Configuring SSL on apache for NMIS and OMK

Enabling SSL for NMIS and OMK on Apache

The process of enabling SSL has variations depending on your requirements, your setup, your company policy and how you are using the servers (internal or external use). We recommend you do your research on the subject to understand the various options.

The subjects below discuss and demonstrate possible methods or options for each piece of the puzzle for enabling SSL.

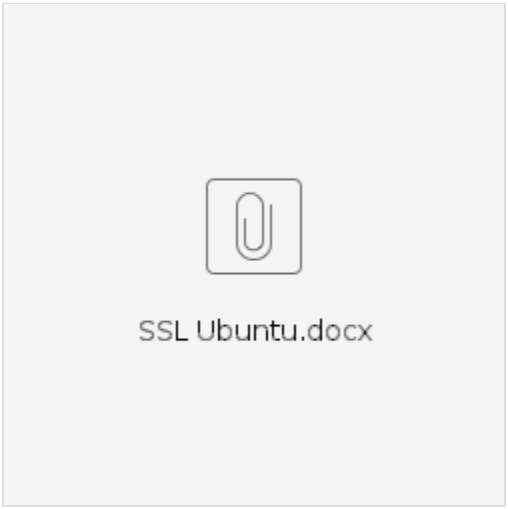
At a minimum you will need the right SSL certificates for your needs and then enable apache to provide SSL using those certificates. There are then further things you may need to do such as redirecting any HTTP connections to HTTPS, redirecting clients to a consistent servername (matching the SSL certificate), allowing internal server to server API connections to not use SSL etc.

The only part below which is specific to Opmantek is vhost configurations which are used to access the OMK web services and rediret users to consistent URLs. All other configurations are generic to SSL certificates or Apache configuration for SSL and as such much further information is available from other sources.

Changing the opmantek apache vhost configurations to use SSL

We have to modify the following file: /etc/httpd/conf.d/04omk-proxy.conf replacing "http" for "https" on this line: RequestHeader set X-Forwarded-Proto "**http**
"

Instructions for SSL implementation on Ubuntu



Obtaining and Installing SSL Certificates

Redirecting connections to HTTPS URL by changing the vhost configurations

Redirecting connections to FQDN and HTTPS URL - apache vhost configurations

Avoiding using SSL for server to server API connections

Other useful Sources

Related topic on SSO

For Single Sign On (SSO) configuration (log in once across all Opmantek applications) please see SSO for Opmantek Applications