

Вкладка «RADIUS»

Вкладка «RADIUS» предназначена для управления сертификатами, используемыми сервером RADIUS. На данной вкладке можно просматривать действующие сертификаты RADIUS, проверять их валидность, формировать запросы на подписание (CSR), а также редактировать параметры сертификатов и управлять доверенными центрами сертификации.

Блок «Просмотреть сертификаты RADIUS»

В данном блоке можно просматривать действующие сертификаты RADIUS.

Сертификат сервера RADIUS — действующий сертификат RADIUS.

RADIUS Сертификат(ы) центра сертификации — сведения о сертификатах доверенных центров.

SSL-сертификаты

HTTP RADIUS

Просмотреть сертификаты RADIUS

Редактировать сертификаты RADIUS

Сгенерировать запрос подписи (CSR)

Сертификат сервера RADIUS

1	Сертификат и ключ совпадают
2	Цепочка действительна
3	Серийный номер 01
4	Эмитент C=FR, ST=Radius, L=Somewhere, O=Example Inc., emailAddress=admin@example.org, CN=Example Certificate Authority
5	Не ранее Jun 24 16:53:22 2025 GMT
6	Не позднее Jun 23 16:53:22 2030 GMT
7	Тема C=FR, ST=Radius, O=Example Inc., CN=Example Server Certificate, emailAddress=admin@example.org
8	Common name (CN) Example Server Certificate, emailAddress=admin@example.org
9	Альтернативные названия темы

RADIUS Сертификат(ы) центра сертификации

3	Серийный номер 1DF04BE238B342330E1472FD79826633BA6551B5
4	Эмитент C=FR, ST=Radius, L=Somewhere, O=Example Inc., emailAddress=admin@example.org, CN=Example Certificate Authority
5	Не ранее Jun 24 16:53:22 2025 GMT
6	Не позднее Jun 23 16:53:22 2030 GMT
7	Тема C=FR, ST=Radius, L=Somewhere, O=Example Inc., emailAddress=admin@example.org, CN=Example Certificate Authority
8	Common name (CN) Example Certificate Authority
9	Альтернативные названия темы

Редактировать

В блоке присутствуют следующие информационные поля:

- Сертификат и ключ совпадают** — показывает, валиден ли сертификат и соответствует ли закрытый ключ сертификату;
- Цепочка действительна** — отражает корректность и действительность цепочки сертификатов до доверенного центра сертификации или самоподписанного сертификата;
- Серийный номер** — уникальный идентификатор сертификата, отображающий SHA1-хэш открытой части сертификата;
- Эмитент** — организация или центр сертификации, выдавший сертификат;
- Не ранее** — дата, начиная с которой сертификат считается действительным;
- Не позднее** — дата окончания срока действия сертификата;
- Тема** — данные владельца сертификата;
- Common name (CN)** — основное имя субъекта, указанное в сертификате;
- Альтернативные названия темы** — дополнительные имена субъекта, на которые распространяется действие сертификата.

Чтобы отредактировать параметры сертификата, нажмите **Редактировать**.

В случае, если необходимо сгенерировать новый запрос подписи сертификата (CSR), который может быть отправлен в центр сертификации для получения действительного SSL-сертификата, нажмите **Сгенерировать запрос подписи (CSR)**. При нажатии открывается окно с параметрами, которые необходимо заполнить.

Сгенерировать запрос на подпись сертификата RADIUS

1 Страна Требуется указать страну.

2 Состояние ! Требуется указать область.

3 Город ! Требуется указать город.

4 Название организации ! Требуется указать имя организации.

5 Common name ! Требуется Common name.

Закрыть **Сгенерировать**

В данном меню необходимо заполнить следующие параметры:

- Страна** — страна владельца сертификата;
- Состояние** — регион или область владельца сертификата;
- Город** — город владельца сертификата;
- Название организации** — официальное наименование организации, которой принадлежит сертификат;
- Common name** — имя субъекта.

Чтобы сгенерировать запрос, заполните все параметры и нажмите **Сгенерировать**. При этом откроется новое окно, в котором находится сертификат.

