SSL Smart Security Scan
Virtual appliance
quickguide and admin manual

Company	KeyTalk IT Security
Author	MR van der Sman
Creation date	12 March 2019
Last updated	13 February 2020
Product	KeyTalk SSL Smart Security Scan virtual appliance (certificate discovery, SSL related vulnerability scanner, advanced network vulnerability scanner)
Data classification	Public
Software/firmware version	5.4.0
Manual version	5.4.0.2

Contents

1. Quickguide Introduction and download

The KeyTalk SSL Smart Security Scan virtual appliance is meant to periodically scan a given network (internal and/or external facing) on a range of ports 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 show the relevant certificate meta data.

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

Our offered 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 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. The KeyTalk 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

In addition to reporting on certificate lifetime, CN, SAN etc, the KeyTalk SSL Smart Security Scanner currently also analyses for the following 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 Smart Security Scan virtual appliance is based upon CentOS 7 and requires:

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

Virtual appliance formats:

- OVF/VMDK compatible with ESXi, VMware Workstation, AWS

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
	443	Outbound	License activation and validation to www.smartsecurityscan.com
	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 upload the KeyTalk Smart Security Scan virtual appliance are not described.

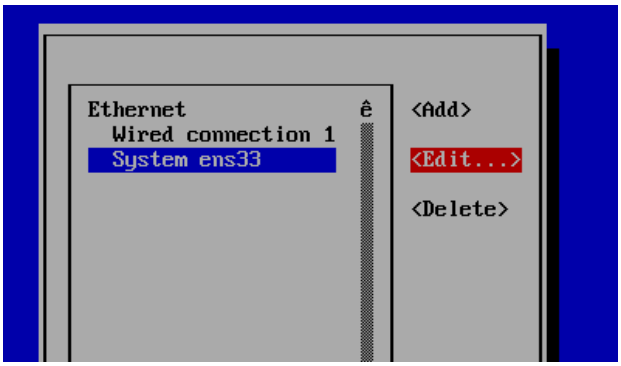
3.1 Assigning IP / Networking

Once the virtual appliance has been uploaded, and the VM is started, a DHCP based IP address will be assigned.

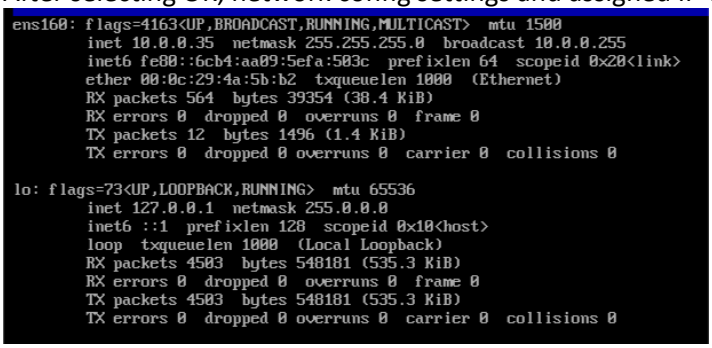
Should DHCP not be applicable, the admin can assign networking details manually, by using the following steps:

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

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



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

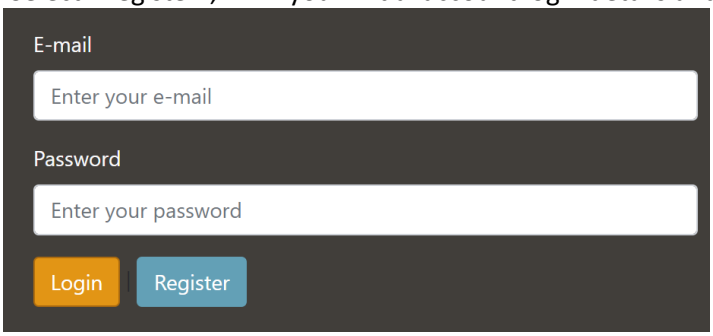


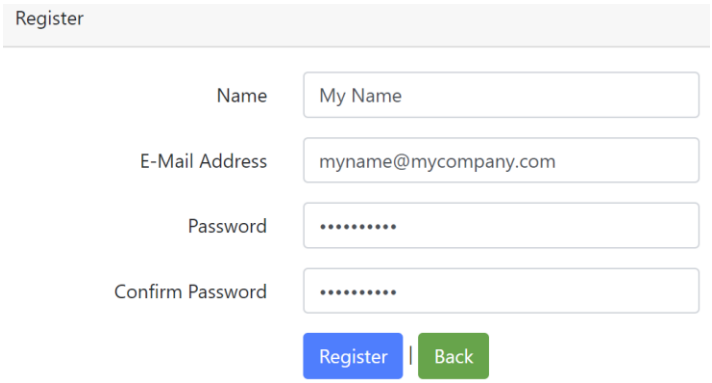
c) Open a browser and go to: https://<IP> or https://<FQDN>

NOTE: Because the KeyTalk SSL Smart Security Scan virtual appliance comes with a 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.

