Пульт зв'язку ССАР

Налаштування SIP/TLS та SRTP

Керівництво адміністратора • редакція 2

Призначення	Налаштування захищеної SIP-сигналізації TLS та шифрованого голосового медіапотоку SRTP.
Керування	Webmin → Служби → Налаштування VoIP.
Режими акаунта	Off / Preferred / Required.
Приклад сервера	Asterisk / PJSIP, TLS + SDES-SRTP.

Документ описує лише налаштування TLS/SRTP та пов'язані з ними особливості SIP-акаунтів ССАР. Інші функції пристрою тут не розглядаються.

1. Як обрати спосіб роботи TLS

Перед налаштуванням SIP-акаунта адміністратор має визначити, чи буде CCAP перевіряти сертифікат SIP-сервера. Сам TLS може працювати у двох практичних варіантах:

- TLS без перевірки сертифіката сервера. Канал SIP шифрується TLS, але CCAP не перевіряє довіру до сертифіката сервера. У цьому випадку заходити до розділу TLS / Сертифікати для звичайного налаштування акаунта не потрібно; прапорець Verify SIP server certificate не повинен бути увімкнений.
- TLS з перевіркою сертифіката сервера. Окрім шифрування каналу, CCAP перевіряє сертифікат SIP-сервера. Тоді необхідно відкрити TLS / Сертифікати, увімкнути перевірку та завантажити CA-сертифікат, якому довіряє CCAP.

Після вибору одного з цих двох варіантів налаштовується режим шифрування конкретного SIP-акаунта - Off, Preferred або Required.

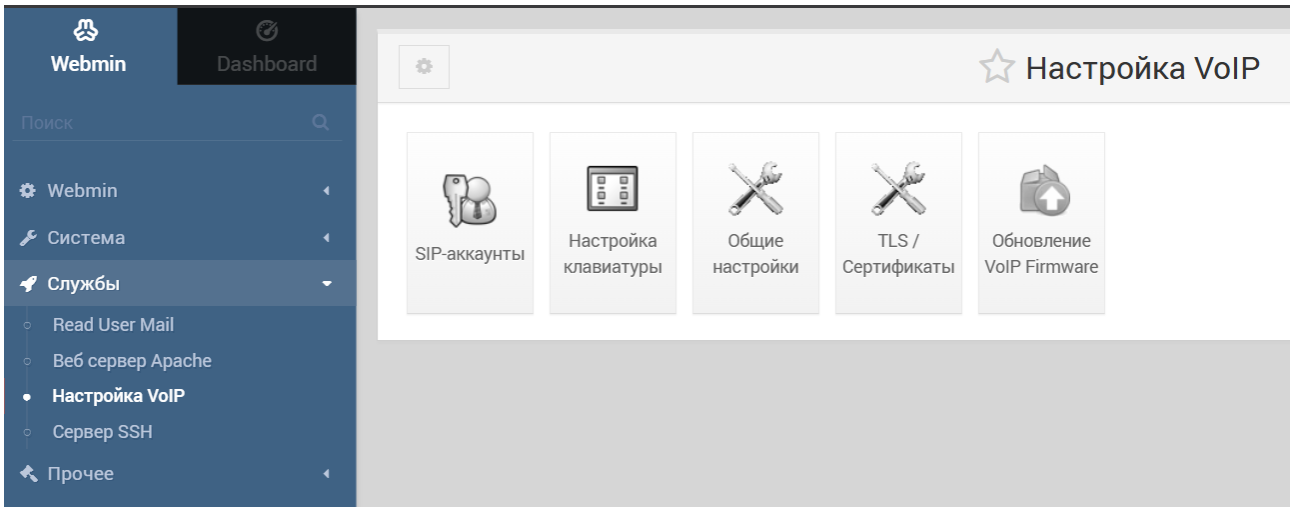


Рисунок 1 - Головне меню «Налаштування VoIP». Для TLS з перевіркою сертифіката використовується пункт «TLS / Сертифікати».

Коротко: якщо перевірка сертифіката не потрібна - налаштовується лише SIP-акаунт. Якщо перевірка потрібна - спочатку налаштовується розділ TLS / Сертифікати, після чого SIP-акаунт.

2. Налаштування SIP-акаунта



Рисунок 3 - Редагування SIP-акаунта. Пароль на ілюстрації приховано.

Поля Encryption та TLS port визначають режим роботи конкретного SIP-акаунта. TLS port використовується для TLS-з'єднання; у прикладі - 5061.