Сгенерировать запрос на подпись сертификата RADIUS

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICsjCCAQAwTTELMAkGA1UEBhMCQVgxDTALBgNVBAgMBM0QwrkxETAPBgNV  
BAcMCMORwobDKMK5MQ0wCwYDVQQDAtDKyMQ0wCwYDVQQDDATDkcKPMIIBIJAN  
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2eu57WxV4XvVWacZ1vkGE3aRimi6  
80wlkxkxxqaFHH13HJcVkcP7XiDEghkaslCrkjHL0aTKetrTPMl87yHScrldb6  
6c/KgqF9xS0+fZEfHPnaNsCaY36Zy4u402GQGbgUkVpPg7eeep5x6G90Kz6s5UG0I  
GTd7y8D0++y12yRSYUykg4vu7L5i4KJCzdXtZoPnhakvzpydiqAj1dTgmxl/NyO  
vsmCvLwp7b/Nk9bijCd0I1FOGR4FHiiIWf1L8P4xej0mLgH0Aq9mk/KsHrZkRu  
l1oa0BhF9wHb70BZGHYkiuRazEty2ytZPiTOeUkojNiy6lLyPQs2mAN/+QIDAQAB  
oCAwHgYJKoZIhvcaNQkOMREwDzANBgNVHREEBJAEggLRjzANBgkqhkiG9w0BAQsF  
AAOCQAQEAzi0Atco8C7yapn27JiMKsMGTYeotGNUC1TIIzpYN5BeeqDb+BbmsPeS+  
WK1Zj6W/789y3gqNfzAG8B+hz/EJj87Nop8GZ/CTL1D28ymHVIYuaEXbmcRhPEe+  
sa1xLSCBgZ+56tz+npkAzflsgDyyJn9mLYbIONYNT/u91loHj/kIBAAbfY08zk+I  
N6L2U9WX8mKfET72isiBKDY+T3BHP2KKRDGGr8+vjl6MFisa/nmFJNV4zjikxd1m  
WeD4W84zSPV5eqfQZfi1FOvST8zHKGallfJPaoLexXqVoNtSKjI25hD633n5xaVQ  
vK73IHyp4hEtYdE6sZH/7/UE7ZGCg==  
-----END CERTIFICATE REQUEST-----
```

Закрыть

Скопировать в буфер обмена

Нажмите **Скопировать в буфер обмена**, чтобы скопировать сертификат в буфер обмена.

Блок «Редактировать сертификаты RADIUS»

В данном блоке можно отредактировать SSL-сертификаты, используемые RADIUS-сервером, а также задать параметры их проверки и хранения.

В меню доступны следующие настройки:

SSL-сертификаты

HTTP RADIUS

Просмотреть сертификаты RADIUS Редактировать сертификаты RADIUS

1 Использовать Let's Encrypt Отключено

2 Сертификат сервера RADIUS Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=FR, ST=Radius, L=Somewhere, O=Example Inc./emailAddress=admin@example.org, CN=Example
Certificate Authority
Validity
Not Before: Jun 22 16:53:22 2025 GMT
Not After : Jun 22 16:53:22 2030 GMT
Subject: C=FR, ST=Radius, O=Example Inc., CN=Example Server
Certificate/emailAddress=admin@example.org
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:d9:eb:b9:ed:6c:55:e1:7b:d5:59:a7:19:d6:f9:
06:13:76:91:8a:68:ba:f0:ec:08:93:19:31:c6:a6:
85:1c:79:77:1c:97:15:91:a7:0f:ed:78:83:12:08:
ce:79:49:28:8c:d8:b2:ea:52:f2:3d:0b:36:98:03:
7f:f9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 CRL Distribution Points:
Full Name:
URI: http://www.example.com/example_ca.crl
Signature Algorithm: sha256WithRSAEncryption
0c:3a:1c:83:88:81:7f:84:33:d6:bc:20:45:8d:50:d3:b8:f3:
e2:03:c3:86:e6:2f:11:7e:18:a7:e5:f1:27:ff:d4:ed:4b:77:
86:24:de:43:04:5e:f3:3b:60:f0:15:a3:8b:08:17:2e:78:53:
c4:41:6c:11:1d:cf:53:82:c2:42:68:3d:9e:21:1c:78:c8:d0:
f5:ea:d7:a5:aa:7d:fe:ab:1b:48:a7:b9:b0:b0:c2:b5:ab:0f:
79:ad:7e:1c
-----BEGIN CERTIFICATE-----
MIID2ICAsKgAwIBAgIBATANBgkqhkiG9w0BAQsFADCkzELMAkGA1UEBRhMCRUx
