How To Configure SSL/TLS With Nagios XI 5

Purpose

This document describes how to configure SSL/TLS With Nagios XI. If you are using Nagios XI 2024, refer to the updated document.

Terminology & Security

For your information:

- **SSL** = Secure Sockets Layer
- **TLS** = Transport Layer Security

TLS replaces SSL, however the tools used to implement both generally use SSL in their name/directives. For simplicity reasons, the rest of this document will use the term SSL.

To implement SSL you need to generate a certificate. When you generate a certificate, you create a request that needs to be signed by a Certificate Authority (CA). This CA can be:

- A trusted company like VeriSign
- An internal CA that is part of your IT infrastructure, like a Microsoft Windows CA
- The Nagios XI server itself (self signed)

The CA will then provide you with a signed certificate.

This documentation can used to generate a request that can be submitted to any of these CA types.

Editing Files

In many steps of this documentation you will be required to edit files. This documentation will use the vi text editor. When using the vi editor:

- To make changes press `i` on the keyboard first to enter insert mode
- Press **Esc** to exit insert mode
- When you have finished, save the changes in vi by typing `:wq` and press **Enter**

Step 1: Installing Necessary Components

Establish a terminal session to your Nagios XI server as root and execute the following command:

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

CentOS / RHEL / Oracle Linux

```
yum install -y mod_ssl openssl
```

Debian / Ubuntu

```
apt-get install -y openssl
```

Step 2: Certificate Directory

The steps in this documentation will be performed from within the `/usr/local/nagiosxi/var/certs/` directory. Execute the following commands to create the directory (if it doesn't exist) and then change into it:

```
mkdir -p /usr/local/nagiosxi/var/certs
chown -R nagios:nagios /usr/local/nagiosxi/var/certs
chmod 775 /usr/local/nagiosxi/var/certs
cd /usr/local/nagiosxi/var/certs/
```

You will continue to use this terminal session throughout this documentation.

Step 3: Generate Private Key File

The first step is to generate the private key file, execute the following command:

```
openssl genrsa -out nagiosxi.key 2048
```

That would have generated some random text.

Step 4: Generate Certificate Request File

Next you will generate the certificate request file by executing the following command:

```
openssl req -new -key nagiosxi.key -out nagiosxi.csr
```

You will need to supply some values, some can be left blank, however the most important value is the **Common Name**.

Note: It's very important that the IP Address / DNS name in **Nagios XI > Admin > System Settings > General** is the same as what is typed in the certificate request "common name".

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

In the example below you can see that `xi-c7x-x64.domain.local` has been used which means that when you access the Nagios XI server in your web browser, this is the address you will need to use. This is particularly important, if these don't match then you will get warnings in your web browser. More detailed information about this can be found in the following KB article:

SSL/TLS - Understanding Certificate Warnings

The following is an example:

```
Country Name (2 letter code) [XX]:AU
State or Province Name (full name) [ ]:NSW
Locality Name (eg, city) [Default City]:Sydney
Organization Name (eg, company) [Default Company Ltd]:My Company Pty Ltd
Organizational Unit Name (eg, section) [ ]:
Common Name (eg, your name or your server's hostname) []:xi-
c7xx64.domain.local
Email Address [ ]:
Please enter the following 'extra' attributes to be sent with your
certificate request
A challenge password [ ]:
An optional company name [ ]:
```

As you can see above, I did not supply an **Organizational Unit Name**, **email address**, **password** or **optional company name**. Specifically, providing a **password** is not necessary.

Step 5: Sign Certificate Request

At this point you have created a certificate request that needs to be signed by a CA.

Option 1: Using A Trusted CA Company

If you are going to use a trusted company like VeriSign to provide you with a certificate you will need to send them a copy of the certificate request.

1. View the certificate request by executing the following command:

```
cat nagiosxi.csr
```


Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

2. You'll get a lot of random text, this is what you will need to provide to your trusted CA:

You must provide the CA with everything including the `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` lines.

3. Once they send you the signed certificate you will need to copy the certificate into a new file called `nagiosxi.crt`. The certificate you receive will also be a lot of random text, so you can just paste that text into the new file which you can open with the vi editor:

```
vi nagiosxi.crt
```

You must paste everything including the `-----BEGIN CERTIFICATE -----` and `-----END CERTIFICATE -----` lines when pasting them into the file.

4. Save the file and close vi.

You can now proceed to the Set Permissions section of this document.

