

Table of Contents

Table of Contents	1
Настройка LogAn	2
Общие настройки	3
Управление устройством	4
Администраторы	7
Управление сертификатами	9
Профили оповещений	11
Серверы аутентификации	12

Общие настройки

Documentation: ☒

Version: 6.1.9

Product: LogAn

Раздел **Общие настройки** определяет базовые установки LogAn:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Настройка времени сервера	Настройка параметров установки точного времени. Использовать NTP — использовать сервера NTP из указанного списка для синхронизации времени. Основной сервер NTP — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org Запасной сервер NTP — адрес запасного сервера точного времени. Время на сервере — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS.
Состояние Log Analyzer	Отображается текущее состояние сервера LogAn: Состояние — показывает текущее состояние сервиса статистики. Версия устройства - версия LogAn.

Раздел **Управление устройством** определяет следующие установки LogAn:

- Настройки диагностики.
- Операции с сервером.
- Экспорт настроек..

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• Off — ведение журналов диагностики отключено. • Error — журналировать только ошибки работы сервера. • Warning — журналировать только ошибки и предупреждения. • Info — журналировать только ошибки, предупреждения и дополнительную информацию. • Debug — максимум детализации. Рекомендуется установить значение параметра Детализация диагностики в Error (только ошибки) или Off (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность LogAn.
Журналы диагностики	• Скачать журналы — скачать диагностические журналы для передачи их в службу поддержки UserGate. • Очистить журналы — очистить содержимое журналов.
Удаленный помощник	• Включено/Отключено — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу LogAn для диагностики и решения проблем. Для успешной активации удаленного помощника ЦК UserGate должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH. • Идентификатор удаленного помощника — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • Токен удаленного помощника — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить — перезагрузка сервера LogAn. • Выключить — выключение сервера LogAn.
Обновления	Выбор канала обновлений ПО LogAn: • Стабильные — проверка наличия стабильных обновлений ПО. • Бета — проверка наличия экспериментальных обновлений.

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта LogAn в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование LogAn](#)). При наличии обновлений в разделе **Управление продуктом** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя LogAn.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе Управление устройством при наличии оповещения Доступны новые обновления нажать на ссылку Установить сейчас . Система установит скачанные обновления, по окончании установки LogAn будет перезагружен.

Экспорт настроек

Администратор имеет возможность сохранить текущие настройки LogAn в файл и впоследствии восстановить эти настройки на этом же или другом сервере LogAn. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

ПримечаниеЭкспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать LogAn с помощью имеющегося ПИН-кода и настроить интерфейсы.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе Управление устройством → Экспорт настроек нажмите Экспорт и выберите Экспортировать все настройки или Экспортировать сетевые настройки. Система сохранит: • текущие настройки сервера под именем: logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename — имя узла LogAn. version — версия LogAn. YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, logan_core-logan_core@ranreahattha_6.1.8.13494RS-1_20211227_091350.bin или network-logan_core-logan_core@ranreahattha_6.1.8.13494RS-1_20211227_091407.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе Управление устройством нажать на ссылку Экспорт настроек → Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе Управление устройством → Экспорт настроек нажать кнопку Добавить , указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера — FTP или SSH. • Адрес сервера — IP-адрес сервера. • Порт — порт сервера. • Логин — учетная запись на удаленном сервере. • Пароль/Подтверждение пароля — пароль учетной записи. • Путь на сервере — путь на сервере, куда будут выгружены настройки.

Наименование	Описание
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7; • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"; • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".

Доступ к веб-консоли LogAn регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

Примечание При первоначальной настройке LogAn создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора	В разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: • Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы авторизации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы авторизации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Разрешения для API	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Объекты описаны документации API. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для веб-консоли	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для CLI	Позволяет разрешить доступ к CLI. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Администратор LogAn может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей	В разделе Администраторы → Администраторы нажать кнопку Настроить
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Сложный пароль — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как - минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • Число неверных попыток аутентификации — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на Время блокировки. • Время блокировки — время, на которое блокируется учетная запись.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования UserGate LogAn. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

Примечание Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

Documentation: ☒
Version: 6.1.9
Product: LogAn

LogAn использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции LogAn использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку Создать в разделе Сертификаты .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Страна — страна, в которой выписывается сертификат. • Область или штат — область или штат, в котором выписывается сертификат. • Город — город, в котором выписывается сертификат. • Название организации — название организации, для которой выписывается сертификат. • Common name — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • E-mail — e-mail вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в LogAn. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата — SSL веб-консоли. После этого LogAn перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

LogAn позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • Экспорт сертификата — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности UserGate LogAn не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и - опционально - приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку Импорт .

Наименование	Описание
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название - название сертификата, под которым он будет отображен в списке сертификатов. • Описание - описание сертификата. • Загрузите файл, содержащий данные сертификата. • Загрузите файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов - файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Профили оповещений

Version: 6.1.9

Product: LogAn

Documentation: ☒

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Авторизация	Включает авторизацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL - 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Серверы аутентификации

Version: 6.1.9
Product: LogAn
Documentation: ☒

Серверы аутентификации — это внешние источники учетных записей пользователей для аутентификации в веб-консоли управления LogAn. LogAn поддерживает только сервер аутентификации LDAP-коннектор. LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять аутентификацию пользователей через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена.

