
New in Secomea Release 16.0



Nice to know information about this release:

- Secomea TrustGate 16.0 build 17434 public 2017.10.28

Version: 1.0, 2017

NewInRelease16.0.docx

Contents

1.	TrustGate RELEASE 16.0	4
2.	IPsec AES-256 support	4
2.1.	IPSec Auto negotiation	4
2.1.1.	EasyTunnel	5
3.	Certificate upgraded from 1024 to 2048 bit key length	5
4.	TrustGate WEB server update	5
4.1.	Protocol and Ciphers	5
4.1.1.	The TrustGate web server (admin GUI) has been upgraded with support for the following:	5
4.2.	Web Server Certificate	6
4.3.	Upgrade Web Server Certificate	6
4.4.	GUI logout	7
5.	Web Proxy	7
6.	GateManager	8
7.	TrustGate 560R+	8
7.1.	To identify if you are running a TG560R or a TG560R+	8
7.1.1.	TrustGate 560R:	8
7.1.2.	TrustGate 560R+	8
8.	Mobile interface	8
8.1.	Diagnostics	8
8.2.	IMEI, IMSI and ICCID are shown	9
8.3.	Mobile broadband	9
8.4.	Broadband adapters	9
9.	WiFi Interface	10
9.1.	WiFi Client	10
9.2.	Static	10
10.	TrustGate SoftClient	10
10.1.	Windows 10 support	10
10.2.	DLL hijacking protection	10
11.	Additional fixes	10
11.1.	Watchdog	10
11.2.	Local Aliases	10
11.3.	DHCP Client perform IP check	10
11.4.	Traffic shaping	10
11.5.	Stability improvements	11
Appendix A		12
12.	Local Certificate and CA-certificate	12
12.1.	Pros and cons	12
13.	How to start using SHA-256/2048 bit Certificate	12
13.1.	Pre-Loaded Certificates	12

13.2. Trusted CA	13
13.3. On EasyTunnel Client	13
13.4. EasyTunnel Server	13

Change log

Version	Change log
1.0	Initial version

1. TrustGate RELEASE 16.0

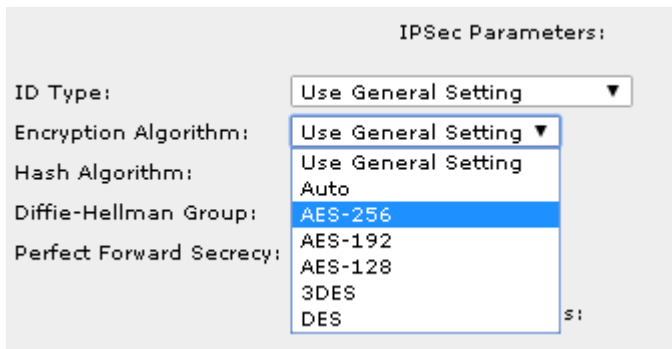
Release 16.0 includes several security related changes, details of which are not disclosed here. We strongly recommend that you upgrade your TrustGate to this release.

This document describes the new features and improvements since previous 15.0.15123 public release. Most bugfixes are not covered here, but a detailed list will be found in the public Release Note:

http://ftp.secomea.com/pub/releasenotes/TrustGate_Release_16.0_17434.txt

2. IPsec AES-256 support

The TrustGate IPsec engine has been upgraded to support AES-256/SHA-512.



Supported crypto and algorithms:

DES, 3DES, AES-128, **AES-192 (new)** and **AES-256 (new)**

MD5, SHA-1, **SHA-256 (new)**, **SHA-384 (new)** and **SHA-512 (new)**

DH1, 2, 5 and **DH 14, 15, 16, 17** and **18 (new)**

IKEv1 (IKEv2 has yet to come).

TrustGate is still using Tunnel-mode/Main-mode and Aggressive/Quick-mode is not an option.

Notice that the AES-256 will require more CPU load and will decrease the IPsec performance.

2.1. IPsec Auto negotiation

Previous release:



Release 16.0:

Default Encryption Algorithm:	Auto ▼
Default Hash Algorithm:	Auto ▼
Default Diffie-Hellman Group:	Auto ▼
Default Perfect Forward Secrecy:	On ▼

The option “Any” has been altered to “Auto”. With the new supported algorithms, there are 400 combinations and it would be too much to try them all, so in Auto mode we limit the proposals as the tables below will show.

