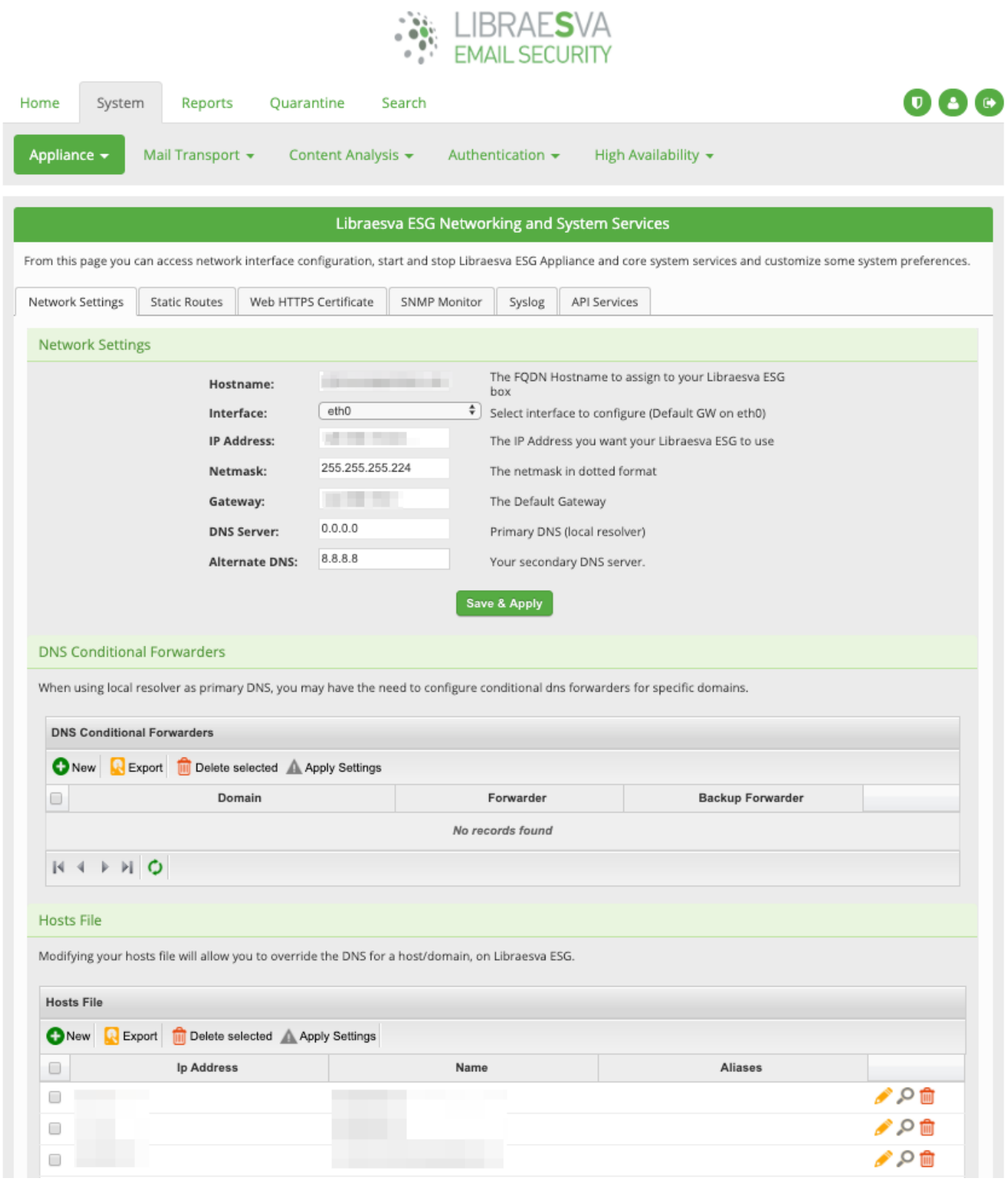
Networking

From this section you can configure network parameters of your Libraesva ESG and tune some general system preferences:

