

Антивирус ClamAV

Модуль «Антивирус ClamAV» расположен в Меню «Защита». Данный модуль предназначен для защиты от проникновения вредоносных программ в локальную сеть. Модуль «Антивирус ClamAV» имеет три вкладки: «Антивирус ClamAV», «Настройки», «Журнал».

Антивирус ClamAV

The screenshot displays the ClamAV interface with three tabs: "Антивирус ClamAV", "Настройки", and "Журнал". The "Антивирус ClamAV" tab is active, showing two service cards. The first card, "Антивирус ClamAV", is "запущен" (running) and displays statistics: "Количество сигнатур: 4566249(main), 1584853(daily), 94(byte)", "Версия баз: 58(main), 25465(daily), 328(byte)", "Версия: 0.101.2", and "Последнее обновление: 30.05.2019 10:58:26". It has buttons for "Обновить сейчас" and "Выключить". The second card, "Антивирусный прокси-сервер", is also "запущен" and "Проверяет HTTP-трафик на наличие вирусов", with a "Выключить" button. Below the cards is the "Журнал" (logs) section, showing a list of events: "Downloading main.cvd [100%] 11:22:13", "main.cvd updated (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr) 11:22:38", "Downloading daily.cvd [100%] 11:23:15", and "daily.cvd updated (version: 25465, sigs: 1584853, f-level: 63, builder: raynman) 11:24:19".

Вкладка «Антивирус ClamAV». На данной вкладке отображается состояние служб «Антивирус ClamAV» и «Антивирусный прокси-сервер» с возможностью «Выключить» (или «Включить» если служба выключена). Служба «Антивирус ClamAV» отвечает за работоспособность предустановленного антивируса ClamAV, который проверяет почтовые письма, если установлен [соответствующий флаг](#), а также трафик HTTP и HTTPS, при условии запущенной службы «Антивирусный прокси-сервер» и [установленного флага](#) в настройках прокси-сервера. Соответственно служба «Антивирусный прокси-сервер» отвечает за передачу HTTP/HTTPS пакетов антивирусу ClamAV, при условии установленного флага в настройках прокси-сервера. В виджете службы «Антивирус ClamAV», также отображается: количество имеющихся сигнатур, текущие версии базы и антивируса ClamAV, время последнего обновления баз, кнопка «Обновить сейчас». Также последние события журнала за текущую дату.

Настройки

Антивирус ClamAV

Настройки

Журнал

Использовать в прокси

Проверять почту

Проверять наличие обновлений вирусных баз

Время начала проверки

Каждый час

00:00

следующая проверка 31.05.2019, 13:00:00

Обновлять вирусные базы при выключенном антивирусе

Сохранить

Обновить

Вкладка «Настройки». Данная вкладка предназначена для настройки работы антивируса ClamAV. Флаги «Использовать в прокси» и «Использовать в почте» соответствуют соответствующим флагам в настройках модулей «Прокси» и «Почта». Данные флаги включают антивирус ClamAV для фильтрации трафика, проходящего через прокси-сервер и вложения в почтовых письмах. Поле «Проверять наличие обновлений вирусных баз» позволяет задать частоту проверок обновлений баз антивируса. По умолчанию этот процесс будет запускаться каждый час, при условии установленного хотя бы одного флага на данной вкладке. При выборе периода «Каждый день» или «Раз в неделю», возможно указать «Время начала проверки». Флаг «Обновлять вирусные базы при выключенном антивирусе» позволит запускать проверку обновления баз при выключенной службе «Антивирус ClamAV».

Журнал

31.05.2019 - 31.05.2019 Сегодня Неделя Месяц Другой период

Экспорт Удалить логи Поиск...

| |
|--|
| freshclam daemon 0.101.2 (OS: freebsd11.2, ARCH: amd64, CPU: amd64) 11:20:33 |
| ClamAV update process started at Fri May 31 11:20:33 2019 11:20:33 |
| Downloading main.cvd [100%] 11:22:13 |
| main.cvd updated (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr) 11:22:38 |
| Downloading daily.cvd [100%] 11:23:15 |
| daily.cvd updated (version: 25465, sigs: 1584853, f-level: 63, builder: raynman) 11:24:19 |

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «Антивирус

ClamAV» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения - желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска, а также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

From:

<https://doc-old.a-real.ru/> - **Документация**

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:clamav&rev=1572508165>

Last update: **2020/01/27 16:28**

