ESET Tech Center

Apache Web Server Configuration

Anish | ESET Nederland - 2018-01-30 - Reacties (0) - ESET Endpoint Encryption

If you have installed the Enterprise Server using the 'all in one' package from our website you can enable SSL/HTTPS settings in the Control Panel.

Access the Enterprise Server 'Control Panel'
Select 'Settings'
Click 'Apache Server SSL Configuration'

SSL Details

To enable SSL please follow the instructions below:

Select the 'SSL Details' tab
Select 'Enable SSL Server support' checkbox
Type in your selected port (the default HTTPS port is 443)

Certificate Options

There are 2 methods to add your own certificates, please follow the instructions below:

Select the 'Certificate Options' tab

Upload certificate

If you have already purchased your SSL certificate:

Click 'Upload certificate'
Simply copy the supplied server.key and server.crt files into the corresponding boxes

Create new certificate (self-signed)

If you do not already have a certificate file, a self-generated certificate can be generated for test purposes:

Click 'Create new certificate'
Enter the appropriate details into the form

Redirect Options

If you wish to force HTTPS usage:

Select the 'Redirect Options' tab
Tick the 'Force HTTPS usage' checkbox

Manual Configuration

If you have installed the Enterprise Server 'standalone' package and manually configured Apache, follow the instructions below:

Certificates

If you have already purchased your SSL certificate, simply copy the supplied server.key and server.crt files into the folder **Program Files\DESlock+ HTTP\conf**

Self Signed Certificates

If you do not already have a certificate file, a self-generated certificate can be generated for test purposes using the openssl tool following the steps below:

Open an elevated command prompt.
Navigate to **Program Files\DESlock+ HTTP\bin** (ProgramFiles (x86)) on 64bit
platforms).
Enter the command "**openssl req -config ..\conf\openssl.cnf -new -out server.csr**"
You will be required to enter and verify the entry of a passphrase. All other requests can be left as default by pressing enter with the

exception of **Common Name** which **MUST** match the name of the webserver address hosting the certificate.
Enter the command "**openssl rsa -in privkey.pem -out server.key**"
Enter the passphrase you specified previously. If successful the command should return the text '**writing RSA key**'.
Enter the command "**del .rnd**"
Enter the command "**openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 365**". Note: this sets the certificate to last 365 days.
Enter the command "**move server.key ..\conf**"
Enter the command "**move server.crt ..\conf**"

Applying the certificate

With either a purchased or test certificate type perform the following steps:

As a security measure, be sure to change the file permissions on the certificate files so that they are read-only and only administrator users can access them.
Open the file **Program Files\DESlock+ HTTP\conf\httpd.conf** (ProgramFiles (x86) on 64bit platforms).
Find the line **#LoadModule ssl_module modules/mod_ssl.so**, remove the #symbol from the line.
Find the line **#Include conf/extra/httpd-ssl.conf**, remove the # symbol from the line.
At the end of the httpd.conf file add these lines (this will redirect attempts to access using http to the https address instead):

LoadModule rewrite_module modules/mod_rewrite.so

RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule ^/dlpes(|/.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=302,L]

Save the updated httpd.conf file.

On 64 bit operating systems the following modification is required:

You need to update the ssl configuration with the short path to the logs folder. You can find the short path filenames using the DIR /X command. The example below is of a default Windows 7 x64 system using the ES preinstall.

Open \Program Files (x86)\DESlock+ HTTP\conf\extra\httpd-ssl.conf in notepad
Find the SSLSessionCache value and change as below commenting out the existing SSLSessionCache and applying the new path (highlighted below) then save the change:

Inter-Process Session Cache:

Configure the SSL Session Cache: First the mechanism

to use and second the expiring timeout (in seconds).

#SSLSessionCache "dbm:C:/Program Files (x86)/DESlock+ HTTP/logs/ssl_scache"

#SSLSessionCache "shmcb:C:/Program Files (x86)/DESlock+ HTTP/logs/ssl_scache(512000)"

SSLSessionCache "shmcb:C:/Progra\~2/DESloc\~1/logs/ssl_scache(512000)"

SSLSessionCacheTimeout 300

On all operating systems:

Restart the DESlockHTTP service within the services control panel.

Note: If access to the server is from external machines you will need to open port 443 on firewalls for external connections.

---

keywords: apache configuration config ssl SSL https HTTPS Apache secure