

Windows

В данной статье описано, как создать агент инициализации **Windows**.

Создание нового агента инициализации Windows

Для того чтобы создать новый агент инициализации, нажмите **Новый агент инициализации** в левом верхнем углу страницы и в выпадающем списке выберите тип агента Windows. После этого откроется меню конфигурации нового агента инициализации.

Новый агент инициализации **Windows** ✕

1

ID инициализации

Требуется указать идентификатор.

2

Описание

3

Обеспечить выполнение

☒

Включено

При активации данного параметра агент инициализации будет принудительно использоваться при проверке соответствия устройства политикам безопасности во время RADIUS- или portalной аутентификации.

4

Авторегистрация

☐

Отключено

При активации данного параметра устройства, авторизованные в агенте инициализации, будут зарегистрированы в сети автоматически.

5

Применить роль

☐

Отключено

При активации данного параметра настроенная роль будет применяться к конечному устройству, если оно авторизовано в агенте инициализации.

6

Применяемая роль

Если опция "Применить роль" активна, она будет определять роль, которая будет применяться при авторизации устройства у провайдера.

7

Роли

Изменения коснутся узлов с выбранными ролями.

8

SSID

Требуется указать SSID.

9

Открытый SSID

☒

Включено

При активации данного параметра беспроводная сеть будет отображаться в списке доступных подключений.

10

Тип безопасности

Выберите тип защиты, применяемый для вашего SSID.

11

WinRS scanner

Select the winrs scanner to setup. Leave empty for no scanner.

Создать

Сбросить

Отмена

В данном меню доступны следующие настройки:

- ID инициализации** — идентификатор агента инициализации, который будет отображаться в таблице со списком всех агентов. Задается при создании агента инициализации и не может быть изменен в дальнейшем;
- Описание** — описание агента инициализации, которое будет отображаться в таблице со списком всех агентов;
- Обеспечить выполнение** — при активации данного параметра агент инициализации будет принудительно использоваться при проверке соответствия устройства политикам безопасности во время portalной или RADIUS-аутентификации;
- Авторегистрация** — при активации данного параметра устройства, авторизованные с помощью агента инициализации, будут зарегистрированы в сети автоматически;
- Применить роль** — при активации данного параметра указанная ниже роль будет применяться к конечному устройству, если оно авторизовано с помощью агента инициализации;
- Применяемая роль** — если параметр **Применить роль** активен, она будет определять роль, которая будет применяться при авторизации устройства через агент инициализации;
- Роли** — список ролей, к которым будет применяться агент инициализации. Изменения затронут только узлы, относящиеся к выбранным ролям;

8. **SSID** — идентификатор беспроводной сети, для которой будет использоваться агент инициализации;
9. **Открытый SSID** — при активации данного параметра беспроводная сеть будет отображаться в списке доступных подключений;
10. **Тип безопасности** — тип защиты, применяемый в указанной беспроводной сети. Возможные варианты:
 - **Открытые** — подключение без применения механизмов шифрования;
 - **WEP** — тип защиты с базовым уровнем шифрования. При выборе данного типа защиты появляются дополнительные поля для заполнения: **Включить DPSK**, **Использовать локальный пароль для DPSK повторно**, **Ключ Wi-Fi**;
 - **WPA** — протокол защиты с улучшенной криптографией по сравнению с WEP. При выборе данного типа защиты появляются дополнительные поля для заполнения: **Включить DPSK**, **Использовать локальный пароль для DPSK повторно**, **Ключ Wi-Fi**;
 - **WPA2** — актуальный и надежный тип защиты, использующий AES-шифрование. При выборе данного типа защиты появляются дополнительные поля для заполнения: **Тип EAP**, **Включить DPSK**, **Использовать локальный пароль для DPSK повторно**;
 - **WinRS scanner** — поле для выбора предварительно настроенного механизма сканирования, для которого агент инициализации создаст учетную запись. В данном поле будут доступны механизмы сканирования, у которых в качестве метода аутентификации выбрано значение **По сертификату** или **Базовый через HTTPS**.
11. **WinRS scanner** — поле для выбора предварительно настроенного механизма сканирования, для которого агент инициализации создаст учетную запись. В данном поле будут доступны механизмы сканирования, у которых в качестве метода аутентификации выбрано значение **По сертификату** или **Базовый через HTTPS**.

Дополнительные настройки, появляющиеся при выборе определенных параметров

Тип безопасности — WEP, WPA

Тип безопасности: **WEP**
Выберите тип защиты, применяемый для вашего SSID.