Network Settings

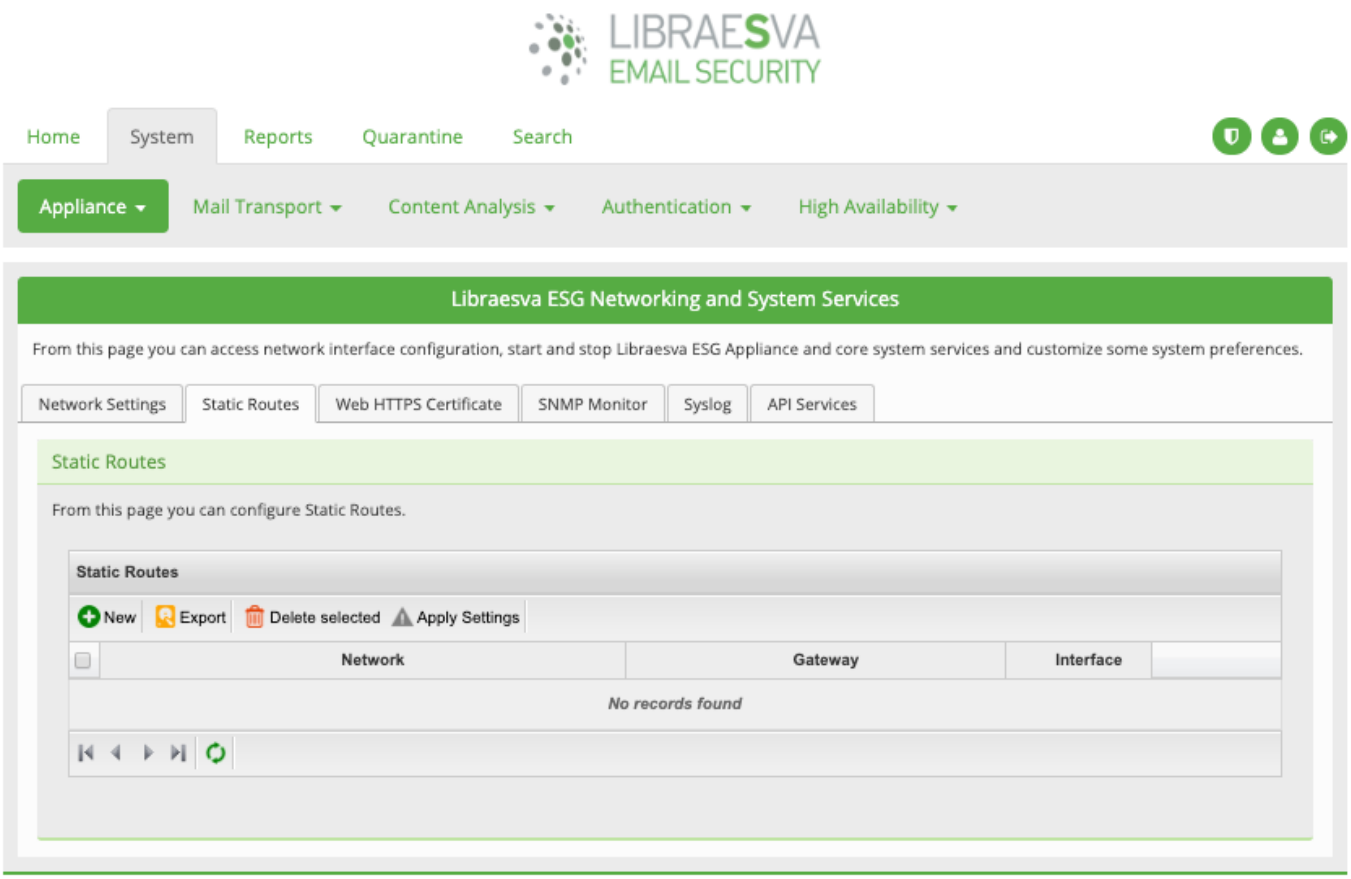


Hostname: the FQDN Hostname to assign to your Libraesva ESG, should be always defined in you public DNS zone
Interface: the Network Interface you want to modify
IP Address: the IP Address you want your Libraesva ESG to use
Netmask: the netmask in dotted format
Gateway: the Default Gateway
DNS Server: 0.0.0.0 as primary. (not customizable because of the multiple request at the

same time)
Alternate DNS: your secondary DNS server
DNS Conditional Forwarders: when using local resolver as primary DNS, you may have the need to configure conditional dns forwarders for specific domains.
Hosts File: this section allows to define local mapping of ip address with their hostnames. Useful to achieve local delivery destination backups (by inserting two entries with different ip's and same hostname, used later on in relay table)

Static Routes

From this page you can configure Static Routes.