DzANBgNVBAgMBUjhZG11czESMBAGA1UEBwwJU29tZXdoZXJIMRUwEwYDVQQKDAxF
eGftcGxjEfuYy4x1DAeBgkqhkiG9w0BCQEWFWFkbWluQGV4YW1wbGUub3JnMSYw
JAYDVQDDDB1FeGFtcGxjEN1c0Rp2mU1YXRIiEF1dgbvcml0eTAefw0vNTA2MjQx
NIUzMiJaFw0MDA2MjMxNIUzMiJaMHwxCzAJBgNVBAYTAKZSMQ8wDQYDVQQIDAZS
YWRpDXMxFTATBgnNVBAgMDExV4YW1wbGUuSw5lIeIMCEGA1UEAwwaRXhhbXBsZSBT
BW29l/pQuH16telqn3+qxtlp7mwsMK1qw95rX4c
-----END CERTIFICATE-----

- Использовать Let's Encrypt** — при активации данного параметра система использует доверенные удостоверяющие центры Let's Encrypt для автоматического выпуска и продления сертификатов. При активации данного параметра все последующие параметры заменяются на:
 - Common name** — указывает общее имя для сертификата;
 - Сертификат(ы) центра сертификации** — сертификаты доверенных центров, включая корневые и промежуточные сертификаты, используемые при аутентификации по EAP-TLS. Сертификат должен быть в формате PEM.
- Сертификат сервера RADIUS** — загружаемый SSL-сертификат, используемый RADIUS-сервером. Сертификат должен быть в формате PEM;

3 Автопоиск промежуточных CA сервера RADIUS Отключено

4 Сертификат(ы) промежуточного центра сертификации (CA)

5 Валидация цепочки сертификатов Включено

6 Закрытый ключ сервера RADIUS

7 Сертификат(ы) центра сертификации

В данное поле должны быть добавлены сертификаты доверенных клиентских центров, включая корневые или промежуточные сертификаты, используемые для EAP-TLS.

3. **Автопоиск промежуточных CA сервера HTTPS** — при активации данного параметра система автоматически определяет и загружает промежуточные сертификаты центра сертификации, скрывая параметр **Сертификат(ы) промежуточного центра сертификации (CA)**. Сертификат должен быть в формате PEM;
4. **Сертификат(ы) промежуточного центра сертификации (CA)** — список сертификатов промежуточных центров сертификации. Сертификат должен быть в формате PEM;
5. **Валидация цепочки сертификатов** — при активации данного параметра выполняется проверка корректности цепочки сертификатов до доверенного центра сертификации;
6. **Закрытый ключ сервера RADIUS** — закрытый ключ, используемый для сертификата сервера RADIUS. Ключ должен быть в формате PEM, а также иметь тип шифрования RSA или не иметь пароля;
7. **Сертификат(ы) центра сертификации** — сертификаты доверенных центров, включая корневые и промежуточные сертификаты, используемые при аутентификации по EAP-TLS. Сертификат должен быть в формате PEM.

Чтобы сохранить параметры, нажмите **Сохранить**. Чтобы сбросить введенные параметры на последние сохраненные, нажмите **Сбросить**.

ID статьи: 1305

Последнее обновление: 16 окт., 2025

Обновлено от: Ильина В.

Ревизия: 7

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Настройки системы» -> Страница «SSL-сертификаты» -> Вкладка «RADIUS»

<https://docs.axel.pro/entry/1305/>