Proposal	TrustGates	Encryption	Hash Algorithm	Diffie-Hellman groups
#1A	TG164, 264, 460R, 560R	AES-256, AES-128	SHA-512, SHA-256	DH15, DH14
#2	-----“”-----	AES-128, 3DES	SHA-256, SHA-1	DH5, DH2
#1B	TG60, 61, 62, 160, 260	AES-256 , AES-128	SHA-512, SHA-256	DH15, DH14
#2	-----“”-----	AES-128, 3DES	SHA-256, SHA-1	DH5, DH2

In Auto mode, the TrustGate will cover any of the combinations in both #1 and #2 proposal. TrustGate 6x and TrustGate x60 will not include the AES-256 in its Auto modes.

DES, MD5 and DH1 have been removed from the auto mode proposals - all are considered unsafe, but can still be configured manually.

2.1.1. EasyTunnel

The EasyTunnel tunnel will default to the highest encryption included in the Auto proposal. This means a TrustGate 62 as EasyTunnel Server will use proposal #1B from the table above. A TrustGate 264 will be using proposal #1A from the table above.

In any case, if the EasyTunnel Client is NOT upgraded to release 16.0 it will use proposal #2 from the table above.

3. Certificate upgraded from 1024 to 2048 bit key length

The TrustGate certificate engine has been upgraded to support SHA-256 and RSA-2048 for both local Certificate and the build in CA-server.

The certificate is used in tunnel negotiation and for the web interface (see next chapter).

A new installed TrustGate will automatically use the upgraded certificate, but upgrading the firmware on an already configured TrustGate, will not automatically upgrade the certificates.

IMPORTANT! Before you upgrade the Web Certificate you should read **Appendix A** that covers what to pay attention to before upgrading the certificates.

4. TrustGate WEB server update

4.1. Protocol and Ciphers

4.1.1. The TrustGate web server (admin GUI) has been upgraded with support for the following:

TLS 1.2 protocol, Ciphers like RSA-2048, DHE-2048 and ECDHE-256. Weak ciphers have been removed see Release Note for details.

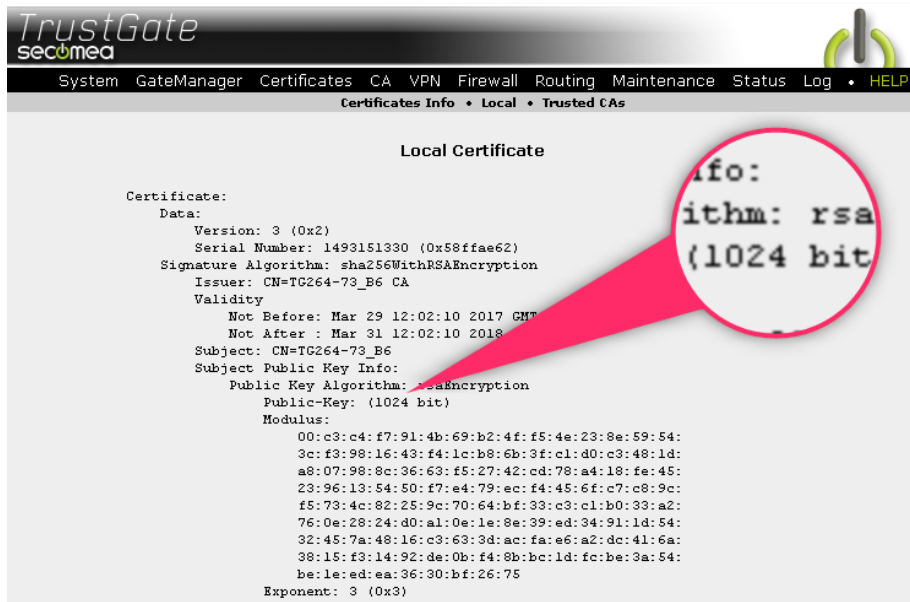
4.2. Web Server Certificate

The TrustGate web servers public key has been increased from 1024 to 2048 key length.

The WEB Certificate is not upgraded automatically on firmware upgrade but will have to be created manually. Creating a new Local Certificate will upgrade the WEB server certificate to use SHA-256 and RSA-2048.

