# Профили подключения

## Использование профиля подключения по умолчанию (default)

AxelNAC имеет предустановленный профиль подключения по умолчанию — **default**. Ниже приведены параметры, которые нужны для настройки того, будет ли использоваться стандартный профиль подключения или будет создан новый:

## URL для переадресации

Данный параметр находится в разделе **Конфигурация → Политики и контроль доступа → Профили подключения →** ***Выбранный вами профиль*** **→ Captive-портал**.

При использовании некоторых браузеров предпочтительнее перенаправлять пользователя на определенный URL, а не на тот, на который он изначально собирался перейти. Для таких браузеров URL, заданный в строке **URL для переадресации**, будет являться тем адресом, на который будет перенаправлен пользователь. Данный параметр затрагивает работу браузеров Firefox, начиная с версии 3.

## IP-адрес обнаружения в сети

Данный параметр находится в разделе **Конфигурация → Расширенные настройки доступа → Captive-портал** .

Этот IP используется в качестве веб-сервера, на котором размещен файл **common/network-access-detection.gif**, представляющий собой пиксельную картинку, используемую для обнаружения доступа к сети. Этот IP-адрес не может быть доменным именем, поскольку он используется во время регистрации и изоляции, когда DNS еще закрыт. Рекомендуется разрешить пользователям обращаться к серверу AxelNAC с помощью IP-адреса локальной сети AxelNAC.

В некоторых случаях может быть представлен другой Captive-портал (см. ниже о доступных настройках) в соответствии с SSID, VLAN, IP/MAC-адресом коммутатора или URI, к которому подключается клиент. Для этого в AxelNAC используется концепция профилей подключения, обеспечивающая такую возможность.

Ниже приведены различные параметры конфигурации для каждого профиля подключения. Единственным обязательным параметром является **Фильтр** — без него AxelNAC не сможет корректно применить профиль подключения.

При настройке профили подключения будут переопределять значения по умолчанию. Если ваше соединение не подпадает ни под один из заданных фильтров, AxelNAC будет использовать значения параметров из профиля подключения **default**.

Управление профилями подключений осуществляется из веб-интерфейса AxelNAC — в разделе **Конфигурация → Политики и контроль доступа → Профили подключения**.

При добавлении нового профиля подключения создается копия стандартного шаблона, в который пользователь может внести изменения.

## Фильтрация подключений

Данный параметр находится в разделе **Конфигурация → Политики и контроль доступа → Профили подключения →** ***Выбранный вами профиль***.

Для работы с фильтрами необходимо выбрать оператор фильтрации. При выборе значения **any** конечное устройство будет попадать в данный профиль при соблюдении любого из выбранных фильтров. Если выбрано значение **all**, конечное устройство будет попадать в данный профиль подключения только при соблюдении всех выбранных фильтров, в том числе расширенных.

В AxelNAC реализована фильтрация по следующим параметрам:

- Протокол аутентификации;
- Тип подключения;
- Сеть;
- Роль узла;
- Порт;
- Область;
- SSID;
- Сетевое устройство;
- Группа сетевых устройств;
- MAC-адрес сетевого устройства;
- Порт сетевого устройства;
- Период времени;
- URI;
- FQDN:
- VLAN.

Пример использования фильтров:

- SSID: Guest-SSID;
- VLAN: 100;
- Порт сетевого устройства: <SwitchId>-<Port>;
- Сеть: IP-адрес или CIDR сети.

Фильтрация по роли узла может быть использована только для соединений 802.1X и совместно с фильтром по VLAN.

## Расширенные фильтры

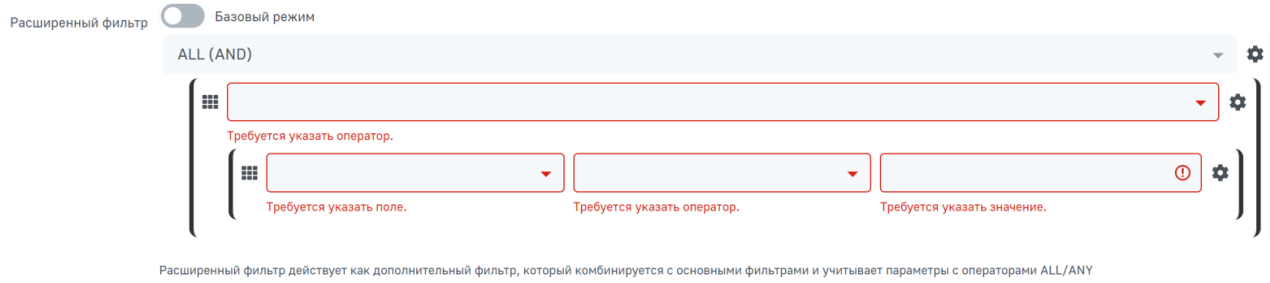
Данный параметр находится в разделе **Конфигурация → Политики и контроль доступа → Профили подключения →** ***Выбранный вами профиль***.

