How To Configure Apache ModSecurity in Nagios XI 2024

Purpose

This document describes how to configure Apache ModSecurity in Nagios XI.

Web Application Firewall (ModSecurity)

In In order to detect and prevent attacks against web applications, the web application firewall (ModSecurity) has been added as an optional tool in Nagios XI 2024 R1.2 and later. It is designed to protect web applications from various cyber threats by monitoring, logging, and filtering HTTP traffic. The core functionality of ModSecurity includes real-time web traffic monitoring, intrusion detection, and prevention capabilities. It uses a rule-based system to detect and block potentially harmful requests, such as SQL injection, cross-site scripting (XSS), and other common web application attacks. ModSecurity also provides logging and reporting features that help administrators analyze and respond to security incidents effectively.

One of the key strengths of ModSecurity is its flexibility and extensibility. Users can create custom rules to meet specific security requirements or use the extensive set of pre-built rules provided by the OWASP Core Rule Set (CRS), which is regularly updated to address new vulnerabilities.

Nagios XI 2024 R1.2 and later's implementation of ModSecurity uses the set of pre-build rules provided by the OWASP CRS. For more information about this rule set, please see the OWASP CRS Project for documentation on use and writing rules.

Learning More

Please see the following links to learn more about general ModSecurity implementation.

- ModSecurity Reference Manual: This comprehensive manual covers installation, configuration, and rule writing for ModSecurity.
- DigitalOcean ModSecurity Tutorial: This step-by-step guide helps you install and configure ModSecurity on an Apache server running Ubuntu
- Red Hat ModSecurity Guide: A detailed guide on configuring and managing ModSecurity on Red Hat Enterprise Linux, which can also be adapted for other Linux distributions.

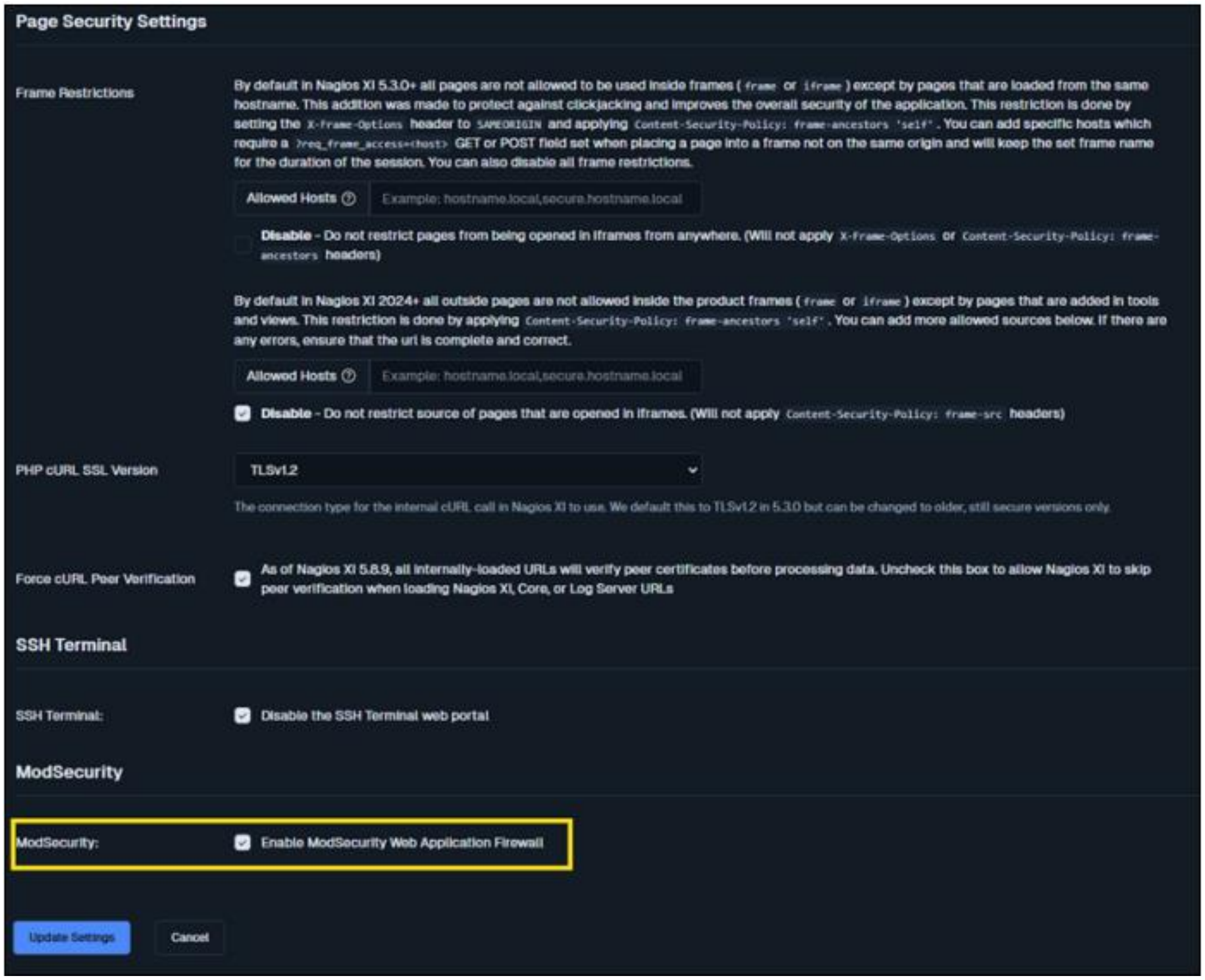
Turning ModSecurity On/Off in Nagios XI 2024