IMPORTANT! Before you upgrade the Web Certificate you should read **Appendix A** that covers what to pay attention to before upgrading the certificates.

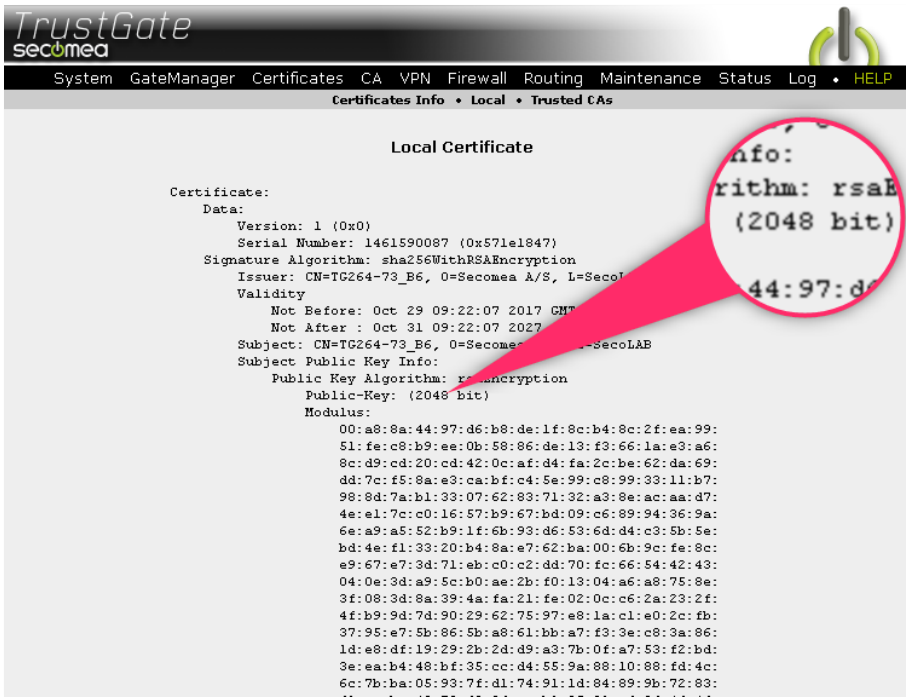
4.3. Upgrade Web Server Certificate



Create a 2048 bit key certificate by pressing the NEW button and follow the wizard.

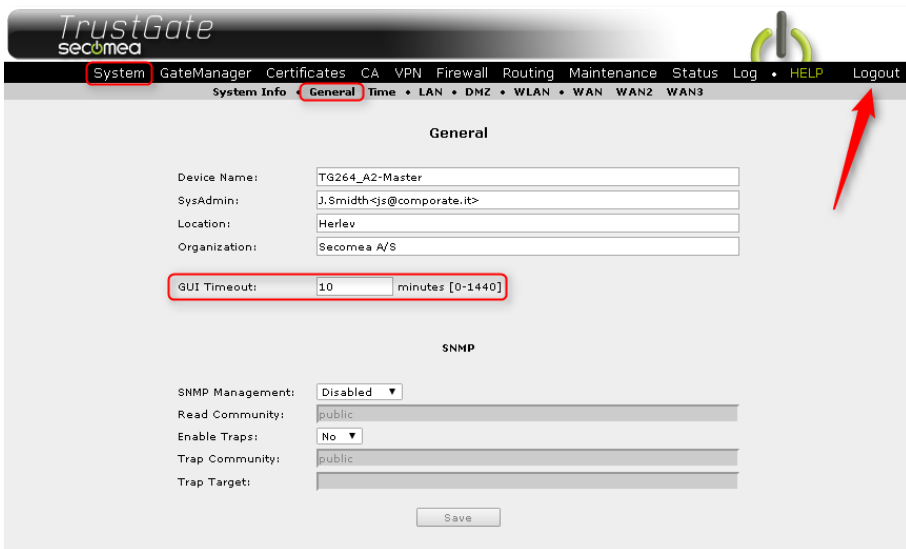


This should bring up a certificate as shown below:



The Web server is now SHA256/RSA-2048 enabled.

4.4. GUI logout



New GUI logout can be configured on the page “SYSTEM > General” if the default 10 minutes logout is not enough.

The logout option is only available when logged in locally with the admin account. When using the [TrustGate GUI] button from the GateManager portal, the logout option is not needed.

