Безопасно ли использовать сервер Mobile SMARTS в открытом доступе

Последние изменения: 2024-03-26

> **Нет! Без принятия дополнительных мер защиты - небезопасно!**

Сервер Mobile SMARTS предназначен в первую очередь для использования во внутренней сети компании. Если Вы вынесли свой сервер на публичный IP-адрес, доступный в сети интернет, и злоумышленник узнал его адрес и порт, то он сможет беспрепятственно получить доступ к нему, просматривать Ваши данные и, возможно, нанести Вам ущерб или взломать компьютер.

> **Поэтому использовать сервер Mobile SMARTS в открытых сетях без использования дополнительных мер безопасности крайне не рекомендуется!**

Если вы публикуете сервер Mobile SMARTS с доступом из открытой сети на публично доступный IP-адрес, то необходимо принимать меры безопасности:

- Использовать специальный протокол https, который шифрует все передаваемые данные.
- Использовать аутентификацию по пользователю.

Вышеуказанные способы являются встроенными методами защиты сервера Mobile SMARTS. Дополнительно к ним Вы можете использовать следующие меры защиты:

- Поменять типовые порты сервера и баз Mobile SMARTS на уникальные.
- Настроить и использовать частную VPN компании для доступа к серверу;
- Установить на сервере антивирус, например Dr.Web для Windows Server;
- Создать для службы сервера Mobile SMARTS отдельную учетную запись с пониженными правами без доступа к запуску программ и системным папкам;
- По возможности настроить фаервол на доступ к портам сервера Mobile SMARTS и использовать фильтр по доверенным IP-адресам для доступа.

безопасность, сервер Mobile SMARTS

Не нашли что искали?

Задать вопрос в техническую поддержку