Для профиля подключения можно задать расширенный фильтр соответствия определенным атрибутам. Данный фильтр может быть

задан как в базовом, так и в расширенном режиме.

## Базовый режим

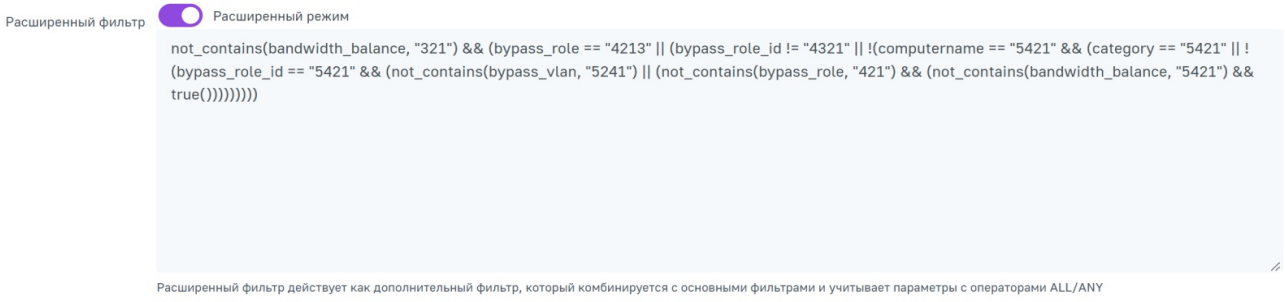
В базовом режиме вы можете настроить дополнительные фильтры с помощью операторов и значений. Для того, чтобы добавить новую строку, нажмите на иконку шестеренки справа от поля выбора оператора и выберите тип строки, которую вы хотите добавить.




Для того, чтобы клонировать или удалить строку, вы также можете использовать иконку шестеренки.

## Расширенный режим

Для переключения в расширенный режим, активируйте переключатель сверху от формы выбора параметров расширенных фильтров. В данном режиме вы можете настроить расширенные фильтры с помощью синтаксиса, описанного ниже.




## Синтаксис расширенного режима конфигурации фильтров.

Ниже приведены примеры атрибутов, операторов и значений.

**Атрибуты предыдущих подключений (база данных, профилирование):**

autoreg
status
bypass_vlan
bandwidth_balance
regdate
bypass_role
device_class
device_type
device_version
device_score
pid
machine_account
category
mac
last_arp
lastskip
last_dhcp
user_agent
computername
dhcp_fingerprint
detect_date
voip
notes
time_balance
sessionid
dhcp_vendor
unregdate
fingerbank_info.device_name
fingerbank_info.device_fq
fingerbank_info.device_hierarchy_names
fingerbank_info.device_hierarchy_ids
fingerbank_info.score
fingerbank_info.version
fingerbank_info.mobile
radius_request.User-Name
radius_request.username

radius_request.Called-Station-Id
radius_request.Calling-Station-Id
radius_request.NAS-Identifier
radius_request.NAS-IP-Address
radius_request.NAS-Port-Id

Использование атрибута **radius_request.NAS-Port-Id** может вызвать некорректную работу сканера WinRS. При использовании сканера WinRS в профиле подключения рекомендуется использовать базовый фильтр с параметром **Порт**.

**Атрибуты текущего подключения:**

connection_sub_type
connection_type
switch
port
vlan
ssid
dot1x_username
realm
machine_account

**Операторы:**

&& — и
|| — или
!= — не равно
== — равно
() — приоритет группы

**Значения:**

В качестве значений могут быть использованы как цифровые выражения, так и буквы латинского алфавита.
Значение __NULL__ может быть использовано для поиска пустых значений параметров в базе данных.