To add a new static route simply press **New** button.

×**NOTE:** Remember to Apply Setting after any modification to make them active!

Web HTTPS Certificate

This section allows to secure your web access with a new https certificate.

First section shows the installed certificate.

From this tab you have options to:

- create a new self signed certificate using Let’s Encrypt authority
- generate a new certificate request to submit to your CA
- upload your wildcard certificate (Standard PEM – Base 64 format)

LIBRAESVA EMAIL SECURITY

Home | System | Reports | Quarantine | Search

Appliance | Mail Transport | Content Analysis | Authentication | High Availability

Libraesva ESG Networking and System Services

From this page you can access network interface configuration, start and stop Libraesva ESG Appliance and core system services and customize some system preferences.

Network Settings | Static Routes | Web HTTPS Certificate | SNMP Monitor | Syslog | API Services

Installed Certificate

MD5 Fingerprint:

Subject:

Issuer:

Let's Encrypt Certificate

Generate a certificate made by **Let's Encrypt** authority, accepted by all major browsers.

Common Name		Full ESG domain name
Email		Email address required to generate the certificate
RSA Key Size	2048	Size of the RSA encryption key

Generate

Certificate Request

To re-generate a new Self Signed Certificate or CA Request for you appliance, please fill the followings:

Country Code	IT	Your two-letter IANA country code
State or province		Your state or province name (NO SPACES)
Locality Name		Your town or city (NO SPACES)
Organization Name		Your organisation name (NO SPACES)
Organization Unit		A dot (period) is usually appropriate here (NO SPACES)
Common Name		The fully qualified name of your Libraesva ESG Appliance
Email Address		A valid email address that will be shown into the certificate.
Bits		The size of the private key to generate, in bits (1024,2048, etc)
Generate:	(•) Self Signed Certificate ( ) Certificate Request	Do you want to generate a self signed certificate or a certificate request?

Generate!

Wildcard Certificate

It is possible to upload your own Wildcard Certificate.
Please note that certificate must be in **Standard PEM - Base 64 format**:

Certificate File (.crt) Scegli file Nessun file selezionato

Key File (.key) Scegli file Nessun file selezionato

Upload

Self Signed Certificate / Certificate Request

To create a new Self Signed Certificate or CA Request for you appliance, please fill the followings:

- *Country Code Your two-letter IANA country code*
- *State or province Your state or province name (NO SPACES)*
- *Locality Name Your town or city (NO SPACES)*
- *Organization Name Your organization name (NO SPACES)*
- *Organization Unit A dot (period) is usually appropriate here (NO SPACES)*
- *Common Name The fully qualified name of your Libraesva ESG*
- *Email Address A valid email address that will be shown into the certificate*
- *Bits The size of the private key to generate, in bits (1024,2048, etc)*
- *Generate: Self Signed Certificate / Certificate Request*

Once filled all required information, press **Generate** button.

×**NOTE:** If you selected to generate a Certificate Request, you must paste back your certificate file once generated with your CA.

Wildcard Certificate

It is possible to upload your own wildcard Certificate. Please note that certificate must be in Standard PEM – Base 64 format, and both private key and certificate file are requested. Please select files:

- Certificate File (*.crt)
- Key File (*.key)

and press **upload** button.

Let’s Encrypt certificate

The process is completely automated. Once filled-in the required fields the certificate is issued and installed. Libraesva ESG web interface must be accessible from the internet.

The periodical renewal of the certificate is also automatic.