Режим	Сигналізація / медіа	Поведінка
Off	SIP/UDP + RTP	Шифрування вимкнено.
Preferred	TLS + SRTP; за потреби fallback → UDP + RTP	Спочатку захищене з'єднання. Fallback дозволено лише при реальній помилці або тайм-ауті TLS-транспорту.
Required	TLS + SRTP	TLS/SRTP обов'язкові; downgrade до UDP/RTP відсутній.

Для функціональної перевірки Preferred можна тимчасово вказати недоступний TLS-порт. Після невдалої спроби встановити TLS CCAP повинен перейти на звичайний SIP/UDP + RTP.

3. TLS з перевіркою сертифіката

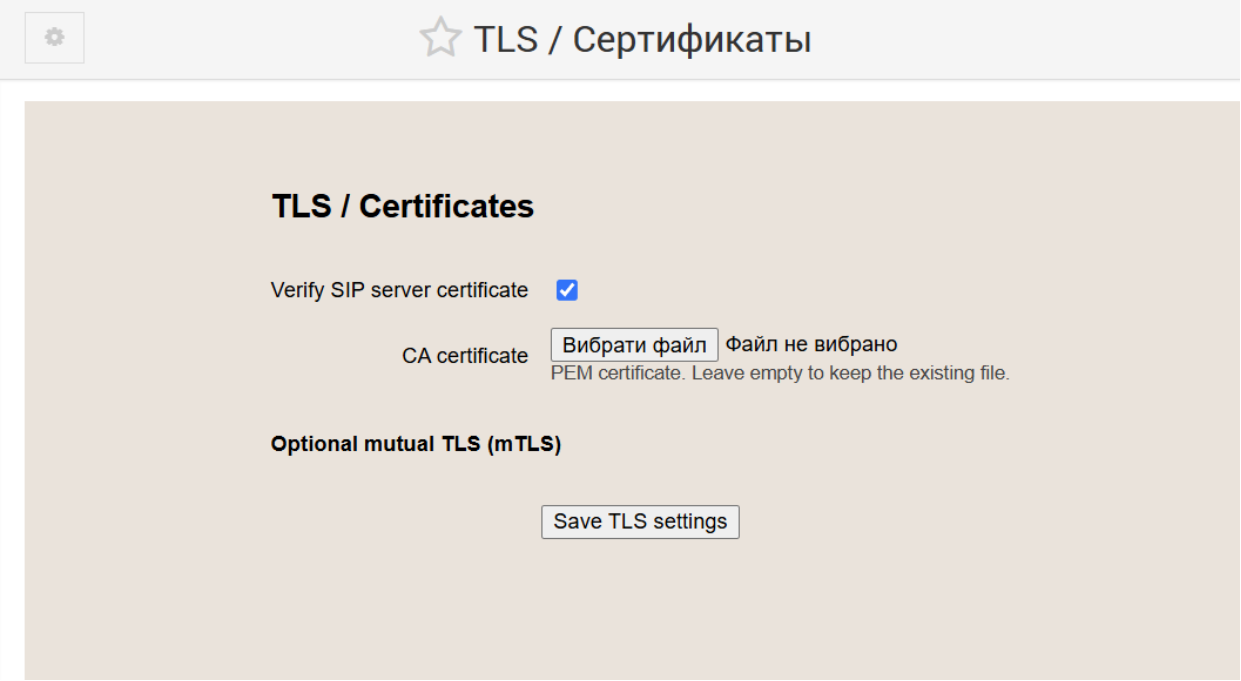


Рисунок 2 - Налаштування перевірки сертифіката SIP-сервера.

Verify SIP server certificate. Увімкнути лише тоді, коли CCAP повинен перевіряти сертифікат SIP-сервера. Сертифікат сервера має бути чинним і мати ланцюжок довіри до CA, відомого CCAP.

CA certificate. Завантажується сертифікат центру сертифікації у форматі PEM. Якщо під час подальшого збереження файл не вибирати, наявний CA-файл залишається без заміни.

Для закритої мережі може використовуватися власний локальний CA: серверний сертифікат підписується цим CA, а CA-сертифікат завантажується на CCAP.

4. Індикація реєстрації та обов'язкова перевірка дзвінка

На CCAP використовується багатокольоровий світлодіод стану SIP-реєстрації:

- жовтий - SIP-акаунт не зареєстрований;
- зелений - SIP-реєстрація успішна.

