How to enable mod security

Enabling Mod Security

1.0 General Information

Starting in version 7.1.1, **mod_security** is available with a comprehensive set of rules to log or protect against web based attacks. **mod_security** is an apache module that acts as a filter for http traffic and blocks traffic that match a set of rules that describe attack vectors exploited by malicious actors. GroundWork has added the ability to enable this feature in the product with a few easy steps.

2.0 Enable Mod Security

Because some of the traffic in GroundWork is of an administrative nature, **mod_security** is set to detection only mode when enabled. Detection only mode will only log traffic that matches rule violations. These violations could be evidence of an attack and should be sent to a log analysis tool for regular auditing and alerting. The rule violations are logged in the apache error log at **/usr/local/groundwork/apache2/logs/error_log**. To enable blocking, see section the below **Enable Application Protection**.

1. To enable **mod_security**, modify **/usr/local/groundwork/apache2/conf/extra/httpd-ssl.conf**.
2. Uncomment the following line:

```
Include httpd-security.conf
```

3. Restart apache:

```
service groundwork restart apache
```

3.0 Enable Application Protection

Some environments have more strict requirements and need to have protection enabled. There is a risk that some features of the product or custom code will not work if protection mode is enabled. If you run into any problems you can open a support ticket and GroundWork Support will assist you.

1. To set **mod_security** in Protection Mode, modify **/usr/local/groundwork/apache2/conf/extra/httpd-security.conf**.
2. Comment out following line:

```
#SecRule Engine DetectionOnly
```

3. Restart apache:

```
service groundwork restart apache
```