Let’s Encrypt certificates expire every 3 months. One month before expiration ESG

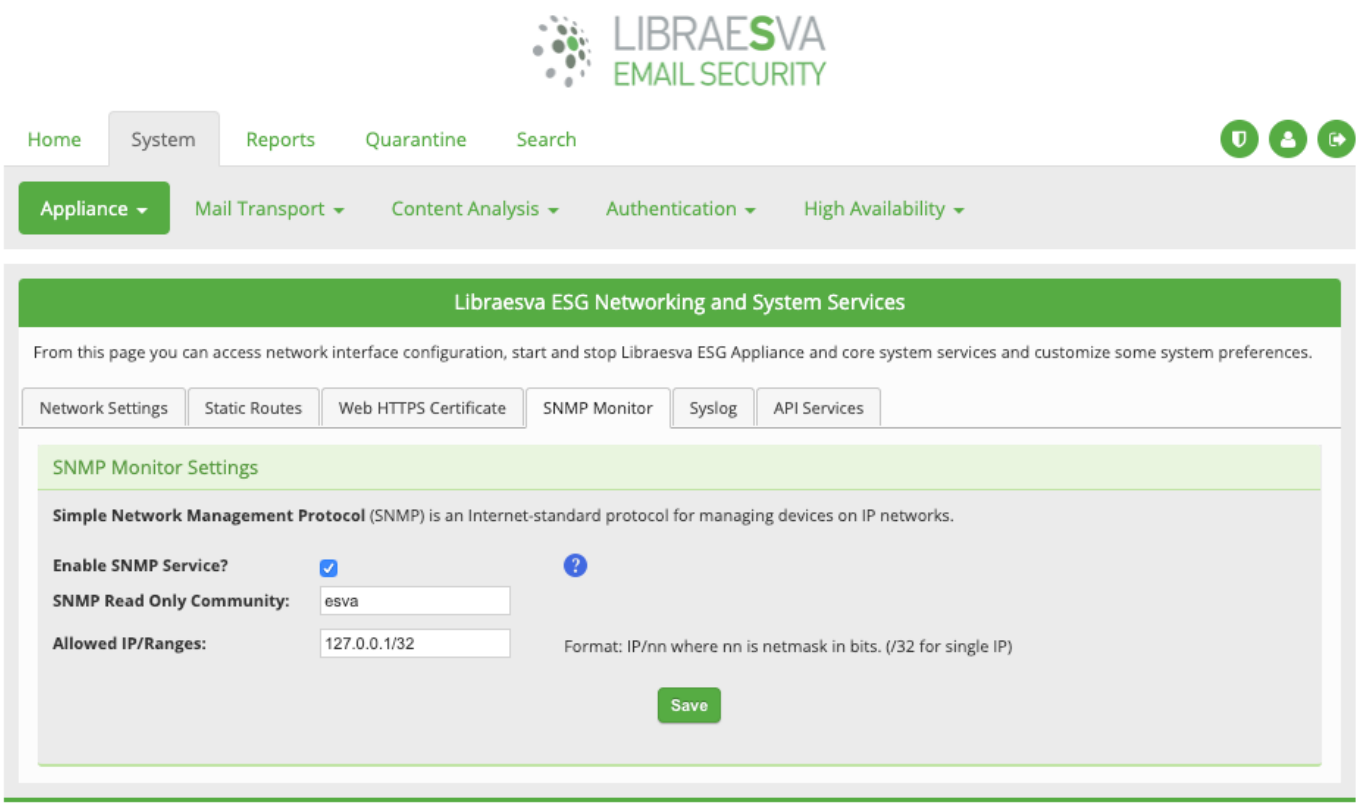
automatically renews the certificate. If the renewal fails for any reason (like a temporary networking issue), a new attempt is made one week later, and so on with a new renewal attempt every week.

20 days before the expiration you will get an email notification from Let's Encrypt, a new reminder will be sent 10 days before expiration and a final email notification as soon as the certificate expires.

×**NOTE:** Let's Encrypt requires port 80 opened, to verify the validity of the certificate request for the provided Hostname!

SNMP Monitor Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Libraesva ESG supports SNMP and can be monitored with an SNMP capable monitoring tool.



