How to configure a certificate chain for Checkmk

This guide is not specific to Checkmk! It applies to web server configuration in general, and we provide this article for your convenience. We can **not** support you with general web server issues.

Table of Contents

Problem

Numerous problems related to TLS encryption come down to a simple reason: The web server is configured improperly.
More specifically, many web servers - especially ones not facing the internet - lack the full certificate chain. They only serve their server certificate.

Reason

Technically TLS encryption works with only the server certificate, but to verify the trust, you need the chain.
Modern browsers assemble the certificate chain themselves, which covers up the issue of a missing chain, but many CLI tools and programming languages expect the chain from the web server.

Solution

Background

There is some further reading on certificate chains, which we want to share in advance and encourage you to read and understand:

- https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
- https://success.qualys.com/discussions/s/article/000005824
- https://success.qualys.com/discussions/s/article/000003198

Simply put, you only need a few things to work properly:

- Your client (monitored system) will need to trust the root certificate of your CA (The internet is full of guides on how to achieve that for several operating systems).
- Your web server has to serve the certificate chain (**without** the root certificate) in addition to the server certificate.

Preparations

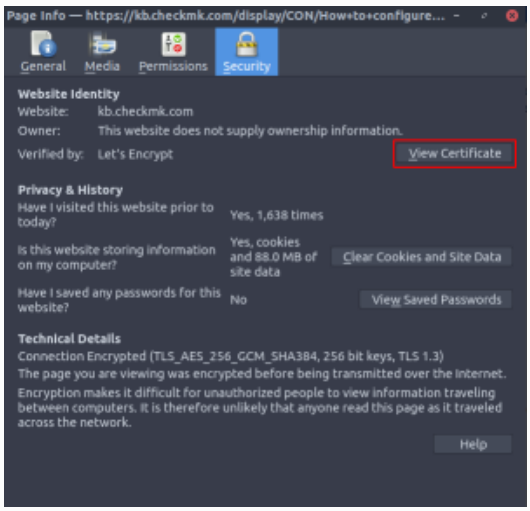
Before moving on to the actual configuration, you need to acquire and prepare the necessary files:

- Private Key file
- Server Certificate file
- CA Intermediate Certificate file(s)
- CA Root Certificate file (not necessary for this guide)

For the first two, if you do not have, or know how to get them, ask your PKI administrator or the person responsible for certificates in your organization.
They should actually be able to provide you with all the files necessary.
If you have the former two files already and don't want to bother your certificate person, you can extract the CA files from your web browser.

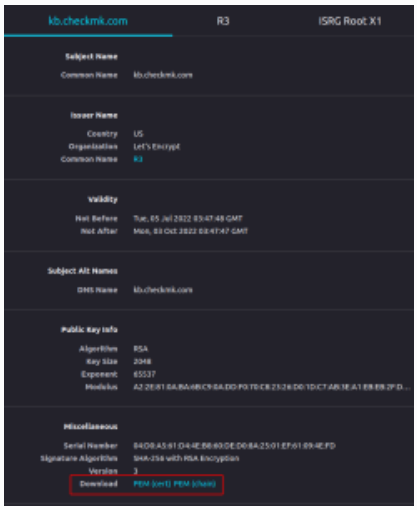
1. Navigate to your Checkmk web interface
   a. Firefox
      i. Click on the little lock icon

ii. Then click on *Connection secure* and *More information*.



iii. Now you see the *Page Info*, where you click on *View Certificate.*

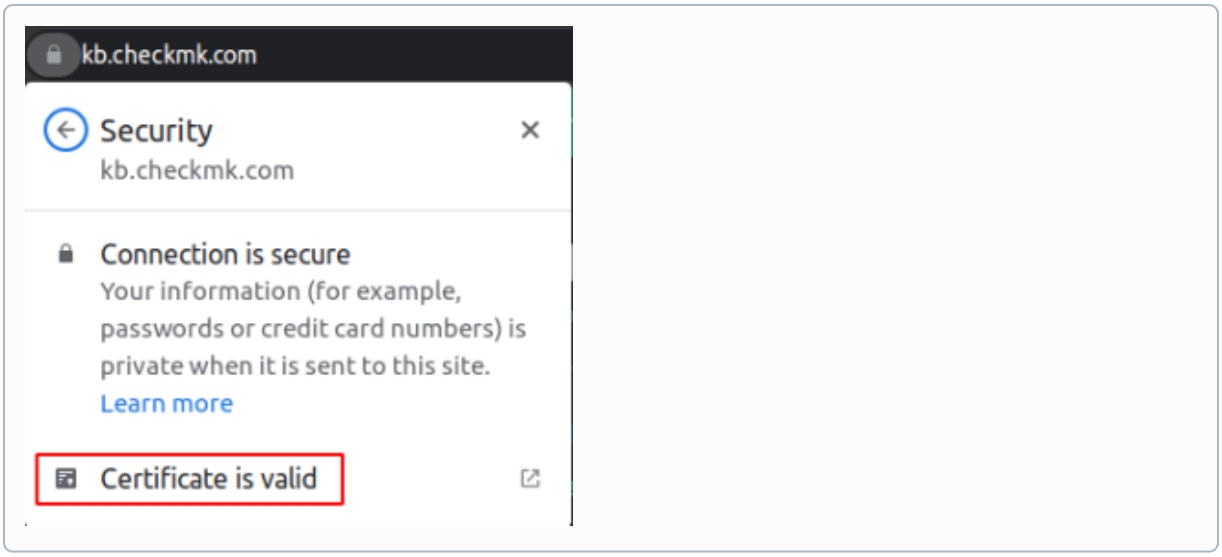
iv. This brings you to a page, where you can inspect and download all certificates involved.



