Параметры безопасности

Параметры данной группы отсутствуют в настольных редакциях (Personal и Community).

Изменения настроек параметров безопасности вступают в силу после нажатия кнопки *Сохранить*.

Параметр	Значение по умолчанию	Описание
Всегда проверять все сертификаты	false	При значении `true` параметр включает принудительную проверку сертификатов на этапе установки TLS-соединения. Распространяется на Подключения: REST-сервис, SOAP-сервис, Kafka, Tableau сервер, MySQL, PostgreSQL, ClickHouse. Также на компоненты: JavaScript(Fetch API), Импорты файловые (по URL). Используется при аутентификации по LDAP, OpenID.
Всегда проверять все сертификаты HTTPS	false	При значении `true` параметр включает принудительную проверку сертификата сервера для HTTPS соединений. Распространяется на *Подключения*: *REST-сервис*, *SOAP-сервис*, *Tableau сервер*. Также на компоненты: *JavaScript (Fetch API)*, *Импорты файловые (по URL)*. Используется при аутентификации по *LDAP*, *OpenID*.

Параметр	**Значение по умолчанию**	**Описание**
OpenSSL приоритетнее SChannel для HTTPS	false	Только для OS Windows. Определяет, какой TLS-клиент будет использоваться компонентами *REST-сервис* и *SOAP-сервис* при работе по HTTPS. Логика выбора TLS-клиента следующая (условия проверяются по очереди): 1. Если был выполнен редирект с HTTP на HTTPS — используется OpenSSL. 2. Если в узле задан клиентский сертификат из хранилища Windows — используется SChannel. 3. Если используется клиентский сертификат из файла — используется OpenSSL. 4. Если в узле или *Параметрах безопасности* отключена проверка сертификата сервера — используется OpenSSL. Если ни одно из условий выше не выполняется, то проверяется значение параметра *OpenSSL приоритетнее SChannel для HTTPS*. Если оно равно `true`, то используется — OpenSSL. Во всех остальных случаях — используется SChannel.
Тайм-аут блокировки сессии (сек)	∞	Тайм-аут неактивности, по истечении которого сессия переходит в заблокированное состояние. Минимальное значение — 60 секунд, максимальное — 2000000 секунд (23 дня). Тайм-аут используется только для сессий, подключенных через websocket, т.е. для интерактивных сессий из веб-клиента.
Тайм-аут закрытия сессии (сек)	∞	Время до завершения сессии, по истечении которого происходит закрытие соединения с сервером при отсутствии действий со стороны пользователя. Минимальное значение — 60 секунд, максимальное — 2000000 секунд (23 дня). Тайм-аут используется только для сессий, подключенных через websocket, т.е. для интерактивных сессий из веб-клиента.
Переподключаться только с текущего IP	false	Включение данного параметра запрещает восстанавливать сессии с других IP-адресов. Нужно учитывать, что при включенной опции не получится восстановить сессию, если изменился провайдер сети или технология подключения, например, с Wi-Fi на 4G.

Параметр	**Значение по умолчанию**	**Описание**
Требовать аутентификацию при переподключении	false	При включении данного параметра для восстановления сессии потребуется повторно пройти аутентификацию
Лимит попыток ввода пароля	Отключено	Лимит, при достижении которого пользователь больше не сможет авторизоваться до тех пор, пока не истечет *Тайм-аут ввода пароля*. История неудачных попыток ввода пароля сбрасывается при перезапуске Loginom Server. Если будет превышено максимальное количество неудачных попыток входа в учётную запись с ролью "Пакетное выполнение", то до истечения тайм-аута ввода пароля станет недоступным выполнение пакетов из-под этой учётной записи через Integrator и BatchLauncher. Минимальное значение - 1 попытка, максимальное - 10000 попыток.
Тайм-аут ввода пароля (сек)	∞	Время ограничения, накладываемого на пользователя, превысившего *Лимит попыток ввода пароля*. Ограничение распространяется на все учётные записи, в том числе учётные записи с ролями *Администрирование* и *Пакетное выполнение*. Минимальное значение - 1 секунда, максимальное - 2000000 секунд, либо ∞. В случае, если установлен бесконечный тайм-аут (∞), то при достижении лимита попыток ввода пароля, пользователь больше не сможет залогиниться до тех пор, пока не будет перезапущен Loginom Server, либо администратор не изменит *Тайм-аут ввода пароля* или *Лимит попыток ввода пароля*.
Запрет мультисессионности для пользователей	false	Запрещает вход пользователю, если с этим же аккаунтом уже есть активная сессия. При разблокировке сессии, которая может быть заблокирована с помощью `Ctrl+Alt+L` , запрет не учитывается.

Параметр	Значение по умолчанию	Описание
Ограничение мультисессионности для администраторов	Нет	Выбор одного из трех вариантов ограничений для Администратора: *Нет*, *Запрет входа*, *Закрыть текущие сессии*. *Нет* - администраторы могут подключаться с одного аккаунта из нескольких мест. *Запрет входа(не рекомендуется)* - действует также как и запрет для пользователей. Не рекомендуется использовать этот режим или использовать его с заданными параметрами *Таймаут закрытия сессии* и *Период проверки соединения*, так как возможно появление незакрытых сессий, в следствие чего, вход с данного аккаунта администратора будет не доступен. *Закрыть текущие сессии* - закрывает существующие сессии с этим аккаунтом, перед повторным входом. Если закрыть сессию не получается, то вход с этим аккаунтом не разрешен.
URL для загрузки изображений	Загрузка изображений запрещена	При редактировании параметра открывается модальное окно, в котором можно задать разрешенные адреса. В адресах нужно использовать полный путь, начиная с протокола; разрешены только протоколы HTTP и HTTPS. Проверяется совпадение URL по начальным символам. При выборе режима *Любые* разрешается загрузка изображений с любых URL адресов. Настройка применяется при следующем входе в систему. Если в настройках веб-сервера Apache был добавлен конфиг `Content Security Policy` с директивой, ограничивающей адреса для загрузки изображений (`img-src`), то для отображения картинок в настройку этой директивы также необходимо прописать URL адреса хостов с изображениями.
URL для формирования ссылок	Формирование ссылок запрещено	При редактировании параметра открывается модальное окно, в котором можно задать разрешенные адреса. В адресах нужно использовать полный путь, начиная с протокола; разрешены только протоколы HTTP и HTTPS. Проверяется совпадение URL по начальным символам. При выборе режима *Любые* разрешается формирование ссылок с любых URL адресов. Настройка применяется при следующем входе в систему.