The custom Libraesva ESG variables you can monitor via SNMP are:

- **Mail Sent** (OID: 1.3.6.1.4.1.41091.1.1.1.0)
- **Mail Received** (OID: 1.3.6.1.4.1.41091.1.1.2.0)
- **Mail Rejected** (OID: 1.3.6.1.4.1.41091.1.1.3.0)

- **Mail Bounced** (OID: 1.3.6.1.4.1.41091.1.1.4.0)
- **Spam Messages** (OID: 1.3.6.1.4.1.41091.1.1.5.0)
- **Virus Messages** (OID: 1.3.6.1.4.1.41091.1.1.6.0)
- **Total Mail Queue** (OID: 1.3.6.1.4.1.41091.1.1.7.0)
- **Incoming Mail Queue** (OID: 1.3.6.1.4.1.41091.1.1.8.0)
- **Outgoing Mail Queue** (OID: 1.3.6.1.4.1.41091.1.1.9.0)
- **Cluster Status** (OID: 1.3.6.1.4.1.41091.1.1.10.0)

Mail counters report the number of new messages since the last SNMP query, the counter is zeroed at each query.

To start monitoring your installation you must Enable SNMP service from the screen above, declare a source IP Address / Network and define a community read only string to query the service.

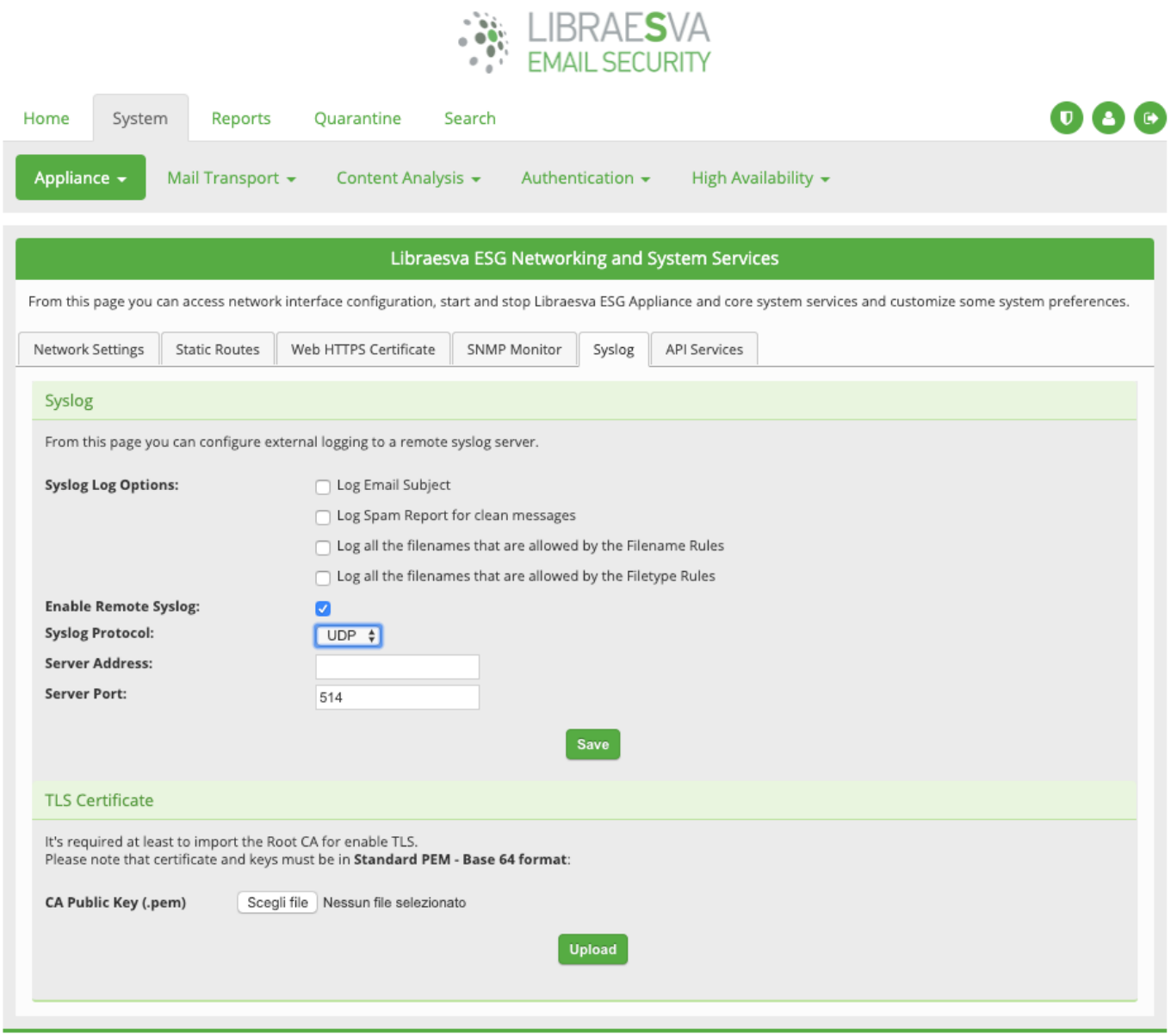
×**NOTE:** Libraesva ESG support SNMP protocol version 2c.

