SSL Smart Security Scan
Virtual appliance
admin manual

Company	KeyTalk IT Security
Author	MR van der Sman
Creation date	12 March 2019
Last updated	23 February 2022
Product	KeyTalk SSL Smart Security Scan virtual appliance (certificate discovery, SSL related vulnerability scanner, advanced network vulnerability scanner)
Data classification	Public
Software/firmware version	6.4.2
Manual version	6.4.2.5

Contents

1. Quickguide Introduction and download

The KeyTalk SSL Smart Security Scanner virtual appliance is meant to periodically scan a given network (internal and/or external facing) on a range of ports or FQDNs for active certificates, and provide the admin running the scan, with insight information as to which roots, Intermediate CAs, issuing CAs and end-point certificates are actually in use, and more importantly show the relevant certificate meta data.

The scanner scans each found end-point for known SSL related vulnerabilities and will report on these accordingly when found using colour coding in the output report.

Our offered SSL Smart Security Scan virtual appliance runs either inside or outside your network, and does NOT share any of its scan data with external parties, nor will it share the data with the company KeyTalk.

The admin can choose to have the scan result data be sent in raw JSON format to a given target over TLS 1.2 for further processing, such as to the KeyTalk Certificate and Key Management Solution virtual appliance. The KeyTalk SSL Smart Security Scan virtual appliance will also provide a readable format report in HTML (print to PDF), as it is stored on the SSL scanner server for archiving purposes.

While the KeyTalk SSL Smart Security Scan has its roots in Nmap, it goes well beyond the free publicly available version of Nmap, since Nmap does not:

- Offer the same certificate scan speed of over 1 port per 0,001 second
- Take into account Network Intrusion Detection Systems and attempts to bypass them
- Actually analyse found end-point certificate data
- Report on CA chains belonging to the found end-point certificates
- Support scanning of Server Name Indication hosts
- Postback scan data in raw JSON output to a target
- Support scheduled scanning
- Optionally do CVE scanning

In addition to reporting on certificate lifetime, CN, SAN etc, the KeyTalk SSL Smart Security Scanner currently also analyses for the following SSL vulnerabilities per end-point:
"Hostname Validation"
"Android CA Store support"
"iOS CA Store support"
"Java CA Store support"
"macOS CA Store support"
"Mozilla CA Store support"
"Windows CA Store suport"
"Symantec 2018 Deprecation"
"Verified CA Chain"
"Verified Chain contains MD5"
"Verified Chain contains SHA1"
"OCSP Status"
"Certificate Transparency check"
"CRL status"
"TLSV1 Cipher Suites"
"SSLV3 Cipher Suites"
"TLSV1_1 Cipher Suites":
"0":"Forward Secrecy",
"1":"RC4",

"2":"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"3":"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"4":"TLS_RSA_WITH_AES_256_CBC_SHA",
"5":"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"6":"TLS_RSA_WITH_AES_128_CBC_SHA",
"Resumption Support With Session IDs"
"Resumption Support With TLS Tickets"
"ROBOT Attack"
"Heartbleed"
"Client-initiated Session Renegotiation"
"Secure Session Renegotiation"
"OpenSSL CCS Injection"
"TLS/SSL Downgrade Attacks"
"Deflate Compression"

2. Quickguide Resource requirements

The KeyTalk SSL Smart Security Scan virtual appliance is based upon CentOS 7 and requires:

- ✓ 30 GB diskspace (disk 1) + 40 GB diskspace (disk 2)
- ✓ 4 CPU's with 1 core each
- ✓ 16 GB memory
- ✓ 1 IPv4 and/or IPv6 address (default assigned through DHCP)

Virtual appliance formats:

- OVF/VMDK compatible with ESXi, VMware Workstation, AWS (also available as AMI)

Firewall information:

	Port		**Function**
Default Gateway	n.a.	In/out	Gateway
IP Address	443	Inbound	Management interface: https://<IP> https://<FQDN>
	443	Outbound	Network HTTP Proxy when applicable
	22	Outbound	SSH based firmware upgrade fetch from bitbucket.org
	any	Outbound	Scan target port

3. Quickguide initial setup

This guide assumes that the person operationalizing the KeyTalk SSL Smart Security Scan virtual appliance, has sufficient knowledge of the Hypervisor/Cloud environment on which the virtual appliance is being deployed on. As such the steps to enable the KeyTalk Smart Security Scan virtual appliance on a Hypervisor/Cloud are not described.