У Webmin стан реєстрації також відображається кольоровою точкою біля SIP-сервера.

Зелений індикатор підтверджує реєстрацію, але не гарантує можливість дзвінка. REGISTER може завершитися успішно, тоді як INVITE буде відхилений через несумісні параметри медіа. Під час тестування спостерігався випадок, коли реєстрація була успішною, але виклик завершувався 488 Not Acceptable Here через невідповідність параметрів SRTP/RTP.

Після кожної зміни Encryption необхідно:

- дочекатися зеленої індикації реєстрації;
- перевірити вихідний дзвінок з CCAP;
- перевірити вхідний дзвінок на CCAP;
- переконатися у наявності двостороннього звуку;
- для Preferred окремо перевірити захищений режим та fallback.

Тільки після успішного реального виклику конфігурацію можна вважати перевіреною.

5. Приклад Asterisk / PJSIP

Нижче наведено орієнтовний серверний приклад. Шляхи до сертифікатів, адреси, паролі та контексти потрібно адаптувати до конкретної інсталяції.

5.1. TLS transport

```
[transport-tls]
type=transport
protocol=tls
bind=0.0.0.0:5061
cert_file=/etc/asterisk/tls/server.crt
priv_key_file=/etc/asterisk/tls/server.key
ca_list_file=/etc/asterisk/tls/ca.crt
method=tlsv1_2
```

Якщо на CCAP увімкнено Verify SIP server certificate, завантажений на CCAP CA повинен дозволяти перевірити сертифікат server.crt.

5.2. Endpoint для SRTP та сумісності з RTP

```
[1001](lab-endpoint)
auth=auth1001
aors=1001
callerid=CCAP 1001 <1001>
media_encryption=sdes
media_encryption_optimistic=yes

[auth1001]
type=auth
auth_type=digest
username=1001
password=CHANGE_ME

[1001]
type=aor
max_contacts=1
remove_existing=yes
qualify_frequency=30
```

media_encryption=sdes вмикає SDES-SRTP. Якщо той самий endpoint повинен приймати як SRTP, так і звичайний RTP, важливим є media_encryption_optimistic=yes.

У тестовій конфігурації media_encryption_optimistic=no призводило до надсилання Asterisk захищеного медіапрофілю RTP/SAVP навіть у сценарії, де CCAP працював без SRTP. CCAP відхиляв такий INVITE відповіддю 488. Це особливість узгодження медіа на серверній стороні, а не помилка SIP-реєстрації.

6. Очікувана поведінка

Умова	Off	Preferred	Required
TLS доступний	UDP/RTP	TLS/SRTP	TLS/SRTP
TLS недоступний	UDP/RTP	Fallback → UDP/RTP	TLS-реєстрація не відбудеться
Через TLS отримано SIP-помилку	-	SIP-код сам по собі не є причиною downgrade	Без downgrade

7. Типові проблеми

Реєстрація зелена, але виклик не проходить. Перевірити SDP у INVITE та SIP-відповідь. Код 488 часто означає, що медіапараметри не вдалося погодити. На Asterisk перевірити media_encryption та media_encryption_optimistic.

Required не реєструється. Перевірити TLS port, доступність TCP-порту, TLS transport Asterisk, сертифікат сервера, CA та Verify SIP server certificate.

Preferred переходить на UDP. Це штатно лише при реальній недоступності/помилці TLS-транспорту або тайм-ауті. SIP-відповіді 401/403/407/503 самі по собі не повинні викликати downgrade.

Off реєструється, але INVITE містить SRTP. Серверна сторона нав'язує захищений медіапрофіль. Для Asterisk перевірити optimistic media encryption або політику endpoint-а.

8. Контрольний перелік

- Визначити: TLS без перевірки сертифіката чи TLS з перевіркою сертифіката.
- Якщо перевірка потрібна - налаштувати TLS / Сертифікати та завантажити CA у PEM.
- Якщо перевірка не потрібна - Verify SIP server certificate залишити вимкненим.
- Для SIP-акаунта вибрати Off, Preferred або Required і перевірити TLS port.
- На Asterisk налаштувати TLS transport та, для SRTP, media_encryption=sdes.
- За потреби одночасної сумісності з SRTP і RTP перевірити media_encryption_optimistic=yes.
- Переконатися у зеленій SIP-реєстрації.
- Обов'язково перевірити реальний вхідний і вихідний виклик та двосторонній звук.
- Для Preferred окремо перевірити fallback при недоступному TLS.

Кінець документа