Table of Contents

Table of Contents 1
Настройка раздела пользователи и устройства 2
- Настройка UserID агента 3
- Настройка профиля редистрибуции UserID 6

Настройка раздела пользователи и устройства

Настройка UserID агента

Documentation:
Product: LogAn
Version: 7.x

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI), Syslog (посредством стандартизированного протокола syslog RFC 3164, RFC 5424, RFC 6587) и RADIUS (начиная с релиза ПО 7.2.0). Подробнее о схеме работы UserID агента читайте в разделе Пользователи и устройства Руководства администратора LogAn.

Настройка UserID в CLI производится на уровне **users userid-agent**.

Настройка параметров UserID агента

Общие параметры UserID агента настраиваются с помощью команды:

Admin@nodename# set users userid-agent configurate-agent <parameters>

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
radius-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей по RADIUS-логу. (Опция доступна начиная с релиза ПО 7.2.0).
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале **Агент UserID**. Список может быть создан в разделе библиотек **(IP-адреса)**. Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID. **Важно!** При задании имени допустимо использовать символ астериск (*), но только в конце строки.
sync	Синхронизация пользователей с NGFW: • **on**; • **off**.

Настройка источника событий

Microsoft Active Directory

Для добавления Microsoft Active Directory в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent active-directory <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.

Параметр	Описание
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
sharing-profile	Профиль редистрибуции, который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).
users-catalogs	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Syslog-senders

Для добавления отправителя syslog в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent syslog-sender <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.
sharing-profile	Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID агента.** Подробнее читайте в разделе Syslog фильтры UserID агента.
users-catalogs	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Параметр	Описание
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

RADIUS-server

Данная опция доступна начиная с релиза ПО 7.2.0.

Для добавления RADIUS-сервера в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent radius-server <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адреса хостов, с которых UserGate будет получать события по протоколу RADIUS.
server-secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
default-domain	Имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
sharing-profile	Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.
attribute-for-group	Номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
attribute-for-name	Номер radius attribute type, в котором находится имя пользователя, по умолчанию 1.
users-catalogs	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Настройка профиля редистрибуции UserID

Documentation:
Product: LogAn
Version: 7.x

Профили редистрибуции UserID предназначены для определения круга устройств UserGate, на которые отправляется информация о найденных агентом UserID пользователях.

Настройка профилей редистрибуции UserID в CLI производится на уровне **users sharing-profile**.

Команда для настройки:

Admin@nodename# create users sharing-profile <parameters>

При настройке необходимо установить следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля (опционально).
sensors	Выбор сенсоров UserGate, на которые будет отправлена информация о пользователях.