In Nagios XI 2024, ModSecurity is turned off by default. Having ModSecurity enabled on your Nagios XI server will help mitigate risk from potential vulnerabilities.

Note: If you run into usability issues in your environment because of ModSecurity enablement, you can turn off ModsSecurity by following either of the two paths described below

To turn on/off ModSecurity in the Nagios XI web interface:

1. Navigate to **Admin** > **System Config** > **System Settings**.
2. Select the **Security** tab on the **System Settings** page.
3. Scroll down to the **ModSecurity** section.



Page Security Settings

Frame Restrictions

By default in Nagios XI 5.3.0+ all pages are not allowed to be used inside frames (`frame` or `iframe`) except by pages that are loaded from the same hostname. This addition was made to protect against clickjacking and improves the overall security of the application. This restriction is done by setting the `X-Frame-Options` header to `SAMEORIGIN` and applying `Content-Security-Policy: frame-ancestors 'self'` . You can add specific hosts which require a `?req_frame_access=<host>` GET or POST field set when placing a page into a frame not on the same origin and will keep the set frame name for the duration of the session. You can also disable all frame restrictions.

Allowed Hosts: Example: hostname.local,secure.hostname.local

□ **Disable** - Do not restrict pages from being opened in iframes from anywhere. (Will not apply `X-Frame-Options` or `Content-Security-Policy: frame-ancestors` headers)

By default in Nagios XI 2024+ all outside pages are not allowed inside the product frames (`frame` or `iframe`) except by pages that are added in tools and views. This restriction is done by applying `Content-Security-Policy: frame-ancestors 'self'` . You can add more allowed sources below. If there are any errors, ensure that the url is complete and correct.

Allowed Hosts: Example: hostname.local,secure.hostname.local

☑ **Disable** - Do not restrict source of pages that are opened in iframes. (Will not apply `Content-Security-Policy: frame-src` headers)

PHP cURL SSL Version: TLSv1.2

The connection type for the internal cURL call in Nagios XI to use. We default this to TLSv1.2 in 5.3.0 but can be changed to older, still secure versions only.

Force cURL Peer Verification: ☑ As of Nagios XI 5.8.9, all internally-loaded URLs will verify peer certificates before processing data. Uncheck this box to allow Nagios XI to skip peer verification when loading Nagios XI, Core, or Log Server URLs

SSH Terminal

SSH Terminal: ☑ Disable the SSH Terminal web portal

ModSecurity

ModSecurity: ☑ Enable ModSecurity Web Application Firewall

4. Select/Deselect the **Enable ModSecurity Web Application Firewall** checkbox
5. Select the **Update Settings** button

To turn on ModSecurity in the command line:

On the Nagios XI server, run the following command script in the command line

```
/usr/local/nagiosxi/scripts/toggle_modsecurity.sh -enable
```

On the Nagios XI server, run the following command script on the command line.

```
/usr/local/nagiosxi/scripts/toggle_modsecurity.sh -disable
```

Log Files (Linux)

Debian based log location = `/var/log/apache2/modsec_audit.log`

RPM based log location = `/var/log/httpd/modsec_audit.log`

To analyze these logs, you can use command-line tools like grep, awk, and tail to filter and examine entries related to ModSecurity events. Additionally, ModSecurity's auditlog directive allows for customization of the logging format and location, making it easier to organize and review logs. For a more comprehensive analysis, you can use tools like the ModSecurity Console or third-party log management solutions that provide advanced search and visualization capabilities, helping you quickly identify and respond to potential security threats.

Finishing Up

This completes the documentation on how to configure Apache ModSecurity in 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