## Примеры использования расширенных фильтров

**Соответствие машинной аутентификации на защищенном беспроводном ssid:**

machine_account!= "" && connection_type == Wireless-802.11-EAP

**Соответствие машинной аутентификации от предыдущего подключения и подключение на защищенном ssid:**

machine_account!= "" && ssid == Secure

**Соответствие пользовательской и машинной аутентификации на защищенном ssid:**

last_connection_type == "Wireless-802.11-EAP" && machine_account!= "" && last_dot1x_username!~ "^host/"

**Соответствие пользовательской аутентификации без машинной аутентификации на защищенном ssid:**

last_connection_type == "Wireless-802.11-EAP" && (machine_account == "" || machine_account == __NULL__) && last_dot1x_username!~ "^host/"

**Соответствие без учета машинной аутентификации (BYOD):**

machine_account == __NULL__

**Пример фильтрации по атрибутам:**

1 'radius_request' => {
2 'NAS-Port-Type' => 15,
3 'Service-Type' => 2,
4 'State' => '0x7cfd15627dba0f5a45baee16526652a6',
5 'Called-Station-Id' => '00:8e:73:5d: f6:9e',
6 'FreeRADIUS-Proxied-To' => '127.0.0.1',
7 'Realm' => 'null',
8 'EAP-Type' => 26,
9 'NAS-IP-Address' => '172.30.255.13',
10 'NAS-Port-Id' => 'GigabitEthernet1/0/30',
11 'SQL-User-Name' => 'gwten',
12 'Calling-Station-Id' => '00:11:22:33:44:55',
13 'AxelNAC-Domain' => 'ZAYM',
14 'Cisco-AVPair' => 'service-type=Framed',
15 'User-Name' => 'zaym',
16 'Event-Timestamp' => 'Aug 15 2019 17:10:03 BST',
17 'EAP-Message' => '0x024700061a03',
18 'Framed-IP-Address' => '172.30.250.149',
19 'NAS-Port' => 50130,
20 'Stripped-User-Name' => 'gwten',
21 'Framed-MTU' => 1500
22 },
23 'autoreg' => 'yes',
24 'last_port' => '37',
25 'device_class' => 'Windows OS',
26 'bandwidth_balance' => undef,
27 'bypass_role' => undef,
28 'device_type' => 'Windows OS',
29 'pid' => 'gwten',

```
30 'dhcp6_enterprise' => '',
31 'last_seen' => \ [
32 'NOW ()'
33 ],
34 'dhcp6_fingerprint' => '',
35 'category' => 'Wire',
36 'mac' => '00:11:22:33:44:55',
37 'portal' => 'Wire',
38 'lastskip' => '0000—00—00 00:00:00',
39 'eap_type' => 26,
40 'last_dhcp' => '0000—00—00 00:00:00',
41 'user_agent' => 'ccmhttp',
42 'computername' => 'zamtop',
43 'dhcp_fingerprint' => '1,15,3,6,44,46,47,31,33,121,249,43',
44 'detect_date' => '2019—08—15 15:33:30',
45 'last_vlan' => '0',
46 'last_connection_sub_type' => 26,
47 'fingerbank_info' => {
48 'device_fq' => 'Операционная система/Windows OS',
49 'device_name' => 'Windows OS',
50 'version' => '',
51 'score' => '73',
52 'mobile' => 0,
53 'device_hierarchy_names' => [
54 'Windows OS',
55 'Операционная система'
56 ],
57 'device_hierarchy_ids' => [
58 1,
59 16879
60 ]
61 },
62 'bypass_role_id' => undef,
63 'last_role' => 'Wire',
64 'dhcp_vendor' => 'MSFT 5.0',
65 'unregdate' => '2019—08—15 20:10:04',
66 'last_switch' => '172.20.20.1',
67 'auto_registered' => 1,
68 '__from_table' => 1,
69 'source' => 'Wire',
70 'last_ifDesc' => 'GigabitEthernet1/0/30',
71 'device_version' => '',
72 'status' => 'reg',
73 'bypass_vlan' => undef,
74 'regdate' => '2019—08—15 17:10:04',
75 'last_dot1x_username' => 'zayme',
76 'tenant_id' => '1',
77 'category_id' => '166',
78 'machine_account' => '',
79 'last_connection_type' => 'Ethernet-EAP',
80 'last_ssid' => '',
81 'realm' => 'null',
82 'last_ip' => '172.20.20.2',
83 'device_score' => '73',
84 'last_arp' => '0000—00—00 00:00:00',
85 'last_start_timestamp' => '1565885356',
86 'stripped_user_name' => 'zayme',
87 '__old_data' => {
88 'autoreg' => 'yes',
89 'device_class' => 'Windows OS',
90 'bandwidth_balance' => undef,
91 'bypass_role' => undef,
92 'device_type' => 'Windows OS',
93 'pid' => 'gwten',
94 'dhcp6_enterprise' => '',
95 'last_seen' => '2019—08—15 16:09:16',
96 'dhcp6_fingerprint' => '',
97 'category' => 'Wire',
98 'mac' => '00:11:22:33:44:55',
99 'lastskip' => '0000—00—00 00:00:00',
100 'last_dhcp' => '0000—00—00 00:00:00',
101 'user_agent' => 'ccmhttp',
102 'dhcp_fingerprint' => '1,15,3,6,44,46,47,31,33,121,249,43',
103 'computername' => 'zamtop',
104 'detect_date' => '2019—08—15 15:33:30',
105 'bypass_role_id' => undef,
106 'dhcp_vendor' => 'MSFT 5.0',
107 'unregdate' => '2019—08—15 20:09:16',
108 'device_version' => '',
109 'status' => 'reg',
110 'bypass_vlan' => undef,
111 'regdate' => '2019—08—15 17:09:16',
112 'category_id' => '166',
113 'tenant_id' => '1',
114 'machine_account' => undef,
```

```
115 'last_arp' => '0000—00—00 00:00:00',
116 'device_score' => '73',
117 'voip' => 'no',
118 'device_manufacturer' => 'Toshiba',
119 'notes' => 'AUTO-REGISTERED',
120 'time_balance' => undef,
121 'sessionid' => undef
122 },
123 'voip' => 'no',
124 'device_manufacturer' => 'Toshiba',
125 'notes' => 'AUTO-REGISTERED',
126 'time_balance' => undef,
127 'last_switch_mac' => '00:8e:73:5d: f6:9e',
128 'sessionid' => undef,
129 'last_start_time' => '2019—08—15 16:09:16'
```