Syslog

Libraesva ESG can export all logs to a remote Syslog Server.

To configure it simply select Enable Remote Syslog, and specify your Syslog Server IP Address.

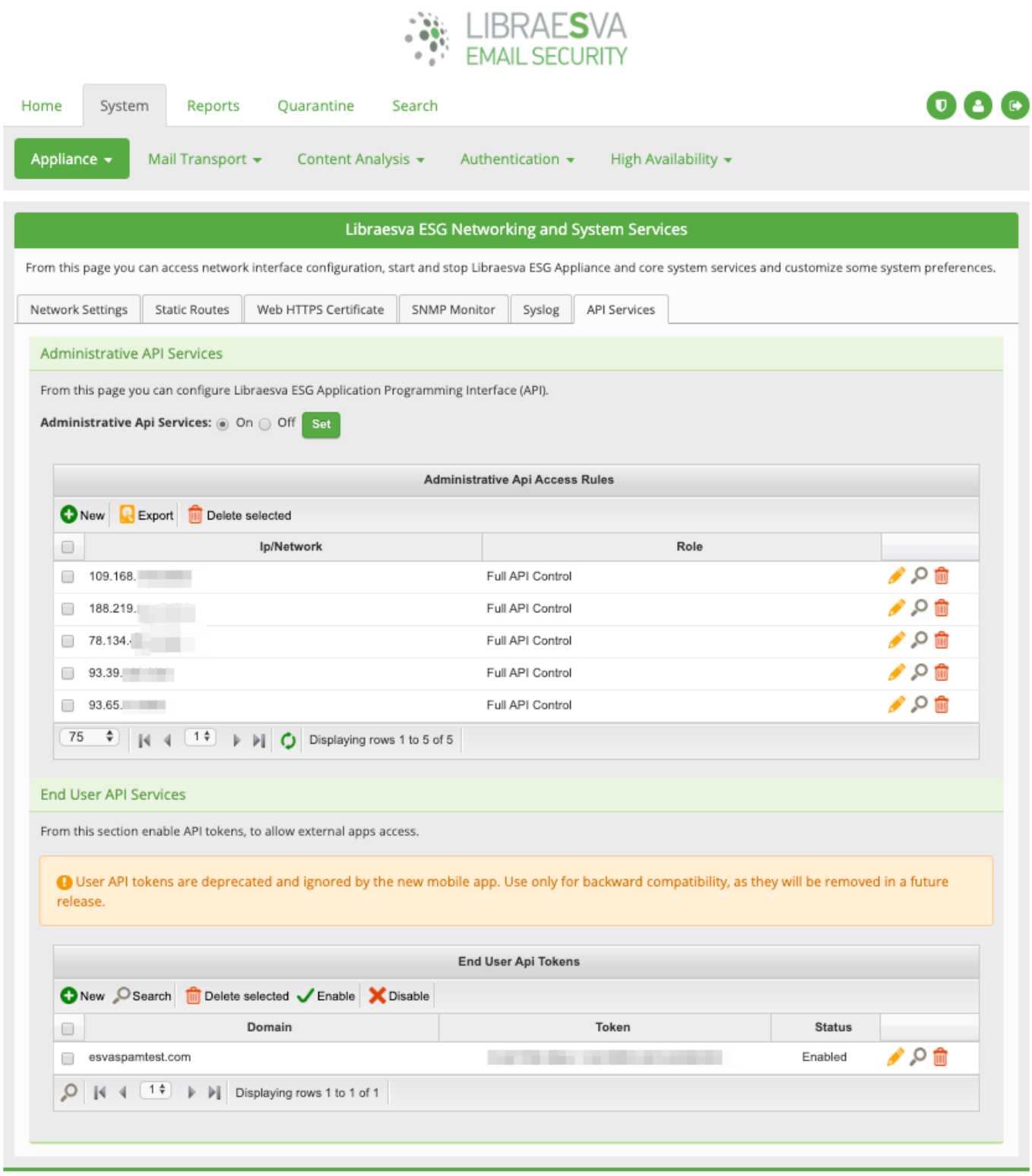
You can also improve security using a TLS certificate.