5. Web Proxy

The Web Proxy now includes auto configuration (WPAD) support, and has been modified to use two distinct ports for explicitly forwarded requests (port 3128) and transparently intercepted requests (port 8080), respectively. In previous firmware versions, port 8080 was used for both kind of requests. If you have manually configured your browser to use port 8080, you should change it to use auto configuration (WPAD) instead. Alternatively, reconfigure it to use

port 3128 instead. No action is needed for Destination NAT rules that intercept web requests and redirect these to port 8080.

No changes have been made to the Web Proxy interface.

6. GateManager

The GateManager connection has been upgraded to support the latest GateManager enhanced protection. The connection to the GateManager will now guard against appliance spoofing. This requires GateManager Server 7.3 or higher.

If you are using GateManager for remote Access to the TrustGate:

- if you, for some reason, need to downgrade the TrustGate to pre-16.0 firmware, you should do it from the GateManager. If downgrading from the TrustGate GUI, you will have to perform an unlock from the GateManager Portal to overcome the spoofing protection, see your GateManager documentation for more details.

7. TrustGate 560R+

Release 16.0 includes support for TG560R with improved CPU performance. All new TG560R+ will be released with an Intel i5 CPU that improve performance.

The IPsec performance has been improved by a factor 2. To be able to keep appx. 1 Gb/s IPsec speed using the new AES-256 encryption. The previous TG560R will still be able to keep the listed speed when using AES-128 as available on release date for that product.

7.1. To identify if you are running a TG560R or a TG560R+

After a reboot, the system log will show the following line:

7.1.1. TrustGate 560R:

```
kern.info smpboot: CPU0: Intel(R) Pentium(R) CPU G2130 @ 3.20GHz (fam: 06, model: 3a, stepping: 09)
```

7.1.2. TrustGate 560R+

```
kern.info smpboot: CPU0: Intel(R) Core(TM) i5-3550S CPU @ 3.00GHz (fam: 06, model: 3a, stepping: 09)
```

8. Mobile interface

8.1. Diagnostics

The Menu has moved from “Status > Diagnostics” to “WAN2/3 > Diagnostics”.

There have been implemented improved Hardware Information and more correct test data.


```

===== Mobile network test =====
Mobile Scan

Last scan: Sun Oct 29 16:09:52 2017

-- FW Information --
v1560_17437

-- HW Information --
HUAWEI_MOBILE MS2372h-153; Rev.: 21.327.07.00.00; IMEI: 866129030007868; IMSI: 238201009434609; ICCID: 89450403160715346090

-- SIM card Information --
SIM IMSI: 238201009434609
SMS service center: +4528187000

-- Mobile networks --
Test 1: Network scan for available networks
Network name      Short name      Network number  Mode    Status (roaming)
Telia DK          Telia           23820           4G      current
Telia DK          Telia           23820           3G      available
TDC               TDC             23801           4G      forbidden
Telenor DK        TelenoDK        23802           4G      available
3 DK              3 DK            23806           4G      available
3 DK              3 DK            23806           3G      available
Telenor DK        TelenoDK        23802           3G      available
TDC               TDC             23801           3G      forbidden
TDC               TDC             23801           2G      forbidden

Test 2: Error: Could not deregister!

-- Mobile network signal and cell ID tests --
Test 3: Register to default network (auto mode) and show status every 5 seconds 5 times
Network name      Network number  Registration status  Location Area  Cell ID  Mode  Signal (0-31)
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22

Test 4: Register to default network with GSM/2G and show status every 5 seconds 5 times
Network name      Network number  Registration status  Location Area  Cell ID  Mode  Signal (0-31)
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    21
TeliaDK           23820           Registered, home network  24043         0        4G    21
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22
TeliaDK           23820           Registered, home network  24043         0        4G    22

Test 5: Register to default network with UMTS/3G and show status every 5 seconds 5 times