Option 2: Using A Microsoft Windows CA

If you are going to use a Microsoft Windows CA to sign your certificate request please follow the steps in this KB article:

SSL/TLS – Signing Certificates with a Microsoft Certificate Authority

After following the KB article you will have a `.crt` file and you can proceed to the Set Permissions section of this document.

Option 3: Self Signing The Certificate

You can also self-sign the certificate by executing the following command:

```
openssl x509 -req -days 365 -in nagiosxi.csr -signkey nagiosxi.key -out nagiosxi.crt
```

Which should produce output saying the Signature was OK and it was Getting Private Key.

Note: When you self sign a certificate you will get warnings in your web browser. More detailed information about this can be found in the following KB article:

SSL/TLS – Understanding Certificate Warnings

Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Step 6: Set Permissions

You need to set permissions on the files, execute the following commands:

```
chmod go-rwx nagiosxi.*
```

Step 7: Update Apache Configuration

Now you have to tell the Apache web server about the certificate. The configuration file for this differs depending on your operating system (OS), open the SSL file in vi by executing the following command:

CentOS / RHEL / Oracle Linux

```
vi /etc/httpd/conf.d/ssl.conf
```

Debian / Ubuntu

```
vi /etc/apache2/sites-available/default-ssl.conf
```

Find these lines and update them as follows:

```
SSLCertificateFile /usr/local/nagiosxi/var/certs/nagiosxi.crt
SSLCertificateKeyFile /usr/local/nagiosxi/var/certs/nagiosxi.key
```

Note: typing `/eFile` and pressing **Enter** in vi should take you directly to this section in the file.

In that same file, navigate to the end (press **SHIFT + G**) and before the line </VirtualHost> add the following lines:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule nagiosxi/api/v1/(.*)$ /usr/local/nagiosxi/html/api/v1/index.php?request=$1 [QSA,NC,L]
RewriteRule nagiosxi/api/v2/(.*)$ /usr/local/nagiosxi/html/api/v2/index.php [QSA,NC,L]
</IfModule>
```

Save the changes, you have finished editing this file.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

You have to update Apache web server config file to force SSL to be used. The configuration file for this differs depending on your OS, open the SSL file in vi by executing the following command:

CentOS / RHEL / Oracle Linux

```
vi /etc/httpd/conf.d/nagiosxi.conf
```

Debian / Ubuntu

```
vi /etc/apache2/conf-enabled/nagiosxi.conf
```

Add the following lines to the end of the file (press **SHIFT** + **G**):

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule nagiosxi/api/v1/(.*)$ \ /usr/local/nagiosxi/html/api/v1/index.php?request=$1 [QSA,NC,L]
RewriteRule nagiosxi/api/v2/(.*)$ /usr/local/nagiosxi/html/api/v2/index.php [QSA,NC,L]
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</IfModule>
```

It is most likely that you only need to add the two lines in bold above, the end result is that all the lines need to exist.

Save the changes, you have finished editing this file.

Step 8: Restart Apache

You need to restart the Apache for the new certificate key to be used.

RHEL/CentOS/Oracle Linux +

```
systemctl restart httpd.service
```

Debian | Ubuntu :

```
systemctl restart apache2.service
```


Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Step 9: Firewall Rules

The following firewall rules may need to be added. If you cannot access the Nagios XI in the next step (Test Certificate) then it's likely you'll need to run these commands:

RHEL/CentOS/Oracle Linux :

```
firewall-cmd --zone=public --add-port=443/tcp
firewall-cmd --zone=public --add-port=443/tcp --permanent
```

Debian:

The local firewall is not enabled on Debian by default and no steps are required here. If it is enabled then the command is:

```
iptables -I INPUT -p tcp --destination-port 443 -j ACCEPT
```

Ubuntu:

The local firewall is not enabled on Ubuntu by default and no steps are required here. If it is enabled then the commands are:

```
sudo ufw allow https
sudo ufw reload
```

Step 10: Test Certificate

Now test your connection to the server by directing your web browser to:

```
https://yourservername/
```

Note: There is no nagiosxi/ extension in the URL, we are just testing a connection to Apache to see if the certificate works.

You may get a self signed certificate warning, but that is OK, you can just add a security exception. If is working you'll see the Nagios XI welcome page. More detailed information about this can be found in the following KB article:

SSL/TLS – Understanding Certificate Warnings

If it returns an error check your firewall and backtrack through this document, making sure you've performed all the steps listed.

Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Step 11: Update Nagios XI Configuration

The Nagios XI configuration file and GUI settings also need updating.