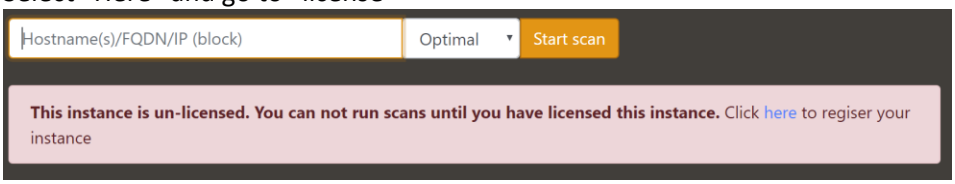
3.2 Registering and activating the scanner license online and offline

d) Select “Register”, fill in your initial account login details and select Register again:

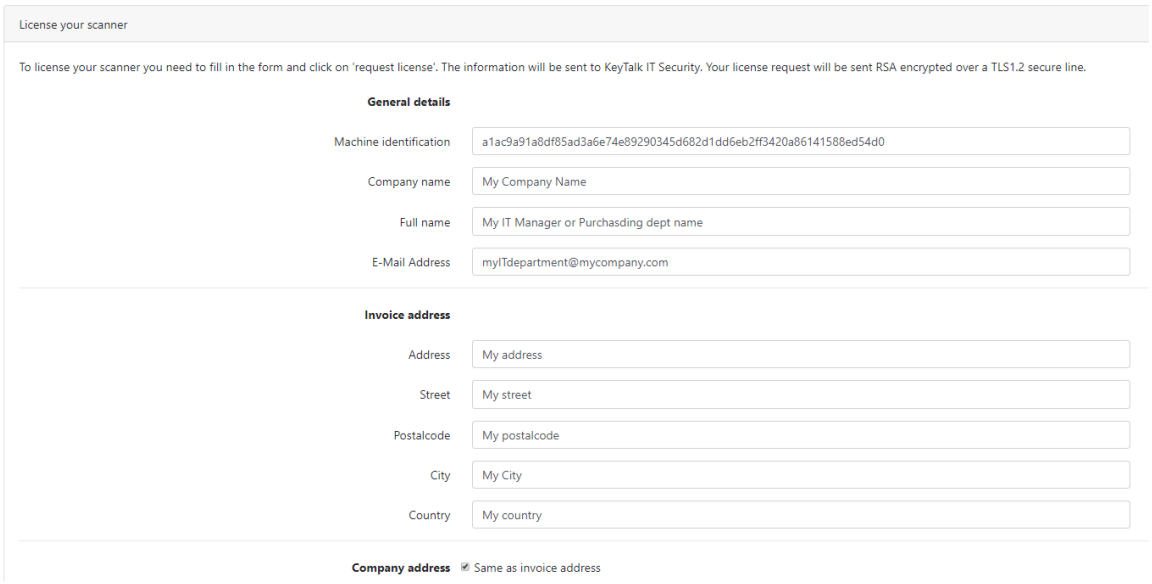




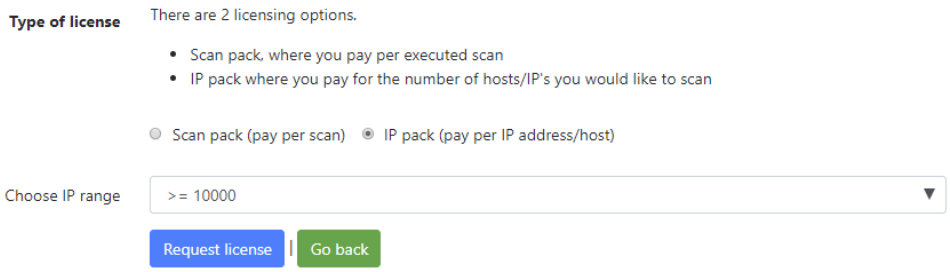
e) Select “Here” and go to “license”



f) Fill in your administrative and billing address details:



g) Select the license you wish. For license pricing kindly contact sales[at]keytalk.com



h) When your KeyTalk Smart Security Scan virtual appliance is online, ie connected to the internet, your license information is sent using a TLS 1.2 secured connection to the Smart Security Scan license server.