```

8.2. IMEI, IMSI and ICCID are shown

```

Last heartbeat: 2017-10-29 18:55:28 (50 seconds ago) Next: 19:05:24 (in 08:52)
-----
Date/time: 2017-10-29 18:46:38
Uptime: 1 hour 8 minutes 10 seconds
WAN port: 192.56.1.1/255.255.255.0 (DOWN)
WAN2 port: 192.56.2.1/255.255.255.0 (DOWN)
WAN3 port: 10.222.146.73/255.255.255.255 (UP)
LAN port: 172.16.99.201/255.255.255.0
DMZ port: 192.56.3.1/255.255.255.0
DMZ2 port: 192.55.1.2/255.255.255.0
DMZ3 port: 192.55.3.1/255.255.255.0
Expansion Slot: 4G [TeliaDK]; Signal: 23
SIM ICCID: 89450403160715346090
SIM IMSI: 238201009434609
Modem IMEI: 866129030007868
System Temp.: 39.0°C
CPU Temp.: 50.5°C
CPU Load: 0.2%
GateManager Address: gm4260secolab.dyndns.org 94.18.233.169
Power Supply: #2: ok #1:
Fan Speed: #4: 2393 RPM #3: 585 RPM #2: 2428 RPM #1: 2481 RPM

```

An inserted Mobile Broadband adapter will show various information in the GateManager Portal:

ICCID: Integrated Circuit Card ID (the number printed on the SIM Card).

IMSI: International Mobile Subscriber (identifying your ISP)

IMEI: International Mobile Equipment (the serial number on the modem).

8.3. Mobile broadband

General name changes from 3G to Broadband have been made to cover 3G/4G and LTE.

8.4. Broadband adapters

Added support for more Mobile Broadband USB adapters like Huawei MS2372h-153 LTE and many others.

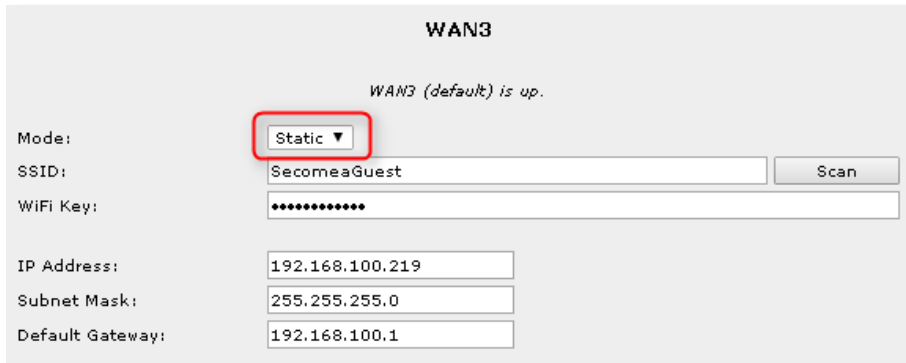
9. WiFi Interface

9.1. WiFi Client

Several improvements made for the WiFi Client mode to improve stability.

9.2. Static

Support for Static IP on WiFi interface in case the AP has no DHCP service.



The screenshot shows the WAN3 configuration page. At the top, it says "WAN3" and "WAN3 (default) is up.". Below this, there are several configuration fields. The "Mode:" field has a dropdown menu with "Static" selected, which is highlighted with a red box. Other fields include "SSID:" with the value "SecomeaGuest" and a "Scan" button, "WiFi Key:" with a masked password, "IP Address:" with "192.168.100.219", "Subnet Mask:" with "255.255.255.0", and "Default Gateway:" with "192.168.100.1".

10. TrustGate SoftClient

10.1. Windows 10 support

Drivers have been digital signed by Microsoft approved authority to fully support any Windows 10 versions including secure boot, Anniversary and Creators updates.

10.2. DLL hijacking protection

Improved protection of SoftClient installer against DLL hijacking.

11. Additional fixes

11.1. Watchdog

Improved watchdog system. Several optimizations have been made to the watchdog to ensure system will reboot correctly on ACM (GateManager connection) failure.

11.2. Local Aliases

You can now use LAN, DMZ, DMZ2 and DMZ3 as aliases for the respective interfaces in various tables and fields where it is already possible to enter a DNS name. Firewall and NAT tables are obvious.

11.3. DHCP Client perform IP check

The DHCP Client now check for address in use and perform a decline that enable the DHCP server to abandon the IP and release a new IP for the DHCP Client. This helps preventing IP conflict on the local network.

