

# nginx or apache mod security installation

## Pre-Packaged, Binary Installation

The easiest method of installing ModSecurity is to use your existing OS Package Manager application (Yum or Aptitude) to install it from your default OS Repository.

### Installation – Ubuntu/Debian

[crayon-678775d64d40e355834313/]

### Installation – Fedora/CentOS

[crayon-678775d64d418451269494/]

### Installation – Microsoft IIS (MSI Installer)

[Installation information for IIS](#)

- [ModSecurity v2.9.1 for IIS MSI Installer – 32bits \(sha256\)](#)
- [ModSecurity v2.9.1 for IIS MSI Installer – 64bits \(sha256\)](#)

# Source Code Downloads

ModSecurity is an open source product licensed under ASLv2. It comes with full source code and documentation. Current releases are signed by Breno Silva. These public keys are available via most PGP key server mirrors.

## ModSecurity for Apache (Stable Release Quality)

[Installation information for Apache](#)

- [ModSecurity for Apache TAR/GZ \(sha256\)](#)

## ModSecurity for Nginx

**NOTE:** The Nginx module is contained within the Apache archive package. You must first compile ModSecurity with the **-enable-standalone-module** flag and then compile the Nginx code to use it. See the [Blog post for more information](#).

**NOTE:** Some instabilities in the Nginx add-on have been reported (see the Github issues page for details). Please use the “nginx\_refactoring” branch where possible for the most up to date version and stay tuned for the ModSecurity version 4.

- [ModSecurity for Nginx TAR/GZ \(sha256\)](#)
- [ModSecurity for Nginx \(Nginx\\_Refactoring Github branch\)](#)