

Сертификаты

Модуль «Сертификаты» расположен в Меню «Защита». Данный модуль предназначен для управления сертификатами, которые используются для установления защищённых SSL/TLS соединений типа клиент-сервер. Более подробно о SSL/TLS можно почитать здесь <https://ru.wikipedia.org/wiki/SSL> и <https://ru.wikipedia.org/wiki/TLS>.

Созданные сертификаты могут применяться как в «ИКС», так и в сторонних программах.

Внимание с версии 7.1.0 прекращена поддержка сертификатов с шифрованием md5.

При первой установке «ИКС» автоматически создаются конечные сертификаты для WEB-интерфейса, телефонии и почты.

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Сертификаты					
Autogenerated Asterisk_5db98833462f26.53185831	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-asterisk
Autogenerated GUI_5db988310e40a5.57388659	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-gui
Autogenerated MailServer_5db988315ad5a2.16533086	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-mail-server

Список сертификатов представлен в виде дерева, а поле модуля поделено на столбцы, в которых показана основная информация о сертификатах: тип ключа родительского сертификата, дата начала действия и окончания, а также имя хоста (или ip-адрес), который представляет данный сертификат.

Модуль позволяет создать новый сертификат или удалить существующий при помощи кнопок «Создать» и «Удалить»; экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт»; просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата».

Создание сертификатов

Чтобы создать новый сертификат, нажмите «Добавить».

Добавление сертификата

Общее

Настройки

Использование ключа

Netscape расширение

Название *

Новый сертификат

Код страны

RU - Russian Federation

Город

Город

Область

Область

Организация

Организация

E-mail

E-mail

Имя или адрес хоста *

test.ru

Добавить

Отмена

Во вкладке «Общее» заполняются данные сертификата: наименование, код страны, местоположение, сведения об организации, имя хоста или ip-адрес.

Добавление сертификата

Общее

Настройки

Использование ключа

Netscape расширение

Тип сертификата

Алгоритм

Тип шифрования

Срок действия сертификата

Длина ключа *

 ↑ ↓ бит

Добавить

Отмена

Во вкладке «Настройки» определяется роль сертификата - CA (корневой) или конечный, устанавливается метод шифрования, время действия и длина ключа в битах.

Добавление сертификата

Общее Настройки **Использование ключа** Netscape расширение

Шаблон

CA

Использование ключа

- CRL sign
- Certificate Sign
- Non Repudiation
- Digital Signature
- Key Encipherment

Расширенное использование ключа

- E-mail Protection
- TLS Web Client Authentication
- Code Signing
- TLS Web Server Authentication
- Time Stamping

Добавить

Отмена

Во вкладке «Использование ключа» можно выбрать шаблон использования открытого ключа сертификата в поле «Шаблон» или указать вручную в разделах «Использование ключа» («Key usage extensions») и «Расширенное использование ключа» («Extended key usage»). Более подробно можно почитать здесь https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/conf_keyusageextensionsandextendedkeyusage_r.html

Добавление сертификата

Общее Настройки Использование ключа **Netscape расширение**

SSL Client

SSL Server

S/MIME

Object Signing

SSL CA

S/MIME CA

Object Signing CA

Добавить Отмена

Во вкладке «Netscape расширение» можно указать использование ключа для совместимости со старыми Netscape приложениями (выпущенными до принятия стандарта X.509 v3).

После нажатия кнопки «Добавить» будет предложено зашифровать ключ паролем. Введите пароль или откажитесь от его использования.

