

## Table of Contents

|                           |   |
|---------------------------|---|
| Table of Contents         | 1 |
| Пользователи и устройства | 2 |
| UserID агент              | 3 |
| Профили редистрибуции     | 6 |



Documentation: ☒  
Product: SIEM  
Version: 7.1.x

Описание

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI) и Syslog (посредством стандартизированного протокола syslog [RFC 3164](#), [RFC 5424](#), [RFC 6587](#)).

Схема работы

UserID агент периодически делает запрос в базу данных для поиска событий входов/выходов пользователей. Поиск происходит только среди записей, полученных при помощи источников UserID, то есть другие записи (полученные через WMI сенсоры, конечные устройства, сборщики логов) игнорируются. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя отправляются на все устройства NGFW, указанные в профиле редистрибуции источника. Таким образом производится авторизация пользователя на всех указанных устройствах. В случае выхода пользователя ситуация аналогична (за исключением Microsoft Active Directory, где данные о выходе пользователя на данный момент не обрабатываются). Информация о входе/выходе/ошибке сохраняется в журнал UserID.

**Примечание**События, полученные с источников, будут отображены в журналах UserID на рабочем столе Журналы и отчёты.

Настройка

В общем случае для настройки сбора информации с источников необходимо выполнить следующее:

| Наименование                                     | Описание                                                                                                             |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Настроить параметры агента UserID. | Настройка осуществляется в разделе <b>Пользователи и устройства → UserID агент</b> , кнопка <b>Настроить агент</b> . |
| <b>Шаг 2.</b> Настроить источник событий.        | В качестве источников могут быть использованы Microsoft Active Directory или Syslog.                                 |

При настройке агента необходимо заполнить следующие поля:

| Наименование                                                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Интервал опроса (сек.)</b>                               | Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Время жизни аутентифицированного пользователя (сек.)</b> | Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).                                                                                                                                                                                                                                                                                                                               |
| <b>Интервал мониторинга syslog (сек.)</b>                   | Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Ignore network list</b>                                  | Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале <b>Агент UserID</b> .<br><br>Список может быть создан в разделе <b>Библиотеки → IP-адреса</b> или при настройке агента (кнопка <b>Создать и добавить новый объект</b> ). Подробнее о создании и настройке списков IP-адресов читайте в разделе IP-адреса.<br><br>Данная настройка является глобальной и относится ко всем источникам. |
| <b>Ignore user list</b>                                     | Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD.<br><br>Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.<br><br><b>Важно!</b> При задании имени допустимо использовать символ астериск (*), но только в конце строки.                                                                         |

**Примечание**При подключении NGFW к Log Analyzer возможна одновременная работа агентов UserID, настроенных на обоих устройствах. Агенты устройств будут работать независимо друг от друга. События журналов агента UserID, полученные NGFW, как и события других журналов, будут переданы на LogAn.

## Microsoft Active Directory

В случае, если в качестве источника информации выступает Microsoft Active Directory необходимо:

| Наименование                                                                  | Описание                                                                                                   |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Настроить параметры агента UserID для мониторинга Microsoft AD. | Параметры агента UserID были рассмотрены ранее.                                                            |
| <b>Шаг 2.</b> Настроить источник событий.                                     | Настроить Microsoft Active Directory в качестве источника. Подробнее о параметрах источника читайте далее. |

При использовании серверов AD в качестве источников событий UserGate выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). Периодичность выполнения запросов регулируется настройками агента UserID (параметр **Интервал опроса**). Найденные события отображаются на рабочем столе **Журналы и отчёты**, в разделе **Журналы** → **Конечные устройства** → **Журнал событий**.

