1/4

Последнее обновление: 12.09.2021 03:03

Настройки безопасности

Перейдите на вкладку «Настройки» в раздел «Настройки безопасности».

Пользователи: Редактировать		×
ФИО Петров		
Общая информация Контактные данные Настрой	іки Свойства	
Интерфейс Тема default Тип Обычный Использовать страницу выбора организации	Карта Тип маркера Размер курсора Иконка Маленький Курсор Обычный Иконка и курсор Большой Показывать названия Окацтовка товка	Сортировать ТС по Имени Серийному номеру прибора Свойству:
Настройки безопасности Срок жизни пароля 90 д (0 - смена па Допустимые IP Пример: 192.168.0.4/24, 192.16 Двухфакторная () отключена	роля не требуется) Сб 8.4.0/255.255.255.0, 192.168.2.3 О через электронную почту (petrov@gm	іросить пароль при следующем входе nail.com)
аутентификация через push-уведомлени через SMS (7951249188 Другие настройки	я vepes FIDO/U2F токен 38) vepes Google Authenticator	
Смещение UTC+5 • Показывать сообще	ния 5 сек 🗘	

Рис. 1: Настройки безопасности

Настройте следующие параметры безопасности для учетной записи:

- Срок жизни пароля, в днях. По истечении указанного срока вход в организации пользователя, используя текущий пароль, будет невозможен пользователю будет предложено сменить пароль. Значение 0 разрешает использование бессрочного пароля. Включите чек-бокс «Сбросить пароль при следующем входе» для отправки пользователя запроса смены пароля при следующем входе на web-сервер.
- Допустимые IP список IP-адресов (через запятую), с которых разрешено подключение к web-серверу, используя учетную запись пользователя.
- Двухфакторная аутентификация дополнительный метод идентификации пользователя при авторизации. Для отключения двухфакторной аутентификации выберите настройку «отключена». В этом случае для входа на web-сервер достаточно ввести логин и пароль на стартовой странице программы.

Ниже рассмотрены методы двухфакторной аутентификации, поддерживаемые в

текущей версии ПО «АвтоГРАФ.WEВ».

Через push-уведомления

Данный метод используется в мобильных приложениях АвтоГРАФ-MOBILE. После ввода пароля пользователя на мобильное устройство будет выслан код подтверждения в виде pushуведомления.

Через SMS

При использовании данного метода, после ввода пароля пользователя на номер телефона, указанный в настройках пользователя, будет выслано SMS-сообщение с кодом подтверждения. Номер телефона дублируется в скобках после настройки «через сервер».

Пример сообщения:

226029 IP Address: 192.168.6.180 Server: ag2new.tk-chel.ru

Через электронную почту

При использовании данного метода, после ввода пароля пользователя на адрес электронной почты, указанный в настройках пользователя, будет выслано письмо с кодом подтверждения. Адрес пользователя дублируется в скобках после настройки «через электронную почту». 6-значный код подтверждения указывается в теме письма. Отправитель письма — webmap@ag-navi.com.

Через FIDO/U2F токен

При выборе данного метода для авторизации пользователя в системе требуется подключение к компьютеру, с которого выполняется вход, USB-устройства (токена), поддерживающего протокол web-аутентфикации U2F.

Регистрация токена

Используемый токен должен быть зарегистрирован. Для этого подключите токен к компьютеру по интерфейсу USB и нажмите кнопку «Регистрировать».

30.04.2025 00:35

3/4

Настройки безопасн	ости		
Срок жизни пароля	90 д 🖕 (0 - смена пароля	(0 - смена пароля не требуется) Сбросить пароль	
Допустимые IP	Пример: 192.168.0.4/24, 192.168.4.	0/255.255.255.0, 192.168.2.3	
Двухфакторная аутентификация	отключена через push-уведомления через SMS (79512491888)	 через электронную почту (ре через FIDO/U2F токен Регис через Google Authenticator 	trov@gmail.com) трировать токен

Рис. 2: Регистрация токена

Через Google Authenticator

При использовании данного метода для авторизации пользователя в системе требуется ввод кода из мобильного приложения Google Authenticator.

Google Authenticator — это мобильное приложение, доступное для OS iOS и Android и предназначенное для создания кодов двухэтапной аутентификации с привязкой к учетной записи. Приложение доступно для скачивания в App Store и Google Play.

Для использования данного метода необходимо зарегистрировать приложение Google Authenticator.

Для этого нажмите кнопку «Регистрировать приложение».

Настройки безопасн	юсти	
Срок жизни пароля	90 д 🔶 (0 - смена пароля н	не требуется) Сбросить пароль при следующем входе
Допустимые ІР	Пример: 192.168.0.4/24, 192.168.4.0/	255.255.255.0, 192.168.2.3
Двухфакторная аутентификация	отключена через push-уведомления через SMS (79512491888)	 через электронную почту (petrov@gmail.com) через FIDO/U2F токен через Google Authenticator Регистрировать приложение

Рис. 3: Регистрация приложения

На экране появится QR-код, который необходимо считать с помощью функции «Сканировать QR-код» в приложении Google Authenticator на вашем телефоне. После этого аккаунт пользователя будет сохранен в приложении.

При входе пользователя на web-сервер нужно будет ввести код подтверждения, сгенерированный в приложении Google Authenticator для сохраненной учетной записи.

Для отключения привязки учетной записи с экземпляром приложения Google Authenticator нажмите кнопку «Отозвать приложение».

Двухфакторная аутентификация,, токен,, Google Authenticator,, безопасность

From: http://wiki.tk-chel.ru/ - Документация АвтоГРАФ.WEB

Permanent link: http://wiki.tk-chel.ru/admin/users/settings/security



Last update: 12.09.2021 03:03