Общее Настройки Использование ключа **Netscape расширение**

Шифровать закрытый ключ паролем

Не шифровать закрытый ключ

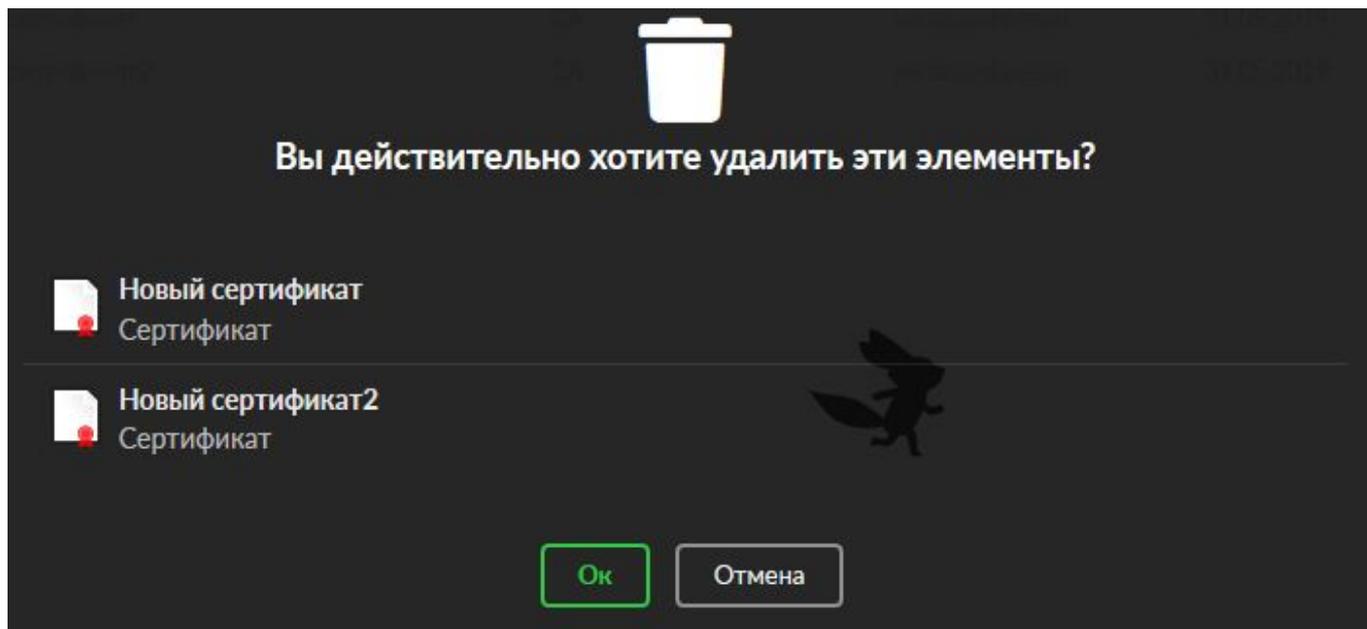
Ок Отмена

Важно: для служб ИКС всегда применяются только нешифрованные сертификаты.

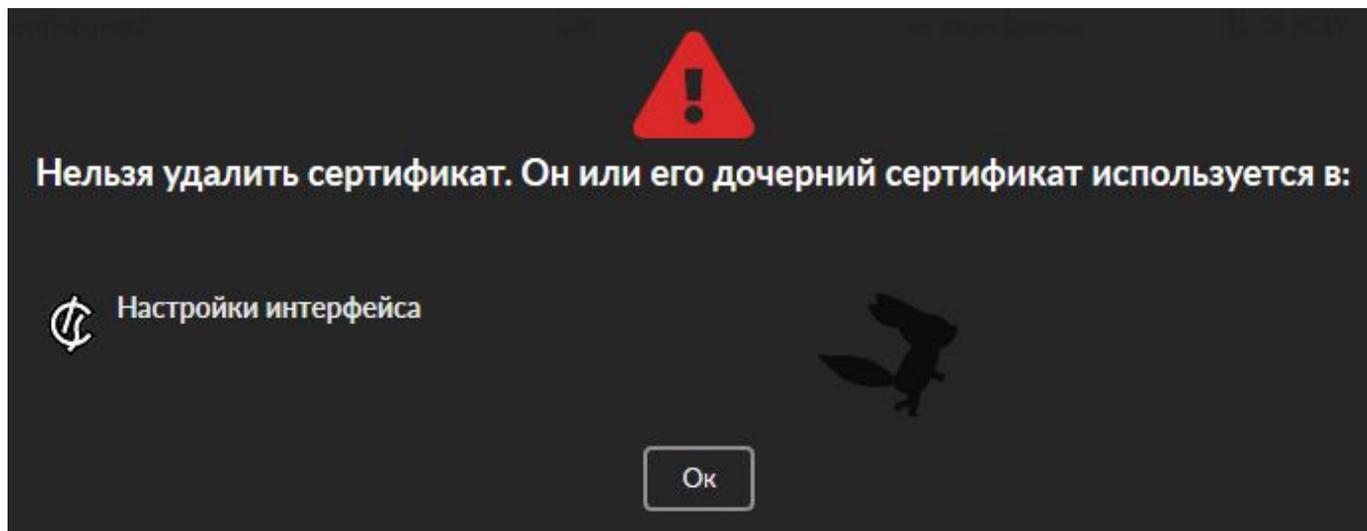
Важно: первоначально всегда должен создаваться корневой сертификат, затем - дочерние конечные сертификаты! К службам ИКС(кроме **SSL-фильтрации**), применяются только конечные сертификаты. Будьте внимательны: неверное применение сертификата к службам может сделать их недоступными для пользователя!

