2025/11/03 23:17 1/8 Сертификаты

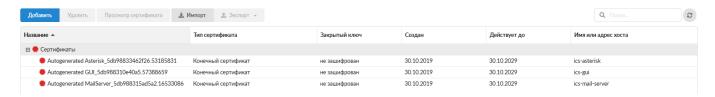
Сертификаты

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.



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 ір-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».

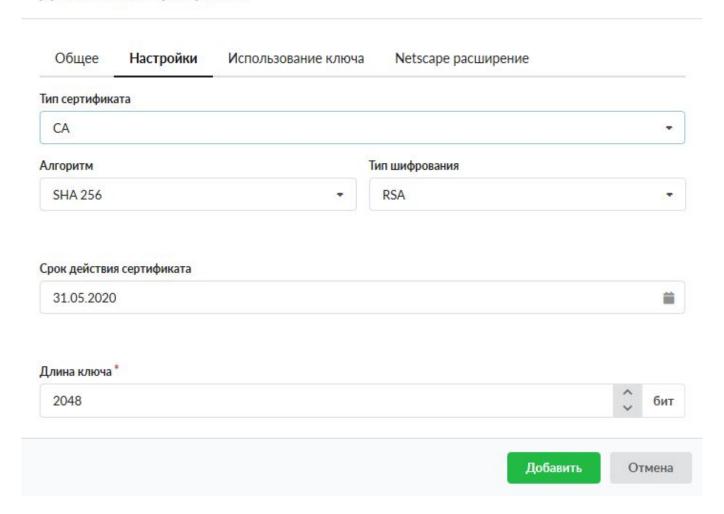
Добавление сертификата

Общее	Настройки	Использование ключа	Netscape расширение			
Название *						
Новый сер	тификат					
Код страны						
RU - Russia	n Federation			•		
Город		C	Область			
Организация		E	E-mail			
Имя или адре	ес хоста *					
test.ru						
			Добавить От	мена		

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

2025/11/03 23:17 3/8 Сертификаты

Добавление сертификата



Во вкладке «Настройки» определяется роль сертификата - СА (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

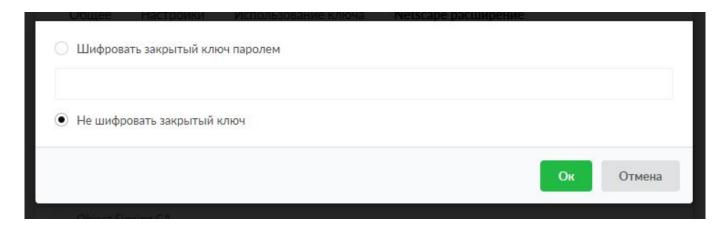
https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/conf_keyusageextensionsand extendedkeyusage r.html

Добавление сертификата

SSL Client SSL Server S/MIME Object Signing SSL CA S/MIME CA	SSL Server S/MIME Object Signing	Общее	Настройки	Использование ключа	Netscape расширение	
S/MIME Object Signing SSL CA	S/MIME Object Signing SSL CA S/MIME CA	SSL Clien	t			
Object Signing SSL CA	Object Signing SSL CA S/MIME CA	SSL Serve	er			
SSL CA	SSL CA S/MIME CA	S/MIME				
	S/MIME CA	Object Sig	gning			
S/MIME CA		SSL CA				
	Object Signing CA	S/MIME (CA			
Object Signing CA		Object Sig	gning CA			

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.

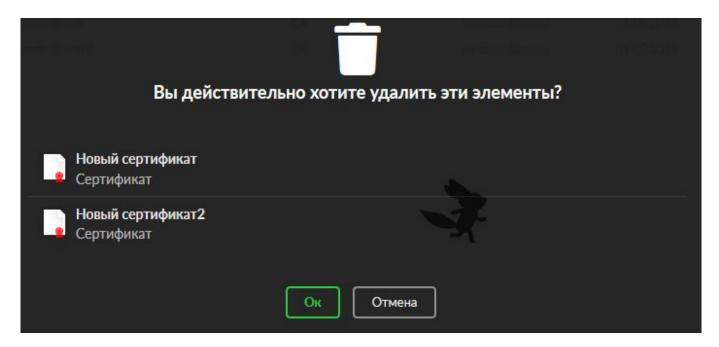


Важно: для служб ИКС всегда применяются только нешифрованные сертификаты.

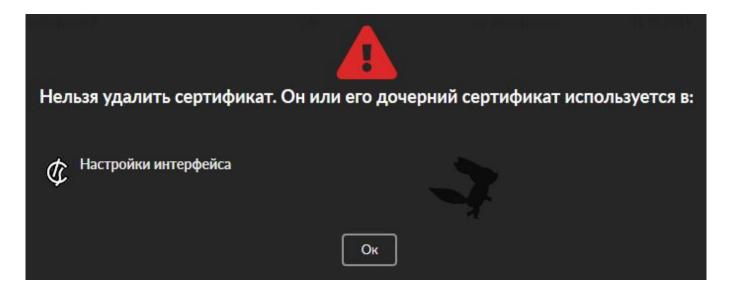
Важно: первоначально всегда должен создаваться корневой сертификат, затем - дочерние конечные сертификаты! К службам ИКС(кроме SSL-фильтрации), применяются только конечные сертификаты. Будьте внимательны: неверное применение сертификата к службам может сделать их недоступными для пользователя!

Удаление сертификатов

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

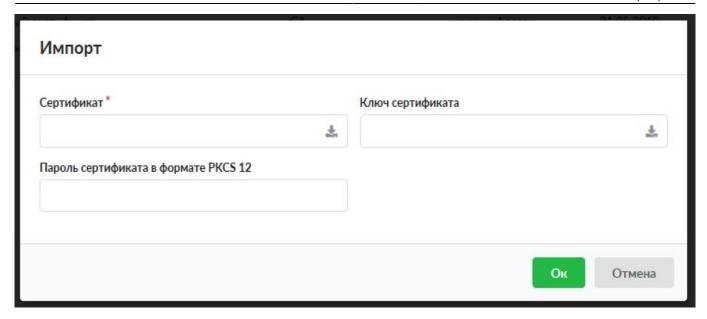


Если сертификат используется какой-либо службой «ИКС», то будет выдано уведомление об ошибке:



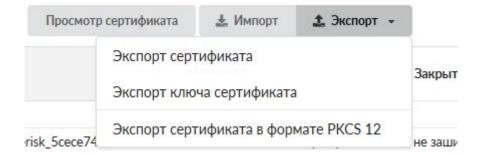
Импорт/экспорт сертификатов

Для импорта сертификата нажмите кнопку «Импорт»:



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: Орепурп-СА

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: СА

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 СА 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