AxelNAC использует Apache для работы с Captive-порталом, веб-интерфейсом и веб-службами. Конфигурация AxelNAC Apache находится в каталоге **/usr/local/pf/conf/httpd.conf.d/**. В этом каталоге находятся конфигурационные файлы служб, используемых для следующих целей:

- **httpd.admin:** управление веб-интерфейсом AxelNAC;
- **httpd.portal:** управление интерфейсом Captive-портала AxelNAC;
- **httpd.webservices:** управление интерфейсом веб-сервисов AxelNAC;
- **httpd.aaa:** управление входящими запросами RADIUS.

Эти файлы динамически генерируются с помощью языка **Perl**, а службы активируются только на тех сетевых интерфейсах, которые необходимы для каждой цели. Остальные файлы в этом каталоге управляются AxelNAC с помощью шаблонов, поэтому их легко модифицировать в зависимости от конфигурации. Для обеспечения безопасности доступа по умолчанию включена работа протокола **SSL**.

В процессе установки в каталоге **/usr/local/pf/conf/ssl/** будут созданы самоподписанные сертификаты (**server.key** и **server.crt**). Эти сертификаты могут быть в любой момент заменены сертификатами сторонних производителей или существующими сертификатами **wildcard**. Обратите внимание, что значение **CN (Common Name)** должно совпадать с именем, заданным в конфигурационном файле AxelNAC **/usr/local/pf/conf/pf.conf**.

## Повторное использование учетных данных 802.1X

При определенных обстоятельствах (например, для демонстрации **Политики допустимого использования (AUP)** после успешного подключения по 802.1X) может использоваться «эмуляция SSO», чтобы пользователю не нужно было повторно вводить свои учетные данные на портале после их ввода в режиме 802.1X-EAP. Для этого необходимо активировать параметр **Использовать учётные данные dot1x повторно** в профиле подключения.

Имя пользователя, использованное во время подключения с использованием 802.1X, будет использоваться с различными источниками аутентификации для повторного определения роли на портале. В качестве меры предосторожности эта опция будет повторно использовать учетные данные 802.1X только при наличии источника аутентификации, соответствующего указанному домену. Это означает, что если пользователи используют учетные данные 802.1X с частью домена (username@domain, domain\username), то часть домена должна быть настроена как домен в разделе RADIUS, а источник аутентификации должен быть настроен для этого домена. Если пользователи не используют учетные данные 802.1X с доменной частью, то будет сопоставлена только NULL-область (если для нее настроен источник аутентификации).

---

ID статьи: 68
Последнее обновление: 17 мар., 2025
Обновлено от: Егоров В.
Ревизия: 8
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Расширенная конфигурация доступа -> Профили подключения
https://docs.axel.pro/entry/68/