Удаление сертификатов

Для удаления сертификата выделите нужный сертификат в списке (или несколько сертификатов зажав клавишу Ctrl) и нажмите кнопку «Удалить»:



Если сертификат используется какой-либо службой «ИКС», то будет выдано уведомление об ошибке:



Импорт/экспорт сертификатов

Для импорта сертификата нажмите кнопку «Импорт»:

Импорт

Сертификат *

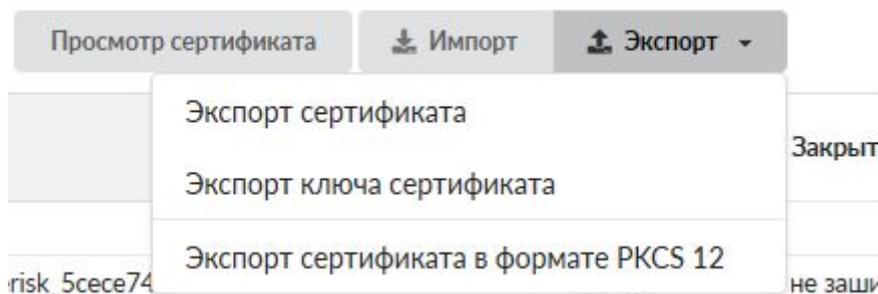
Ключ сертификата

Пароль сертификата в формате PKCS 12

Ок **Отмена**

В полях «Сертификат» и «Ключ сертификата» выбираются файл сертификата и файл ключа соответственно. Для импорта сертификата в формате PKCS12 необходимо в поле «Сертификат» выбрать соответствующий файл и в поле «Пароль сертификата в формате PKCS 12» указать пароль.

Для экспорта сертификата нажмите кнопку «Экспорт» и выберите необходимый вариант:



Просмотр сертификата

Для просмотра сертификата, выделите нужный сертификат в списке и нажмите кнопку «Просмотр сертификата».

Данные сертификата Openvpn-CA

Общее

Название: Openvpn-CA
Код страны: RU - Russian Federation
Город: Yaroslavl
Область: The same
Организация: A-Real
E-mail: gu@me.ton
Имя или адрес хоста: openvpn

Настройки

Тип сертификата: CA
Алгоритм: MD 5
Тип шифрования: RSA
Создан: 08.02.2017
Действует до: 08.02.2018
Длина ключа: 2048 бит

Использование ключа

Использование ключа: Certificate Sign
CRL Sign

Добавить в доверенные сертификаты

Ок

ВНИМАНИЕ Если провайдер расшифровывает трафик и выдал CA сертификат, то после импорта сертификата на ИКС, необходимо нажать «Просмотр сертификата». В открывшейся форме необходимо нажать «Добавить в доверенные сертификаты», иначе ИКС не будет доверять данным сертификатам и не откроет запрашиваемые страницы.

From:
<https://doc-old.a-real.ru/> - **Документация**

Permanent link:
<https://doc-old.a-real.ru/doku.php?id=ics70:serts>

Last update: **2020/06/12 10:51**

