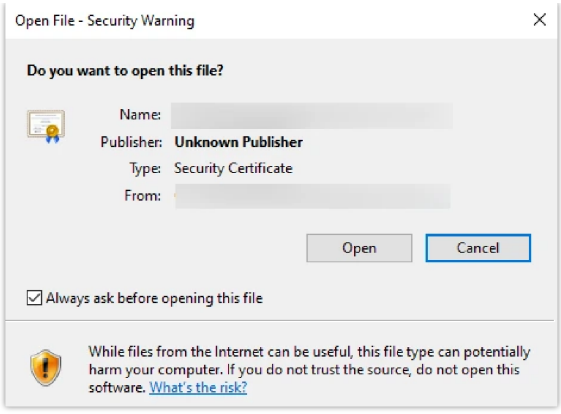
Creating CA Certificate

Installing CA Certificates on Endpoints

Depending on the operating system of your connected device, the process of installing the CA certificate will be different, we advise you to check the documentation provided by your operating system on how to install Custom trusted CA certificates.

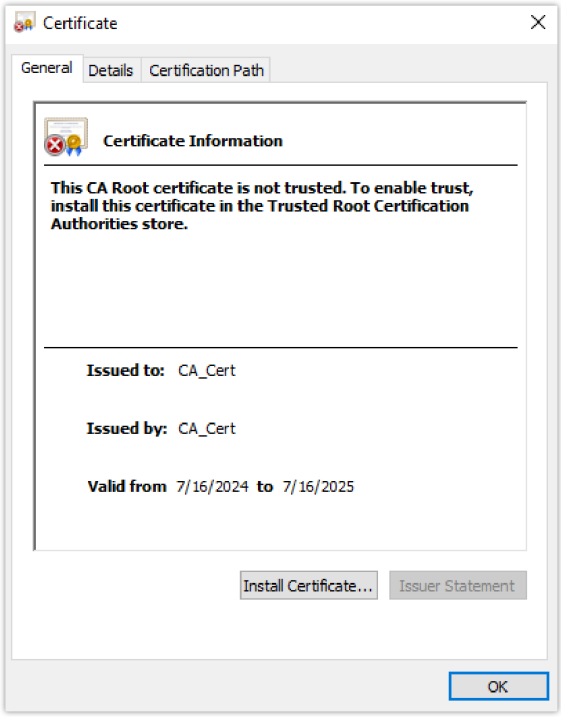
We will however show an example of how to install the CA certificate on a Windows machine,

- Once the CA certificate is downloaded and stored in the corresponding download folder, Double click the .crt file



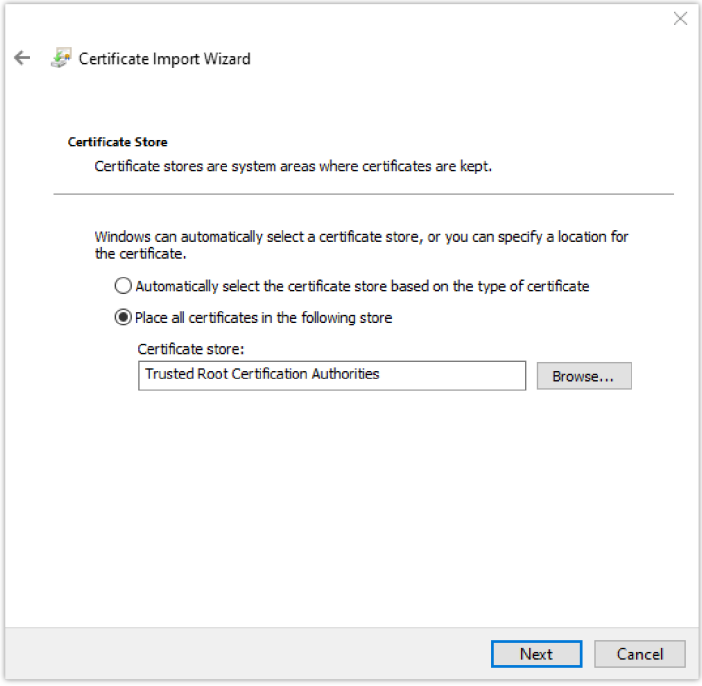
Open certification

- Open the certificate then, click on “Install Certificate”