Open the `/usr/local/nagiosxi/html/config.inc.php` file in vi by executing the following command:

```
vi /usr/local/nagiosxi/html/config.inc.php
```

Find the following line:

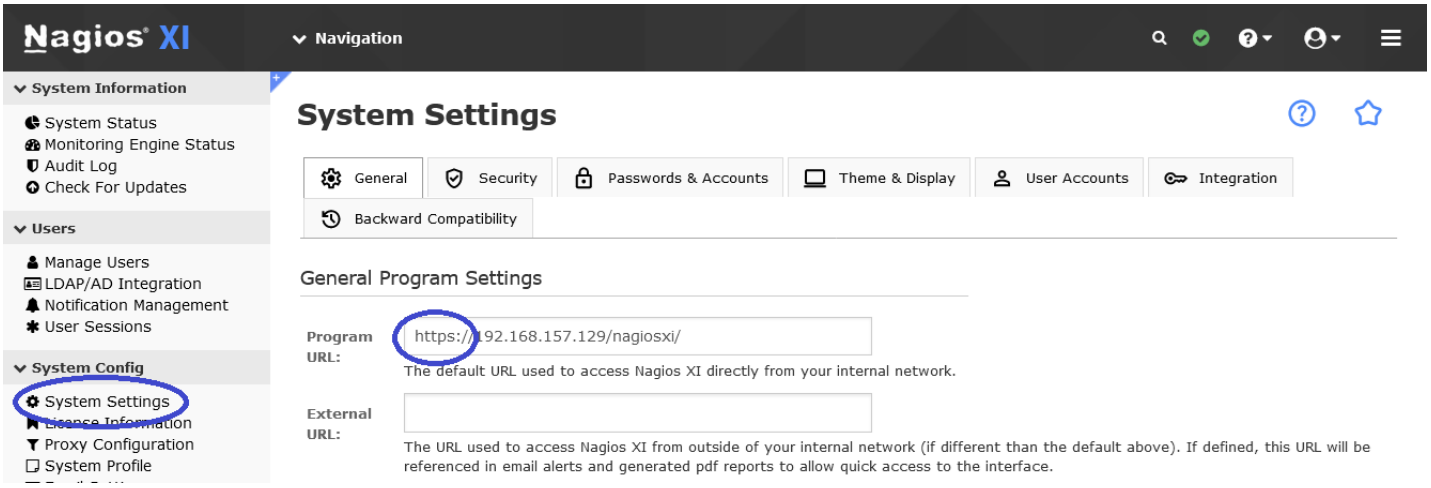
```
$cfg['use_https']=false;
```

Change it to:

```
$cfg['use_https']=true;
```

Save the changes, you have finished editing this file.

Open the Nagios XI web interface to `https://yourservername.orIP/nagiosxi/` and navigate to **Admin > System Config > System Settings**.



Change the Program URL to `https` instead of the default `http` and click the **Update Settings** button.

Note: It's very important that the IP Address / DNS name is the same here as it was typed in the certificate request "**common name**".

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Step 12: Update Custom URL Dashlet

A line of code in the Custom URL Dashlet needs to be changed to force it to use https.

Open the file:

`/usr/local/nagiosxi/html/includes/dashlets/custom-dashlet/customdashlet.inc.php`

...in vi using the following command:

```
vi /usr/local/nagiosxi/html/includes/dashlets/custom-dashlet/custom-dashlet.inc.php
```

Find the following line *(type **:61** and press Enter to take you to that line)*:

```
  <input type="text" name="url" id="url" value="http://">
```

Change it to:

```
  <input type="text" name="url" id="url" value="https://">
```

Save the changes, you have finished editing this file.

Thanks to Steve Beauchemin for bringing this to our attention in the Nagios Support Forums.

Notes On Redirecting

With this configuration, if a user types `http://xiserver` in their web browser, it will redirect them to `https://xiserver` which can cause certificate warnings in certain scenarios. If you wanted to redirect them to https://xiserver.yourdomain.com then you simply need to change the `RewriteRule` in the `/etc/httpd/conf/httpd.conf file:`

```
  RewriteRule (.*) https://xiserver.yourdomain.com%{REQUEST_URI}
```

Then restart the httpd service.

More detailed information about this can be found in the following KB article:

SSL/TLS – Understanding Certificate Warnings

Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Troubleshooting

Check out the links below for SSL specific troubleshooting topics:

Troubleshooting SSL Issues

SSL Certificate does not validate properly

OpenSSL causes issue with check_nrpe plugin with NSClient++

Finishing Up

This completes the documentation on How To Configure SSL/TLS With Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.