×**NOTE:** Libraesva ESG uses standard port UDP 514

API Services

From this page you can configure ESG Application Programming Interface (API) access rules. There are two kinds of API Services: Administrative API and End User ones.



Administratives API Services

You can Enable / Disable API Services and, when enabled, define access policies to API.

To add an Access Rule press **New** button and specify:

- Source IP/Network to grant access

- Role, as Read Only access to API or Full Access also to API that can modify your system

×**NOTE:** A full documentation of each function available through the API is available at the following link.

End User API Services

The End Users API Services are based on a per domain access token. That means the user needs both it's username and password an a valid token to access the service.

The Administrator can Enable/Disable API access to any of the authorized domains.

The Libraesva Personal APP (available for Apple IOS devices and Google Android ones) is using this service to connect to Libraesva ESG.

×**NOTE:** If you need to develop an application that uses End User API please contact us for the relevant API Documentation.

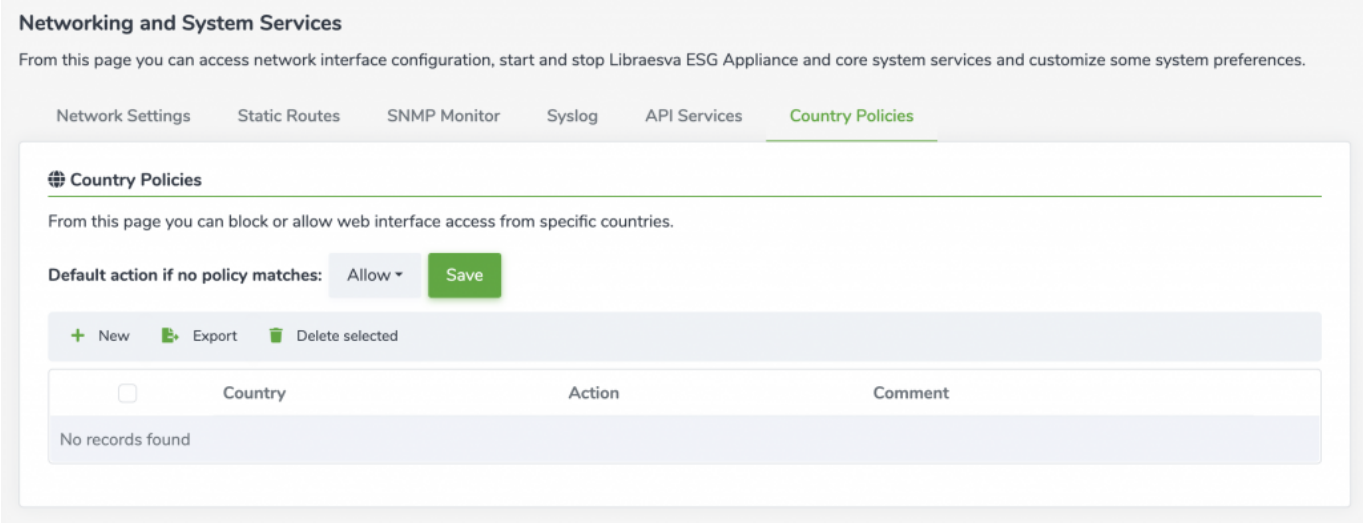
Country Policies

In both versions (v4.9 and v5) of ESG we added the "Country Policies" feature.

You can decide a list of allowed or blocked countries, and the default behavior if no policy matches.

The UI will be blocked preventing login from that countries.

Block is based on origin IP.



×**NOTE:** If you need to reset the block (if you made a mistake), you can log into console via SSH or from your hypervisor and reset the block.