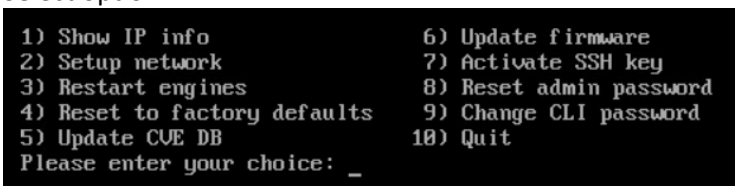
3.1 Assigning IP / Networking

Once the virtual appliance has been activated, a DHCP based IP address will be assigned.

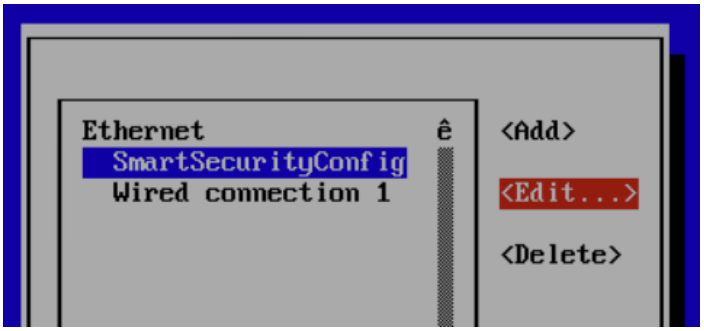
Should DHCP not be applicable, the admin can assign networking details manually, by using the following steps:

a) Login into the Command Line Interface using:
Username: client
Password: change!

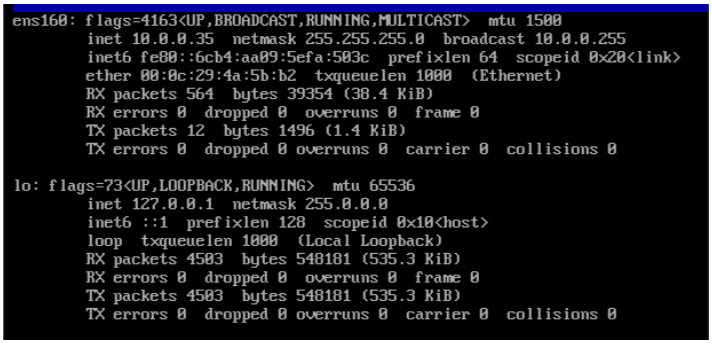
b) Select option 2



c) Apply the appropriate network settings when not using DHCP, by editing the connection:



After making appropriate changes and selecting OK, network config settings and assigned IP will be shown:

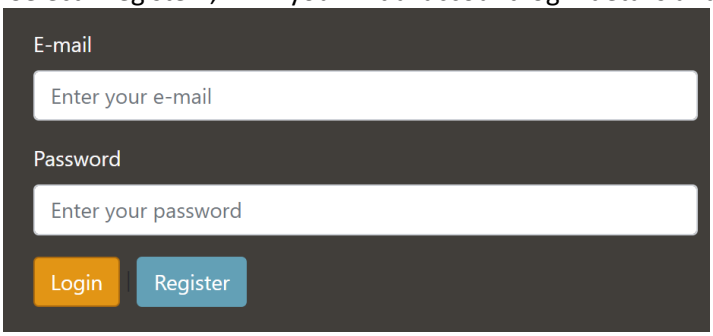


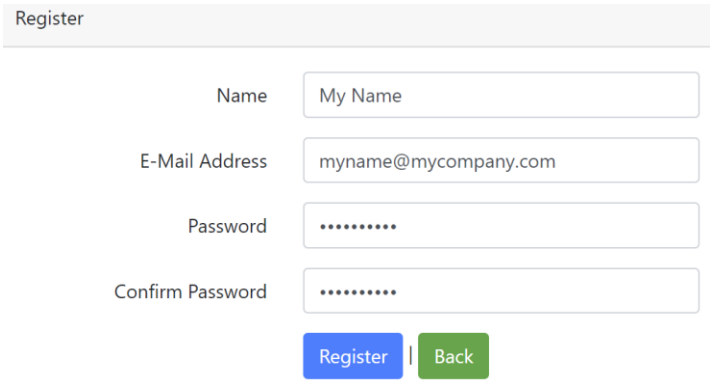
d) Open a browser and go to: https://<IP> or https://<FQDN>

NOTE: Because the KeyTalk SSL Smart Security Scan virtual appliance comes with a factory default self signed certificate, your browser will give a warning. Provided that company policy allows for it, ignore this warning and continue, allowing you to configure a proper SSL/TLS/HTTPS certificate during the next steps.

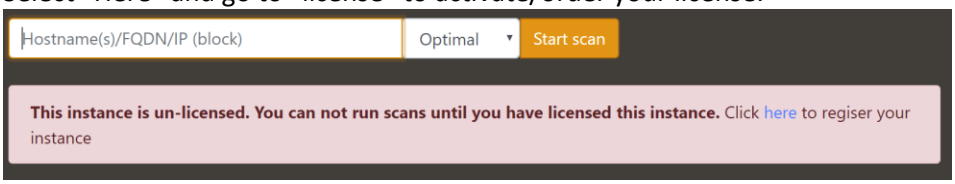
3.2 Registering and activating the scanner license online and offline

e) Select "Register", fill in your initial account login details and select Register again:

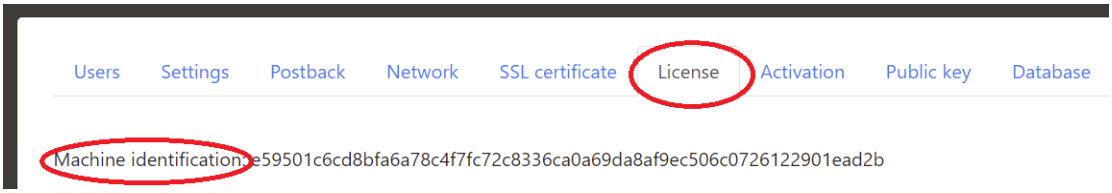




f) Select "Here" and go to "license" to activate/order your license:

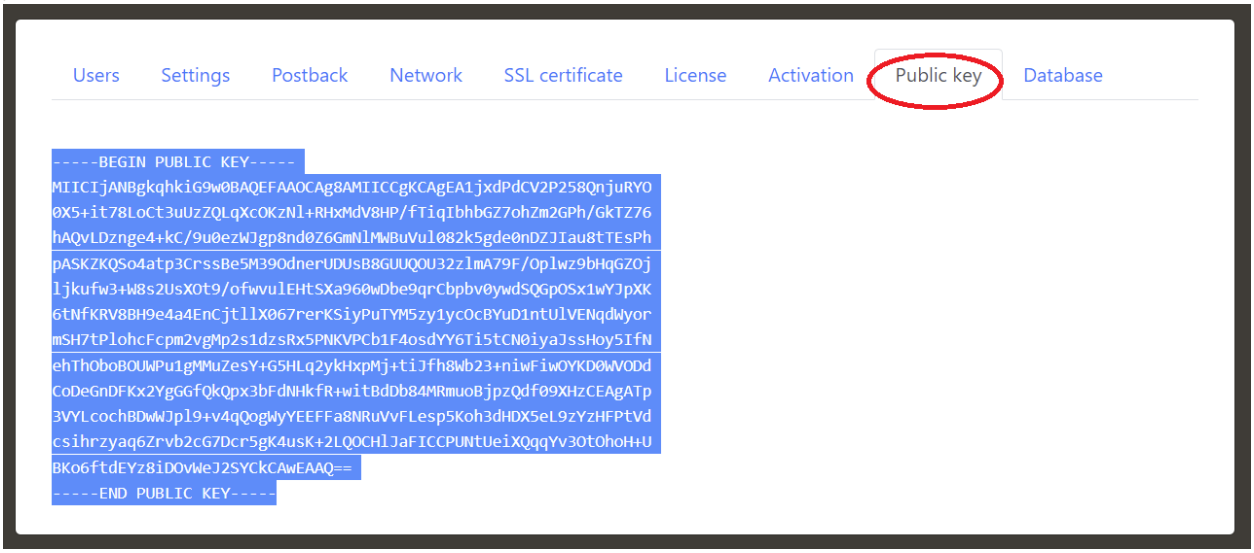


Now copy your 64 character alphanumeric machine identification number and note it in an email. It will look similar to
e59501c6cd8bfa6a78c4f7fc72c8336ca0a69da8af9ec506c0726122901ead2b



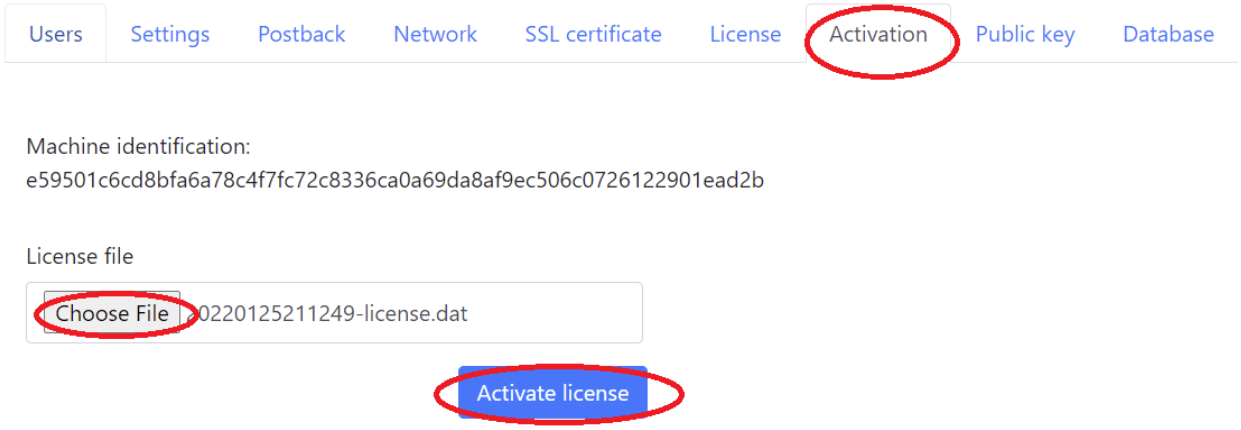
Next select your machines unique public key starting with
`-----BEGIN PUBLIC KEY-----`
Up to
`-----END PUBLIC KEY-----`

, and note it in an email:



Send your license request machine identification and Public Key by email to license@keytalk.com to request your license.

g) As soon as you receive your KeyTalk SSL Smart Security Scanner license, upload it under activation, and your Scanner will become operational:



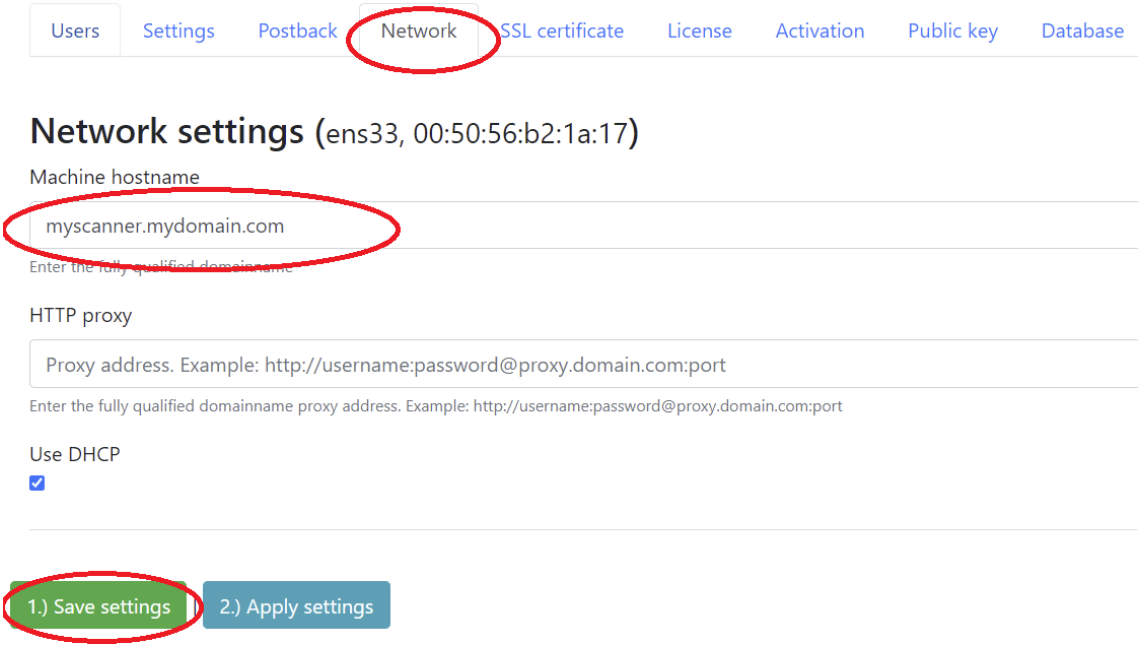
3.3 Enabling proper HTTPS

By default your KeyTalk SSL Smart Security Scan virtual appliance comes with a factory default self signed certificate

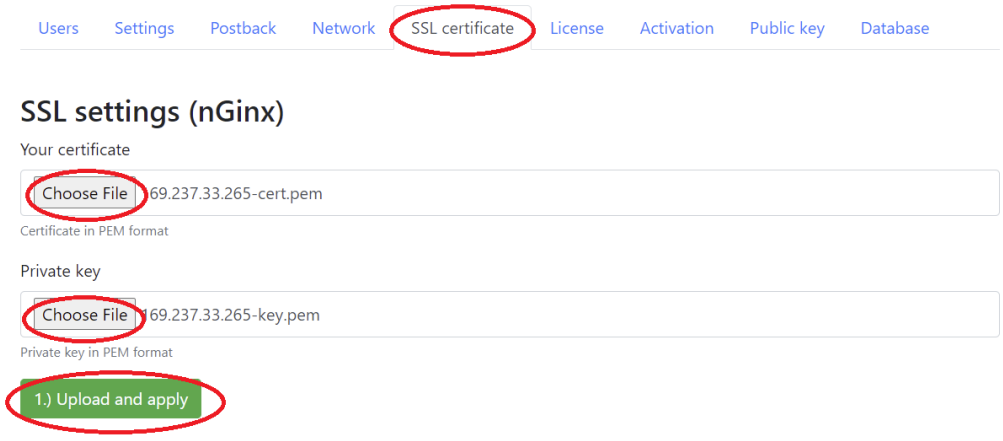
To enable a proper trusted HTTPS connection, you will need to provide the virtual appliance with a certificate issued by a Certificate Authority trusted by your (corporate) device(s), and which contains at least a proper Fully Qualified Domain Name as a DNS entry in the SAN value of the certificate.