11.4. Traffic shaping

The QoS queueing is using FQ CoDel algorithm (rather than FIFO) on each individual QoS queue to improve latency for interactive sessions during high load. In other words – an attempt to improve traffic shaping when you have

configured the Rx/Tx parameter on the WAN interface. New connections (opening a browser, DNS requests and so on) should be more reliable on high loaded networks.

11.5. Stability improvements

Several bugfixes have been made regarding potential memory leaking.

Release Note

A Complete list of bugfixes are listed in the public Release Note text file.

http://ftp.secomea.com/pub/releasenotes/TrustGate_Release_16.0_17434.txt

Appendix A

12. Local Certificate and CA-certificate

The TrustGate certificate engine has been upgraded to support SHA-256 and RSA-2048 for both local certificate and the build in CA-server. The Local certificate is used for the X509 enabled tunnels but also the TrustGate web interface.

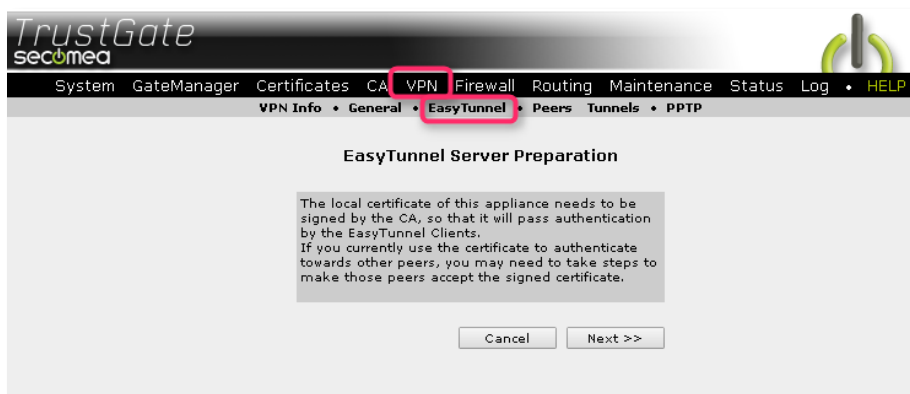
12.1. Pros and cons

Using RSA-2048 on the local certificate will increase the security level of the WEB certificate and the tunnel authentication. The WEB certificate is usually not exposed to the internet (local firewall block for TCP:443) but sometimes it is and then it is an important to upgrade to RSA-2048.

The tunnel authentication part is a needed security upgrade and should be performed.

It is important to notice that changing the Local Certificate require all VPN tunnels using Pre-loaded Certificates to be updated with the new certificate. If using Trusted CA you have to update the remote sites trusted CA list with the new certificate.

If your setup is a EasyTunnel set up the system will automatically request the necessary certificate and all actions will be handled by the system. You just have to select the EasyTunnel menu and you will be prompted the ET Wizard.



13. How to start using SHA-256/2048 bit Certificate

13.1. Pre-Loaded Certificates

Are you using Pre-loaded Certificates on your tunnels you create a new Local Certificate and distribute the new certificate to all remote sites.



Peer shown GREEN Icon is using Pre-Loaded Certificate.

Select Certificate > Local

Press [New] button:



Press [Create] and follow the guiding on the screen.

The TrustGate should end up having a new Local certificate with a SHA-256/RSA-2048 enabled certificate.

This certificate must be distributed to all remote sites having a PEER to this TrustGate.

In the same process, the local web certificate has been upgraded because the web server is using the local certificate.

13.2. Trusted CA

Create a new Local Certificate on the TrustGate and get this certificate re-signed by the CA server. The new signed certificate is re-installed on the TrustGate and no further action is needed.

In same process, the local web certificate has been upgraded because the web server is using the local certificate.



Peer using Trusted CA.