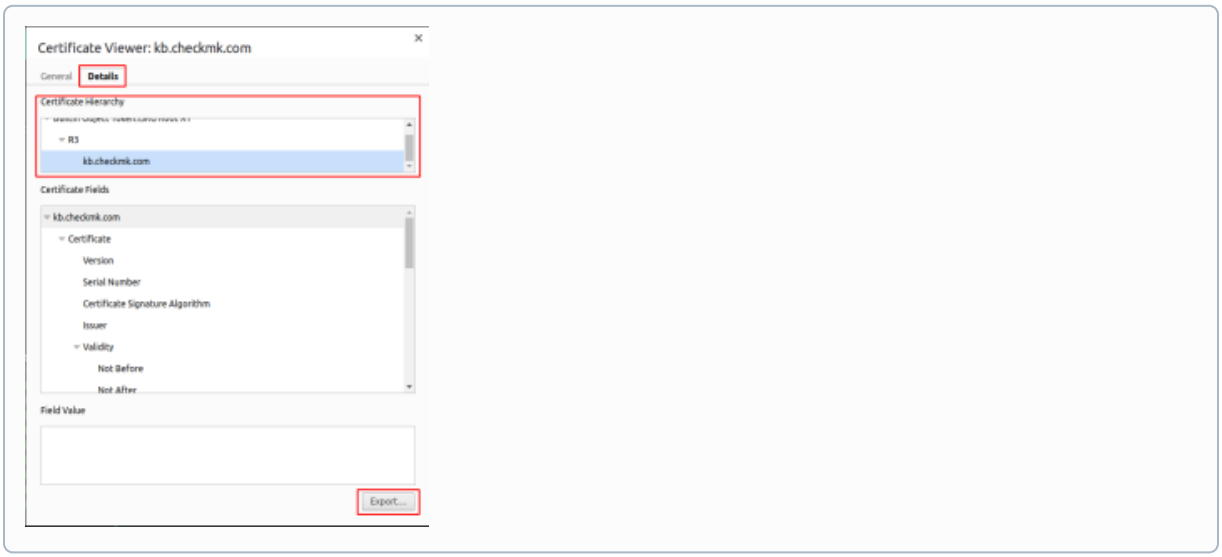
2. Chrome(ium)

a. Click on the little lock icon

b. Then click on *Connection is secure* and *Certificate is valid*.



c. This brings you to a page, where you can inspect and download all certificates involved.



If you are running the Checkmk Appliance (virtual or physical) follow the below steps to configure the certificate chain. We have prepared the steps for our Checkmk Appliance as well as for the Apache web server on Linux.

Now, depending on your Checkmk infrastructure, choose the appropriate manual:

Checkmk Appliance

1. Log into the webconf
2. Navigate to *Device Settings* > *Web Access*
3. Choose *Upload Certificate*
4. Now choose the appropriate files and click *Upload*
    a. For the certificate chain, you only need the intermediate certificate(s), without the root certificate

Linux Server

The following steps depend on your specific Linux distribution.

1. Log into the server as root
2. Navigate to "/etc/[apache2|httpd]/"
3. Locate your website configuration file. In a default installation this would be:
    a. Debian derivates: /etc/apache2/sites-available/default-ssl.conf
    b. RedHat derivates: /etc/httpd/conf.d/my-ssl.conf
4. In the configuration file you will find the following directives:

```
SSLCertificateFile      /path/to/certificate.pem
SSLCertificateKeyFile   /path/to/certificate.key
SSLCertificateChainFile /path/to/chain.pem
```

5. Save the file and reload Apache2: "systemctl reload [apache2|httpd]"

Related articles

Content by label

There is no content with the specified labels