h) This release of the virtual appliance does not support the KeyTalk automated certificate management protocol yet. To manually upload a valid certificate and key order one, either directly from your CA, or through your KeyTalk solution. And ensure both the key and the certificate are available in PEM format. (in KeyTalk CKMS download it as PEM and split the certificate file into a key and a certificate part)

i) Configure the KeyTalk Smart Security Scanner Fully Qualified domain Name



j) Upload and apply the certificate and key under SSL Certificate, and ensure the configured FQDN matches with the uploaded certificate SAN DNS entry

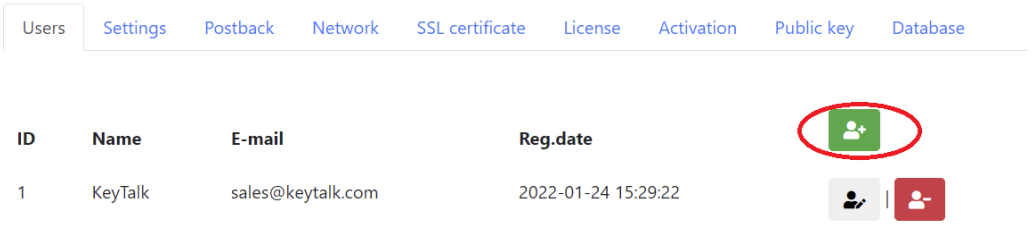


3.4 Create additional users allowed to perform scans

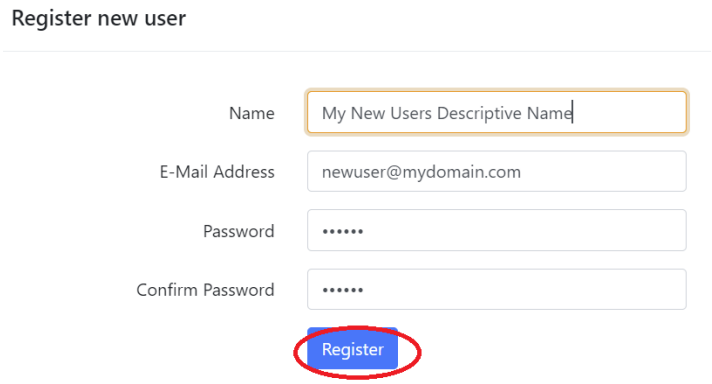
To allow multiple people or teams in your organization to perform network SSL scans, you can create multiple users. Your first user is your admin. The other accounts can only start scans.

Each made scan can only be seen by said user, as well as by the Admin.

k) Select the green + and enter relevant details



Define the user details and register the user



3.5 Performing your scan

Select the Smart Security Scan logo, or go to https://<IP> or https://<FQDN> to perform your first scan.

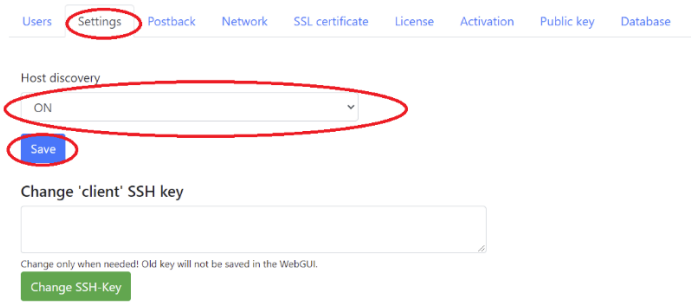
l) Enter the hostname, or FQDN, or IP address you wish to scan.