1. Включить DPSK ☐ Отключено
Данный параметр отвечает за генерацию PSK.

2. Использовать локальный пароль для DPSK повторно ☐ Отключено
Если включена функция DPSK и у пользователя есть локальная учетная запись с паролем в виде простого текста, вместо генерации нового PSK этот пароль будет использоваться повторно. Данная функция будет работать только с локальными пользователями, для которых существует пароль в виде простого текста.

3. Ключ Wi-Fi

Тип безопасности: **WPA**
Выберите тип защиты, применяемый для вашего SSID.

1. Включить DPSK ☐ Отключено
Данный параметр отвечает за генерацию PSK.

2. Использовать локальный пароль для DPSK повторно ☐ Отключено
Если включена функция DPSK и у пользователя есть локальная учетная запись с паролем в виде простого текста, вместо генерации нового PSK этот пароль будет использоваться повторно. Данная функция будет работать только с локальными пользователями, для которых существует пароль в виде простого текста.

3. Ключ Wi-Fi

1. **Включить DPSK** — при активации данного параметра генерируется PSK;
2. **Использовать локальный пароль для DPSK повторно** — при активации данного параметра не будет производиться повторная генерация пароля для пользователя, у которого есть локальная учетная запись с паролем в открытом виде;
3. **Ключ Wi-Fi** — пароль от Wi-Fi-сети, к которой подключается пользователь.

Тип безопасности — WPA2, тип EAP — No EAP

Тип безопасности: WPA2
Выберите тип защиты, применяемый для вашего SSID.

1 Тип EAP: No EAP
Выберите тип EAP для вашего SSID. Оставьте это поле пустым, если EAP не используется.

2 Включить DPSK: ☐ Отключено
Данный параметр отвечает за генерацию PSK.

3 Использовать локальный пароль для DPSK повторно: ☐ Отключено
Если включена функция DPSK и у пользователя есть локальная учетная запись с паролем в виде простого текста, вместо генерации нового PSK этот пароль будет использоваться повторно. Данная функция будет работать только с локальными пользователями, для которых существует пароль в виде простого текста.

4 Ключ Wi-Fi:

1. **Тип EAP** — тип EAP для вашего SSID. Оставьте это поле пустым, если EAP не используется;
2. **Включить DPSK** — при активации данного параметра генерируется PSK;
3. **Использовать локальный пароль для DPSK повторно** — при активации данного параметра не будет производиться повторная генерация пароля для пользователя, у которого есть локальная учетная запись с паролем в открытом виде;
4. **Ключ Wi-Fi** — пароль от Wi-Fi-сети, к которой подключается пользователь.

Тип безопасности — WPA2, тип EAP — PEAP

Тип безопасности: WPA2
Выберите тип защиты, применяемый для вашего SSID.

Тип EAP: PEAP
Выберите тип EAP для вашего SSID. Оставьте это поле пустым, если EAP не используется.

1 Файл сертификата сервера RADIUS: Требуется сертификат.
Путь к сертификату RADIUS-сервера.

2 Файл CA сервера RADIUS: Требуется сертификат.
Путь к центру сертификации RADIUS-сервера, где подписан сертификат RADIUS-сервера.

1. **Файл сертификата сервера RADIUS** — путь к сертификату RADIUS-сервера;
2. **Файл CA сервера RADIUS** — путь к центру сертификации RADIUS-сервера, где подписан сертификат RADIUS-сервера.

Тип безопасности — WPA2, тип EAP — EAP-TLS.

Тип безопасности: WPA2
Выберите тип защиты, применяемый для вашего SSID.

Тип EAP: EAP-TLS
Выберите тип EAP для вашего SSID. Оставьте это поле пустым, если EAP не используется.

1 PKI-провайдер:

1. **PKI-провайдер** — провайдеры для управления инфраструктурой открытых ключей (PKI). PKI-провайдера можно создать на вкладке **Конфигурация** → **Политика и контроль доступа** → **Расширенные настройки доступа** → **PKI-провайдеры**.

Для того чтобы создать новый агент инициализации, заполните параметры конфигурации и нажмите **Создать**. Чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для возвращения на предыдущую страницу без сохранения выполненных на странице действий, нажмите **Отменить**.

Ревизия: 3

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.2.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Расширенные настройки доступа» -> Страница «Агенты инициализации» -> Windows

<https://docs.axel.pro/entry/1996/>