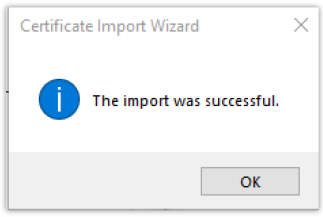
Install Certificates

- Set the store location to “Local Machine”
- Set the path where the CA certificate will be stored, in our case it will be “Trusted Root Certification Authorities”



Trusted CA Certificate

- Click “Next”, then “Finish” to finalize the import of the certificate, you should be prompted with a pop-up message confirming the upload of the certificate



Successful Certificate upload

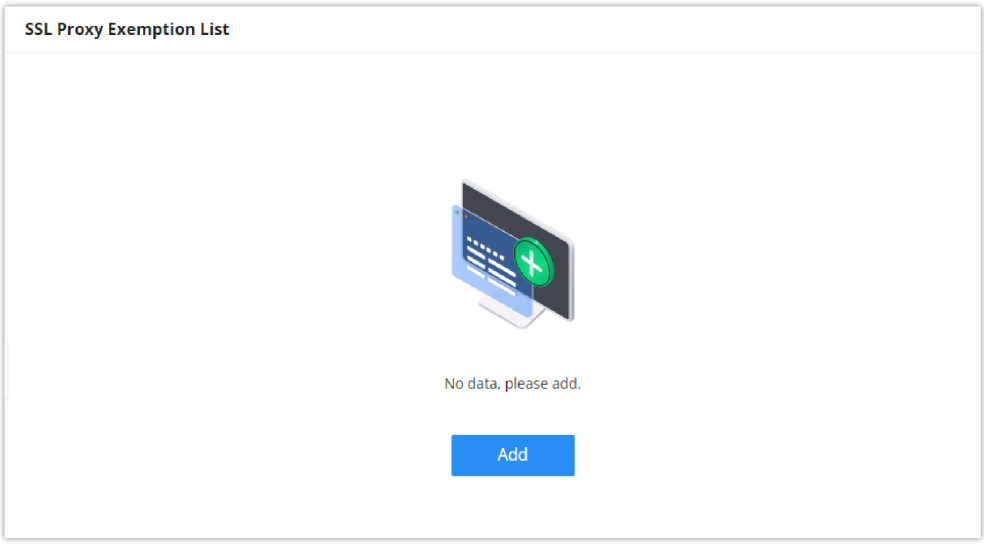
> **Note**
>
> To avoid adding the certificate manually on each desktop, you can use a configuration server or a Group Policy rule to push the CA certificate automatically on all the endpoints allowed to access the internet.

SSL Proxy Exemption List

In some scenarios we can use the SSL proxy only for specific types of web access, for example, access that requires higher security levels and the input of sensitive data, in other scenarios, we will want some services and websites to be accessible even without requiring an SSL proxy certificate, in this case,e we can create an SSL Proxy Exemption List

