

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](#)

Сертификат сервера RADIUS

[Сгенерировать запрос подписи \(CSR\)](#)

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.

[Заккрыть](#) [Сгенерировать](#)

В данном меню необходимо заполнить следующие параметры:

1. **Страна** — страна владельца сертификата;
2. **Состояние** — регион или область владельца сертификата;
3. **Город** — город владельца сертификата;
4. **Название организации** — официальное наименование организации, которой принадлежит сертификат;
5. **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-----
MIICsjCCAzoCAQAwTTElMAkGA1UEBhMCQVgxDALBgNVBAgMBM0QwrkxETAPBgNV
BAcMCMORwobDkMK5MQ0wCwYDVQQKDAtDkMKyMQ0wCwYDVQQDDAtDkcKPMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE2eu57WxV4XvVWacZ1vkGE3aRimi6
80wlkxkxxqaFHHI3HJcVkcP7XiDEghkaslCKrkjHL0aTKetrTPMI87yHScrhd6
6c/KgqF9xSO+fZfHPnaNsCaY36Zy4U402GQGbUkVyPg7eep5x6G90Kz6s5UG0I
GTd7y8DO++y12yRSYUykg4vu7L5i4KJCzdXtZoPhnakvzpydiqAj1dFtgmxl/NyO
vsmCvcLwps7b/Nk9bijCd0I1FOGR4FHIIWf1L8P4xejOmLgH0Aq9mk/KsHrZkRu
l1oa0BhF9wHb70BZGHYkiuRazEty2ytZPI0eUkojNiy6LLyPQs2mAN/+QIDAQAB
oCAWHgYJKoZIhvcNAQkOMREwDzANBgNVHREEBjAEggLRjzANBgkqhkiG9w0BAQsF
AAOCAQEazi0Atco8C7yapn27JiMKsMGTyeotGNUCT1IzpyN5BeeqDb+BbmsPeS+
WK1Zj6W/789y3gqNfzAG8B+hz/EJj87Nop8GZ/CTl1D28ymHVIYuaEXbmcRhPEe+
sa1xLSCBgZ+56tz+nqkAzflsgDyyJn9mLYbIONYNT/u91loHj/klBAAbfY08zk+I
N6L2U9WX8mKFET72isiBKDY+T3BHP2KKRDGGr8+vjl6MFisa/nmFJNV4zjikxd1m
WeD4W84zSPV5eqfQZfi1FOvST8zHKGallfJPaoLexXqVoNtSKjI25hD633n5xaVQ
vK73lHyNp4hEtYdE6sZH/7/UE7ZGCg==
-----END CERTIFICATE REQUEST-----
```

[Заккрыть](#) [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)

X.509v3 extensions:

X.509v3 Extended Key Usage:
TLS Web Server Authentication

X.509v3 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-----

MIIID2CCAsKqAwIBAgIBATANBakqhkiG9w0BAQsFADCkzEIMakGA1UEBhMCRUlx
DzANBgNVBAsMBIjZG11czESMBAGA1UEBjwJU291ZXd0ZXJlMRUwFwYyDQYKDAxY
eGFtcGxlIFluYy4xIDAeBakqhkiG9w0RCQEWFEWfkbWluQGV4YW1wbGUub3InMSYw
JAYDVQQDDDB1FeGFtcGxlENlcnRpZmlYXRUEF1dGhyeml0eTAeFw0vNTA2MjI0x
NIUzMiJaFw0zMDA2MjI0xNIUzMiJaMHwxZzAJBgNVBAYTAkZSMQ8wDQYDVOQIDAZS
YWRpdXMxFTATBgNVBAoMDEV4YW1wbGUgSW51LjEiMCEGA1UEAwwaRXhhbXBsZSBT
BW29I/pQquH16telqn3+qxtlp7mwsMK1qw95rX4c

-----END CERTIFICATE-----

1. **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:
 1. **Common name** — указывает общее имя для сертификата;
 2. **Сертификат(ы) центра сертификации** — сертификаты доверенных центров, включая корневые и промежуточные сертификаты, используемые при аутентификации по EAP-TLS. Сертификат должен быть в формате PEM.
2. **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

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBkwwggSlAgEAAoIBAQDZ67ntbFXhe9VZ
pxnW+QYTdpGKaLrw7AiTGTGpUceXcclxWRpw/teIMSCGRqyUIquSMcvRpMp62t
M8yXzVldJyF1vrpz8qCoX3FI759kR8c+do2wJpjfnLhTg7YZAZtSRXI+Dt556n
nHob04rPqzIQbQgZn3vLwM777LXbJfJhTKSDi+7svmlgokLN1e1mg+eFqS/OnJ2K
oCPV0W2CbGX83I6+yYJVwvCmztv82T1uKMJ04jUU4ZHGueIghZ/Uvw/jF6PSYuAf
-----END PRIVATE KEY-----
```

7 Сертификат(ы) центра сертификации

```
-----BEGIN CERTIFICATE-----
4jizQjMOfHL9eJmM7pUbuUwDwYDVR0TAQH/BAUwAwEB/za2BgNVHR8ELzAtMCug
KaAnhiVodHRwOi8vd3d3LmV4YW1wbGUub3JnL2V4YW1wbGVfY2EuY3JsMA0GCsqG
S1b3DQEBcUAA4IBAQCcaAOHfgSOsgpi603DLG95+stg2oarIKhwwwwJavJC9kji1
IF97IkOpdydlPteqf7aubhA4HH/Huia/la0jnJujlfjV1zm0j6/TlxN5Qc7S2g/L
Q540ofF3CoOuc5qhXp4giue1tu4fcEnVhmqr/re1EERYqlr9VnkqiBmhp3367HkQ
RCCjYBUqjCA8EeBNeR5bB1TcksK6Zxdb3FIU2h14hR91DpE2ByQA0VqOoXZWvYCd
-----END CERTIFICATE-----
```

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

- 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;
- Сертификат(ы) промежуточного центра сертификации (CA)** — список сертификатов промежуточных центров сертификации. Сертификат должен быть в формате PEM;
- Валидация цепочки сертификатов** — при активации данного параметра выполняется проверка корректности цепочки сертификатов до доверенного центра сертификации;
- 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;
- 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: 1508

Последнее обновление: 19 янв., 2026

Обновлено от: Ильина В.

Ревизия: 1

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.1.0 -> AxelINAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Настройки системы» -> Страница «SSL-сертификаты» -> Вкладка «RADIUS»

<https://docs.axel.pro/entry/1508/>