

Table of Contents

Table of Contents	1
Журналы событий	2
Как настроить выгрузку журналов на FTP сервер	3
С какой периодичностью отсыдаются уведомления о переполнении памяти?	6

Как настроить выгрузку журналов на FTP сервер

Product: UserGate NGFW, UserGate LogAn

Version: 6.x, 7.x

Задача

Необходимо настроить выгрузку журналов за предыдущие сутки на FTP-сервер.

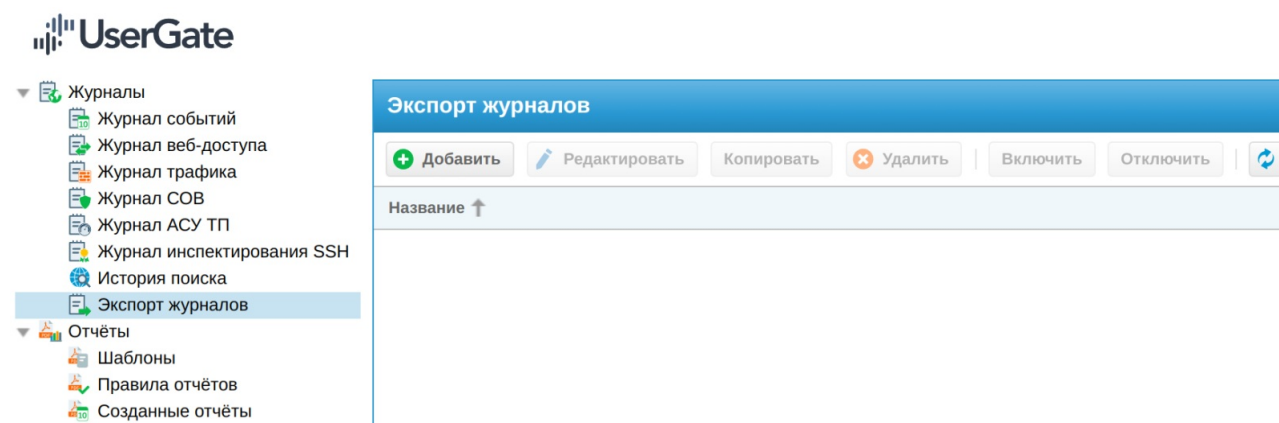
Решение

Функция экспорта журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или обработки. Подробную информацию о типах журналов и способах экспорта можно найти в разделе [Журналы](#) Руководства администратора.

При отправке журналов на серверы ftp и ssh UserGate сохраняет данные для отправки во временных файлах в кодировке UTF-8. Журналы за предыдущие дни (по количеству дней ротации) хранятся в виде архивов, журнал за текущий день не архивирован. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.

Для создания правила экспорта журналов необходимо выполнить следующие шаги:

1. В разделе **Журналы** → **Экспорт журналов** добавить новое правило:



2. На вкладке **Общие** установить флажок **Включено**, указать название нового правила и его краткое описание:

3. На вкладке **Удаленный сервер** указать параметры сервера, на который будут экспортироваться журналы:

Свойства правила экспорта журналов

Общие Удалённый сервер Журналы для экспорта Расписание

Тип сервера: FTP

Адрес сервера: 10.10.10.10

Порт: 21

пассивный режим: ☒

Логин: user

Пароль:

Путь на сервере: /Logs/

Проверить соединение Послать разово Сохранить Отмена

4. Нажать на кнопку **Проверить соединение** и убедиться в доступности сервера:

Свойства правила экспорта журналов

Общие Удалённый сервер Журналы для экспорта Расписание

Тип сервера: FTP

Адрес сервера:

Порт:

пассивный режим:

Логин:

Пароль:

Путь на сервере: /Downloads/Logs/

Проверить соединение Послать разово Сохранить Отмена

Проверить соединение

Успешно

Закрыть

4. На вкладке **Журналы для экспорта** установить период ротации журналов, выбрать тип экспортируемых журналов и их формат. Доступны следующие типы форматов:

- CEF;
- CEF Compact;
- JSON;
- @CEE: JSON;

Свойства правила экспорта журналов

Общие
Удалённый сервер
Журналы для экспорта
Расписание

Период ротации журналов (дней):
7

Журналы	Формат	Размер журнала
☐ Журнал DNS	JSON	—
☐ Журнал событий	JSON	—
☐ Журнал COB	JSON	—
☐ Журнал АСУ ТП	JSON	—
☐ Журнал инспектирования SSH	JSON	—
☐ Журнал трафика	JSON	—
☒ Журнал веб-доступа	JSON	—

Проверить соединение
Послать разово
Сохранить
Отмена

5. На вкладке **Расписание** указать периодичность и время выполнения данного правила. Если журнал необходимо экспортировать разово, нажать кнопку **Послать разово**:

Свойства правила экспорта журналов

Общие
Удалённый сервер
Журналы для экспорта
Расписание

☒ Ежедневно
Каждый день в [01:00](#)

☐ Еженедельно

☐ Ежемесячно

☐ Каждые ... часов

☐ Каждые ... минут

☐ Задать вручную

Проверить соединение
Послать разово
Сохранить
Отмена

6. Сохранить созданное правило экспорта журналов, нажав **Сохранить**.

Примечание Возможно сохранение журнала администратором вручную непосредственно из веб-консоли. При этом данные сохраняются только в формате CSV.

Примечание Если в настройках указан Log Analyzer, то обработка и экспорт журналов производятся сервером LogAn.

С какой периодичностью отсыдаются уведомления о переполнении памяти?

Version: 6.1.8, 6.1.9, 7.0.0, 7.0.1, 6.x, 7.x

Вопрос

С какой периодичностью отсыдаются уведомления о переполнении памяти?

Ответ

Проверка на переполнение памяти происходит раз в 10 секунд, при этом берется моментальное значение памяти. И если есть переполнение отсылается уведомление.