13.3. On EasyTunnel Client

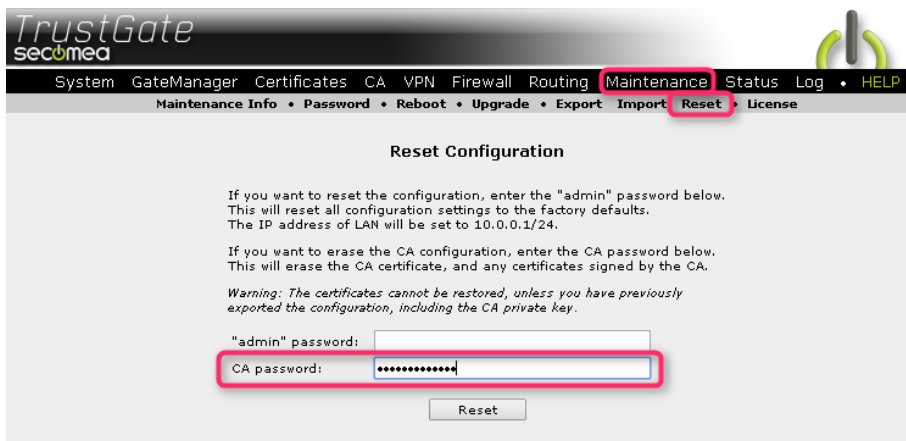
Create a new Local Certificate, as in chapter 13.1 and delete the EasyTunnel servers certificate located in Trusted CA. This will automatically make the local certificate signed by the EasyTunnel server on the next tunnel rekey. Easy step is simply to reboot the TrustGate.

In same process, the local web certificate has been upgraded because the web server is using the local certificate as Web Server Certificate.

13.4. EasyTunnel Server

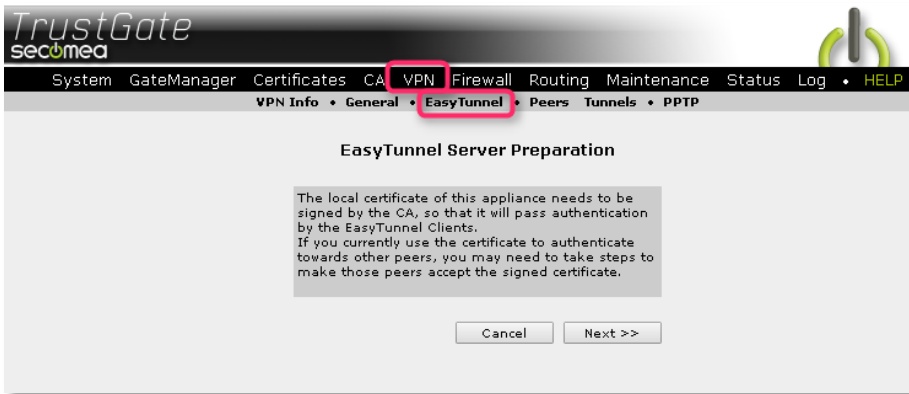
Both the Local Certificate (see chapter above) and the CA-Server should be renewed to increase security to the highest level.

The CA-server certificate is renewed by resetting the CA-Server select: Maintenance > Reset and ONLY type in the CA password as shown below:



Enter only the CA password to reset the CA server certificate.

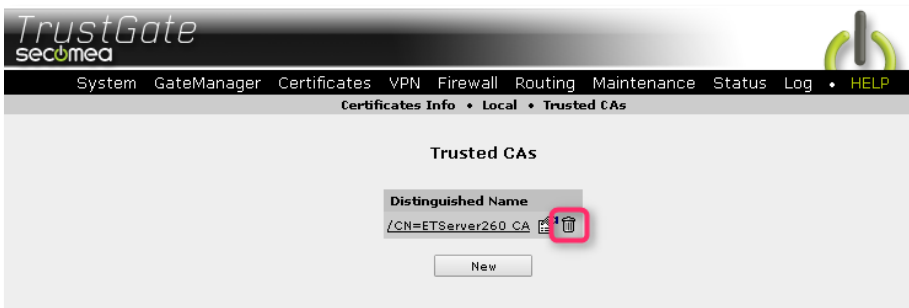
Select VPN > EasyTunnel and follow the EasyTunnel wizard to make all the necessary certificate signing automatically executed.



Now the EasyTunnel server is up to date with the latest SHA256/RSA-2048 certificate.

IMPORTANT! All the ET-Clients tunnels will fail and they will need to get re-signed as well. This is easily done simply by deleting the Trusted CA in the ET-Clients Trusted CA list. Reboot the client and the system will automatically get reestablished with all new certificates.

On each EasyTunnel Client locate the Trusted CA and delete the EasyTunnel Server certificate, reboot the EasyTunnel client or just rekey the tunnel.



Delete the Trusted CA certificate on all ET-Clients.

Secomea A/S
Denmark
CVR No. DK31 36 60 38
Email: support@secomea.com
www.secomea.com