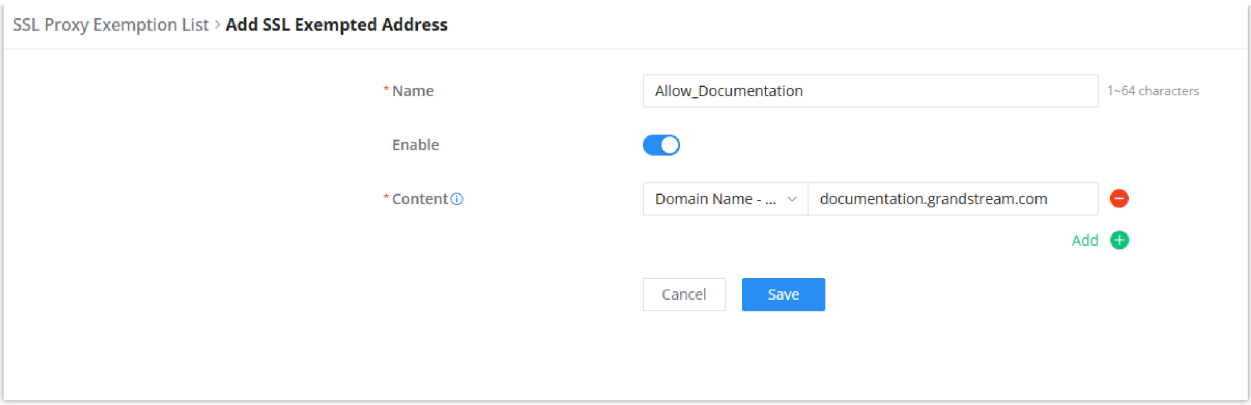
To configure this please follow the below steps:

- Navigate to **Firewall Module → SSL proxy → SSL Proxy Exemption List**
- Click “Add” to add a new exception rule



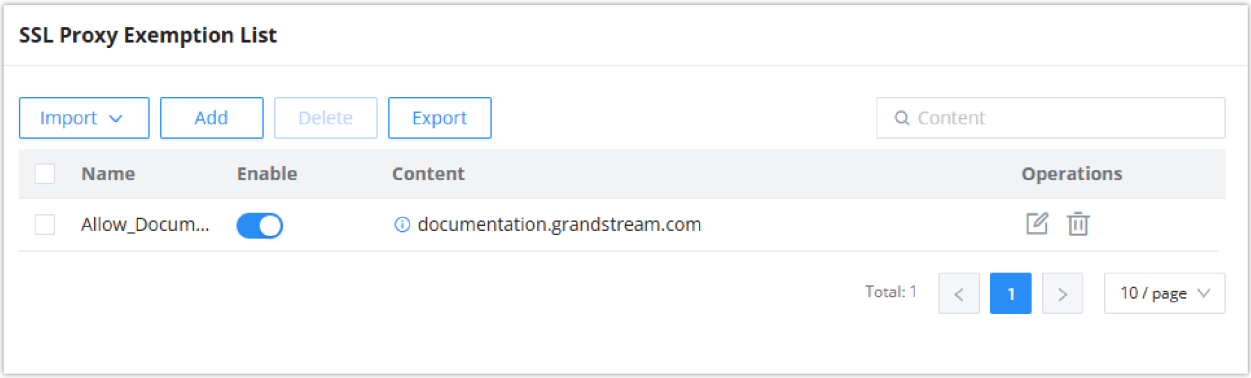
SSL Proxy Exemption List

- Provide a name for the SSL exemption rule
- Enable the rule by toggling the status field,
- Select the content that will be exempted from requiring an SSL proxy certificate, the options are:
  1. **IP Address / Mask**: Excludes specific IP addresses or networks defined by a mask from requiring an SSL proxy certificate.
  2. **Domain** – **Simple Match/Wildcard**: Excludes specific domain names from requiring an SSL proxy certificate, either an exact domain name using **Simple Match**, or keywords of the domain name using **Wildcard**.
  3. **IP Range**: Excludes a range of IP addresses from requiring an SSL proxy certificate.
  4. **Web Category**: Excludes certain categories of websites (e.g., social media, finance) from requiring an SSL proxy certificate.
- In our case, we will allow access only to our documentation center domain name



SSL Proxy Exemption

- Once the rule is saved, endpoints, with no SSL proxy certificate installed will only be able to access the documentation website: **documentation.grandstream.com**



SSL Exemption Rule Created

> **Note**
>
> Users can import a list of SSL proxy Exemption domains and IP ranges using a predefined template that can be downloaded from the GCC device.

Supported Devices

Device Model	Firmware Required
GCC6010W	1.0.1.7+
GCC6010	1.0.1.7+
GCC6011	1.0.1.7+
