Configure ClamAV Scanner

For cPanel & WHM 11.46

(Home >> Plugins >> Configure ClamAV Scanner)

- Overview
- How to install ClamAV Scanner
- ClamAV Scanner configuration
- Configure ClamAV Scanner for specific users
  - Add or remove configured users
  - Configure defaults for new configured users
  - Configure settings for an individual user
- Configure ClamAV Scanner for Exim
- Command line interface
- ClamAV Scanner cron job

Overview

Clam AntiVirus (ClamAV) is an antivirus software toolkit that is available for cPanel & WHM installations. The scanner searches your server for malicious programs. If it identifies a potential security threat, it will flag the file to allow you to take the appropriate action.

Important
After you configure *ClamAV Scanner*, we recommend that you create a root cron job that will run daily during off-peak hours.

How to install *ClamAV Scanner*

To install or uninstall ClamAV Scanner, use the Manage Plugins interface in WHM *(Home >> cPanel >> Manage Plugins)*.

ClamAV Scanner configuration

To configure *ClamAV Scanner*:

1. Select the services that you wish to scan.
   - *Scan Entire Home Directory* — Scans the `home` directory on your server.
   - *Scan Mail* — Scans all mail folders on your server.
   - *Scan Public FTP Space* — Scans all folders that are publicly accessible through FTP services.
   - *Scan Public Web Space* — Scans all folders that are publicly accessible through the web.
2. Click *Save*.

Important
You must perform additional steps if you wish to integrate *ClamAV Scanner* with Exim.

Configure *ClamAV Scanner* for specific users

If you wish to override the *ClamAV Scanner* configuration for specific users, click *User Configuration*. The *User Configuration* interface also allows you to set override defaults for all configured users.

Add or remove configured users

Before you can configure a user's *ClamAV Scanner* settings, that user must appear on the *Configured Users* menu.

To add a user to the *Configured Users* menu:

1. Select the desired user from the *User List* menu.
2. Click *Add*.
    - If you wish to add all of the users that are on the *User List* menu to the *Configured Users* menu, click *Add All*.

To remove a user from the *Configured Users* menu:

1. Select the desired user from the *Configured Users* menu.
2. Click *Remove*.
    - If you wish to remove all of the users that are on the *Configured Users* menu, click *Remove All*.

> **Note**
> After you remove a user from the *Configured Users* menu, *ClamAV Scanner* will use the main configuration to scan that user's portion of the server.

Configure defaults for new configured users

ClamAV Scanner applies the settings that you specify under the *Defaults* header to all new configured users.

To set the default settings for new configured users:

1. Select the services that you wish to scan.
    - *Scan Entire Home Directory* — Scans the user's `home` directory.
    - *Scan Mail* — Scans the user's mail folders.
    - *Scan Public FTP Space* — Scans all of the user's folders that are publicly accessible through FTP services.
    - *Scan Public Web Space* — Scans all of the user's folders that are publicly accessible through the web.
2. Click *Save*.

Configure settings for an individual user

To configure *ClamAV Scanner* for an individual user:

1. In the *Group Scanner Configuration* section's *Configured Users* menu, select the user for whom you wish to configure *ClamAV Scanner*.
    - If the desired user does not appear in the *Configured Users* menu, use the instructions above to add that user.
    - The user that you select will appear in the *Configure User* text box in the *User Scanner Configuration* section.
2. In the *User Scanner Configuration* section, click *Configure*.
3. Select the services that you wish to scan.
    - *Scan Entire Home Directory* — Scans the user's `home` directory.
    - *Scan Mail* — Scans the user's mail folders.
    - *Scan Public FTP Space* — Scans all of the user's folders that are publicly accessible through FTP services.
    - *Scan Public Web Space* — Scans all of the user's folders that are publicly accessible through the web.
4. Click *Save Defaults.*

Configure *ClamAV Scanner* for Exim

> **Important**
> You must perform these additional steps if you wish to integrate *ClamAV Scanner* with Exim.

To configure *ClamAV Scanner* for Exim:

1. Navigate to *the Exim Configuration Manager* interface *(Home >> Service Configuration >> Exim Configuration Manager >> Basic Editor >> Security)*.
2. For the *Scan messages for malware from authenticated senders (exiscan)* option, select the *On* setting.
3. For the *Scan outgoing messages for malware* option, select the *On* setting.
4. Click *Save*.

Command line interface

If you prefer to use the command line interface to run ClamAV, the binaries are located in the `/usr/local/cpanel/3rdparty/bin/` directory:

```
/usr/local/cpanel/3rdparty/bin/clamscan
/usr/local/cpanel/3rdparty/bin/freshclam
```

If you have scripts that expect ClamAV binaries in the `/usr/local/bin` directory, you can create symbolic links with the following commands:

```
ln -s /usr/local/cpanel/3rdparty/bin/clamscan /usr/local/bin/clamscan
ln -s /usr/local/cpanel/3rdparty/bin/freshclam /usr/local/bin/freshclam
```

ClamAV Scanner cron job

After you configure *ClamAV Scanner*, we recommend that you create a `root` cronjob that will run daily during off-peak hours. The cronjob should run the following command:

```
for i in `awk '!/nobody/{print $2 | "sort | uniq" }' /etc/userdomains |
sort | uniq`; do /usr/local/cpanel/3rdparty/bin/clamscan -i -r /home/$i
2>>/dev/null; done >> /root/infections&
```

This command recursively searches the `home` directory for spam and infected files.