Separate each hostname/FQDN/IP by a space to scan multiple targets.
Example: www.keytalk.com downloads.keytalk.com smime.keytalk.com

Add a – to enable a range to be scanned
Example: 192.168.1.1-24
10.0.0.1-12 10.0.0.100-199

m) Select the port range you wish to scan for:
- ✓ Local Only = Scans all local certificate stores based on end-point which have the Smart Security Scan agent deployed to them
- ✓ Optimal = ports 1-1500
- ✓ Full = all ports (65.535)
- ✓ Bacnet = scans for SSL certificates based on the Bacnet (IoT) protocol
- ✓ Scheduled enables regular scanning

n) When scanning based on FQDN, switch off HOST DISCOVERY.
This feature primarily exists for IP(v4) based scanning and will result in the DNS being queried for corresponding A records, which in turn will be used to scan for additional SSL certificates.



IMPORTANT!!!

It is highly recommended, to initially scan a single IP or hostname, so see how much time a single OPTIMAL scan takes in your network (affected by latency, Intrusion Detection Solutions etc.) followed by a single IP scan using FULL ports.

After the single scan perform a smaller range scan, for example 10-20 Ips before doing larger ranges.

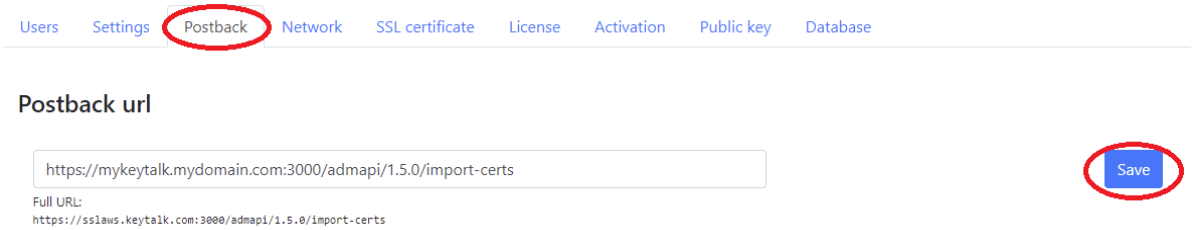
Doing an immediate large range, for example: .1-254 on all ports, will likely take a significant amount of time (sometimes multiple days) as not only are all ports scanned for SSL certs, but also common SSL vulnerabilities are being scanner for on each port and each given IP.

Should you have a need for large amounts of (daily) scans, contact KeyTalk to see how we may assist in getting multiple scanners setup to run in parallel.

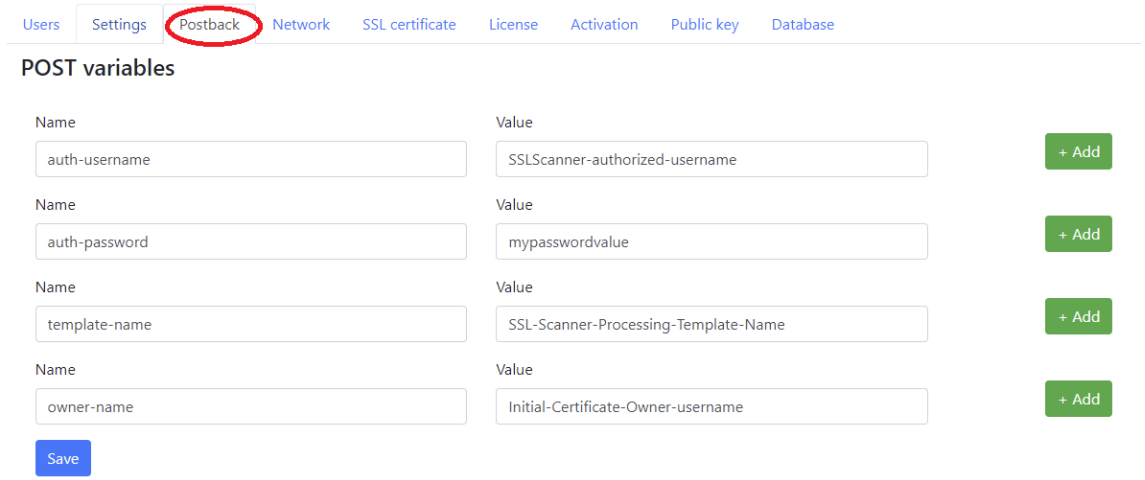
3.6 Scan data (Raw JSON) output for analysis and further processing