При добавлении источника событий типа Microsoft Active Directory необходимо указать следующие данные:

| Наименование                  | Описание                                                                                                                                                                                                      |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Включено</b>               | Включение/отключение получения журналов с источника.                                                                                                                                                          |
| <b>Название</b>               | Название источника.                                                                                                                                                                                           |
| <b>Описание</b>               | Описание источника (опционально).                                                                                                                                                                             |
| <b>Адрес сервера</b>          | Адрес Microsoft Active Directory.                                                                                                                                                                             |
| <b>Протокол</b>               | Протокол доступа к AD (WMI).                                                                                                                                                                                  |
| <b>Имя</b>                    | Имя пользователя для подключения к AD.                                                                                                                                                                        |
| <b>Пароль</b>                 | Пароль пользователя для подключения к AD.                                                                                                                                                                     |
| <b>Профиль редистрибуции</b>  | Профиль редистрибуции, который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел <a href="#">Профиль редистрибуции</a> .          |
| <b>Каталоги пользователей</b> | Предназначена для выбора LDAP-коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID.<br><br>Можно выбрать настроенный ранее каталог или добавить новый. |

## Syslog

**Примечание**Для корректной работы сборщика логов UserID, необходимо настроить сервер Syslog для отправки журналов на адрес агента UserID. Подробнее см. документацию Syslog.

Для настройки источника событий необходимо выполнить следующие действия:

| Наименование                                                                       | Описание                                                                                                                |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Разрешить сбор информации с удалённых устройств по протоколу syslog. | В разделе <b>Сеть</b> → <b>Зоны</b> разрешить сервис <b>Сборщик логов</b> для зоны, в которой находятся сервера Syslog. |
| <b>Шаг 2.</b> Настроить параметры агента UserID для мониторинга сервера syslog.    | Параметры агента UserID были рассмотрены ранее.                                                                         |
| <b>Шаг 3.</b> Настроить источник событий.                                          | Настроить сервер Syslog в качестве источника. Подробнее о параметрах источника читайте далее.                           |

При добавлении источника событий типа Syslog необходимо указать следующие параметры:

| Наименование           | Описание                                                                                                                                                                                                                     |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Включено               | Включение/отключение получения журналов с источника.                                                                                                                                                                         |
| Название               | Название источника.                                                                                                                                                                                                          |
| Описание               | Описание источника.                                                                                                                                                                                                          |
| Адрес сервера          | Адрес хоста, с которого UserGate будет получать события по протоколу syslog.                                                                                                                                                 |
| Домен по умолчанию     | Название домена, который используется для поиска найденных в журналах syslog пользователей.                                                                                                                                  |
| Часовой пояс           | Часовой пояс, установленный на источнике.                                                                                                                                                                                    |
| Профиль редистрибуции  | Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел <a href="#">Профиль редистрибуции</a> .                          |
| Фильтры                | Фильтры для поиска необходимых записей журнала.<br>Фильтры создаются и настраиваются в разделе <b>Библиотеки → Syslog фильтры UserID агента</b> . Подробнее читайте в разделе <a href="#">Syslog фильтры UserID агента</a> . |
| Каталоги пользователей | Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID.<br>Можно выбрать настроенный ранее каталог или добавить новый.                    |

Найденные события отображаются на рабочем столе **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

Documentation: ☒  
Product: SIEM  
Version: 7.1.x

Описание

Предназначены для определения круга устройств UserGate, на которые отправляется информация о найденных агентом UserID пользователях. Для добавления профиля необходимо нажать кнопку **Добавить** и настроить профиль.

| Наименование     | Описание                                                                                                                                                                                                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название         | Название профиля.                                                                                                                                                                                        |
| Описание         | Описание профиля (опционально).                                                                                                                                                                          |
| Сенсоры UserGate | Список устройств UserGate, на которые будет отправлена информация о найденных пользователях.<br>Добавление сенсоров доступно разделе <b>Сенсоры → Сенсоры UserGate</b> рабочего стола <b>Настройки</b> . |

**Примечание** По умолчанию создан профиль *Share with all UserGate sensors*, при выборе которого информация о пользователях будет отправлена на все сенсоры SIEM.