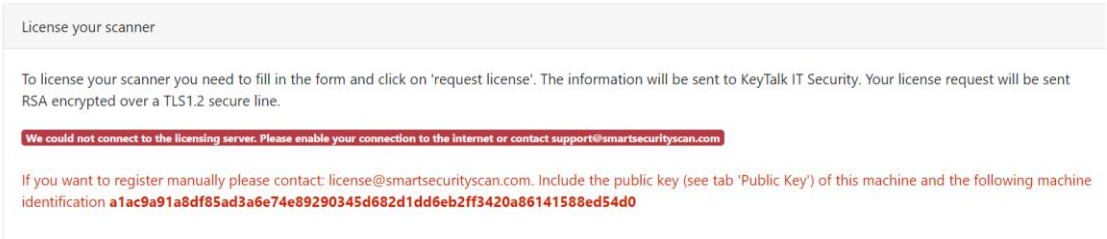
Once licensed, you will receive a message similar to:

Machine identification: a1ac9a91a8df85ad3a6e74e89290345d682d1dd6eb2ff3420a86141588ed54d0

Your scanner has a valid license which is valid until 2020-03-13

You have scanned 0 of the 10000 hosts allowed.

When your KeyTalk Smart Security Scan virtual appliance is offline, ie **NOT** connected to the internet, you will need to send an email to license[at]keytalk.com with the requested information.
An example offline registration message looks like:



Once you receive through email the returned activation code, upload this value to activate your Smart Security Scan

3.3 Enabling proper HTTPS

By default your KeyTalk Smart Security Scan virtual appliance comes with a 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.

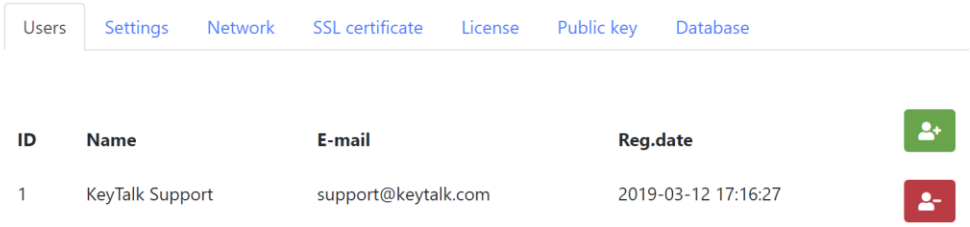
i) This release of the virtual appliance does not support the KeyTalk automated certificate management protocol yet. To manually upload a valid certificate and key order one, either directly from your CA, or through your KeyTalk solution (DEVID USERS -> Select/create FQDN entity -> Select Enroll -> Download in PEM format ->Open in Notepad and split into 2 files 1) certificate 2) key)

j) Upload and apply the certificate and key under

3.4 Create additional users allowed to perform scans

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

k) Select the green + and enter relevant details



3.5 Perform 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

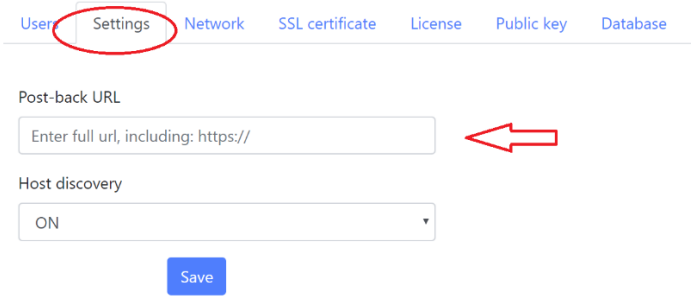
m) Select the port range you wish to scan for:

- ✓ 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
- ✓ Bacnet = scans for SSL certificates based on the Bacnet (IoT) protocol
- ✓ Scheduled enables regular scanning

3.6 Raw JSON output for internal analysis

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:

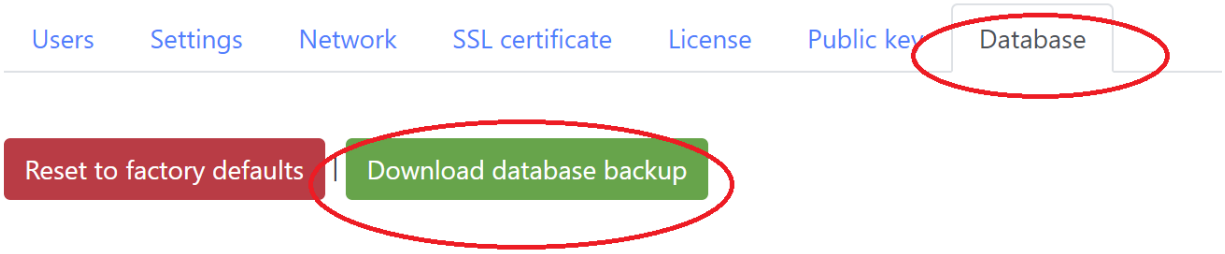


To view the found raw data select the report you wish to examine and add ***?raw*** behind the report url

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

3.5 Backup and factory reset

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



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