The KeyTalk Smart Security Scan virtual appliance enables its full scan data to be sent to a target server in raw JSON format

To enable this feature, simply add the preferred and valid postback url under:



After saving the URL configure the POST variables:



When the target server to send the scan data to is a KeyTalk CKMS server, use the following url construct:
https://*<FQDN>*:3000/admapi/1.5.0/import-certs

The following POST vales are REQUIRED when using a KeyTalk CKMS as the target (case sensitive):

POST Name	**POST Value**
auth-username	<as defined in your KeyTalk instance>
auth-password	<as defined in your KeyTalk instance>
template-name	<as defined in your KeyTalk instance>
owner-name	<as defined in your KeyTalk instance>

To view the found raw JSON scan data select the report you wish to examine and add ***?raw*** behind the report url

A JSON beautifier such as https://jsonformatter.curiousconcept.com/ can make the JSON data more readable

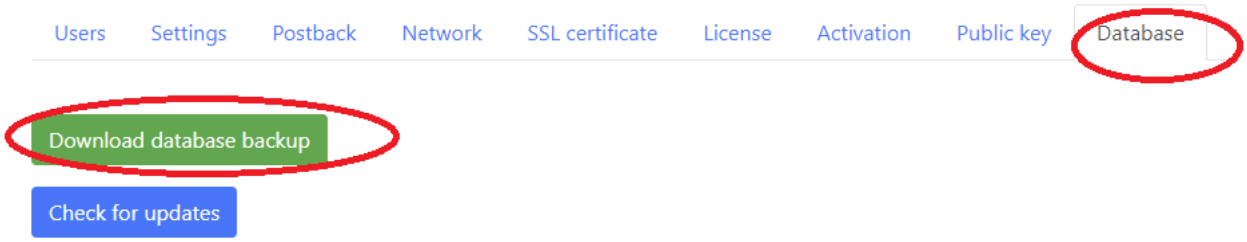
NOTE: Each user can have its own Postback settings, allowing each user's scans to go to its own target. In the case of using a KeyTalk CKMS, this means that each scan can go to its own template, thus allowing separate DevOPS teams to have their own data set to work with.

When no unique Postback data is configured per user, then the default Admin Postback data will be used.

NOTE: Cert based authentication is currently not supported to KeyTalk CKMS!!

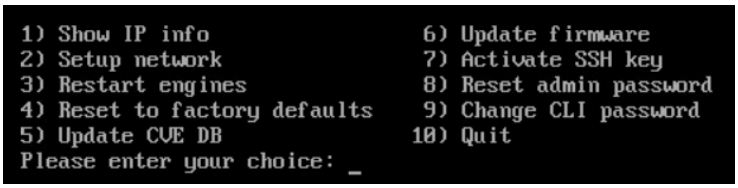
3.5 Backup

To backup your settings and existing reports, select DATABASE and choose Download



3.6 Factory reset

To factory reset, login using the Command Line interface and select option 4:



4 KeyTalk contact details and 3rd line support

KeyTalk IT Security is registered with the Dutch chamber of commerce under: 59072555
with registered VAT number: NL853305766B01

Our office address:
Maanlander 47
3824MN Amersfoort
The Netherlands

Phone: +31 88 KEYTALK or +31 88 5398255
Email: sales[at]keytalk.com
Opening hours: Mo-Fr 08:00 – 18:00 (10/5)

Customer and partner technical 3rd line support
Phone: +31 88 KEYTALK or +31 88 5398255
Email: support[at]keytalk.com
Opening hours: Mo-Su 00:00 – 24:00 (24/7)

Website: https://www.keytalk.com
Firmware/software: https://www.keytalk.com/support