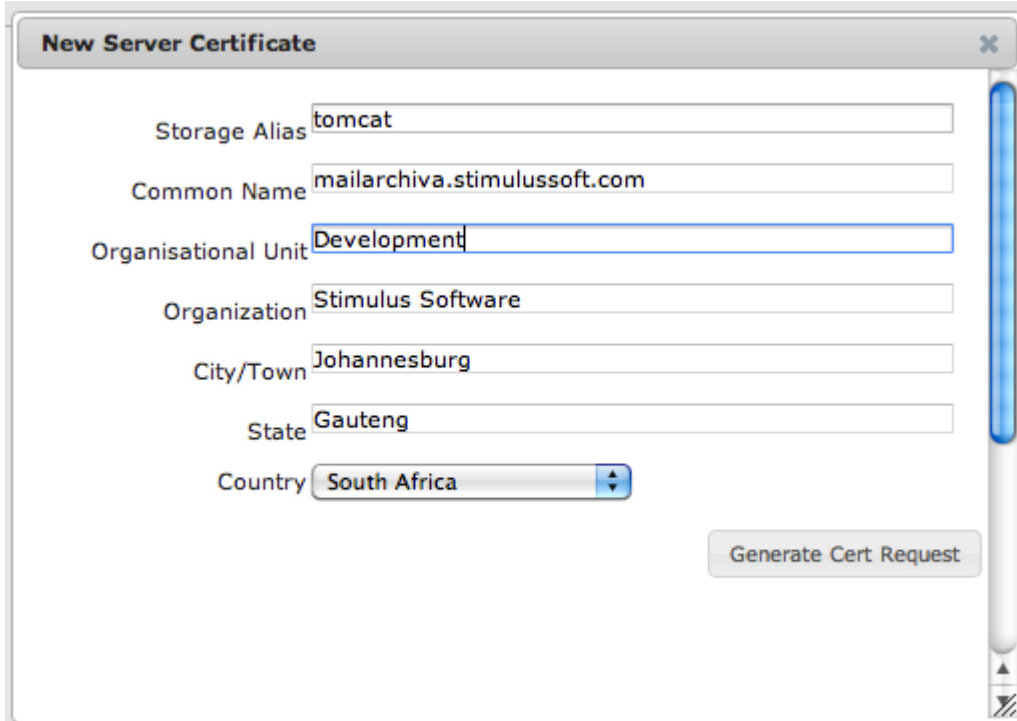


Сертификаты

В этом разделе описывается, как создать и установить серверный и доверенный сертификат. Сертификаты используются для безопасного доступа к Архива по [HTTPS](https://).

Создать подпись сертификата, сгенерировать тестовый сертификат (CSR)


1. Нажмите "Новый сертификат сервера" в "Сертификаты"




- 2.
3. Введите storage alias. Этот псевдоним это произвольное имя (выбранное Вами) потом его вы будете использовать для ссылки на сертификат.

 если устанавливаете HTTPS, используйте "tomcat" как alias

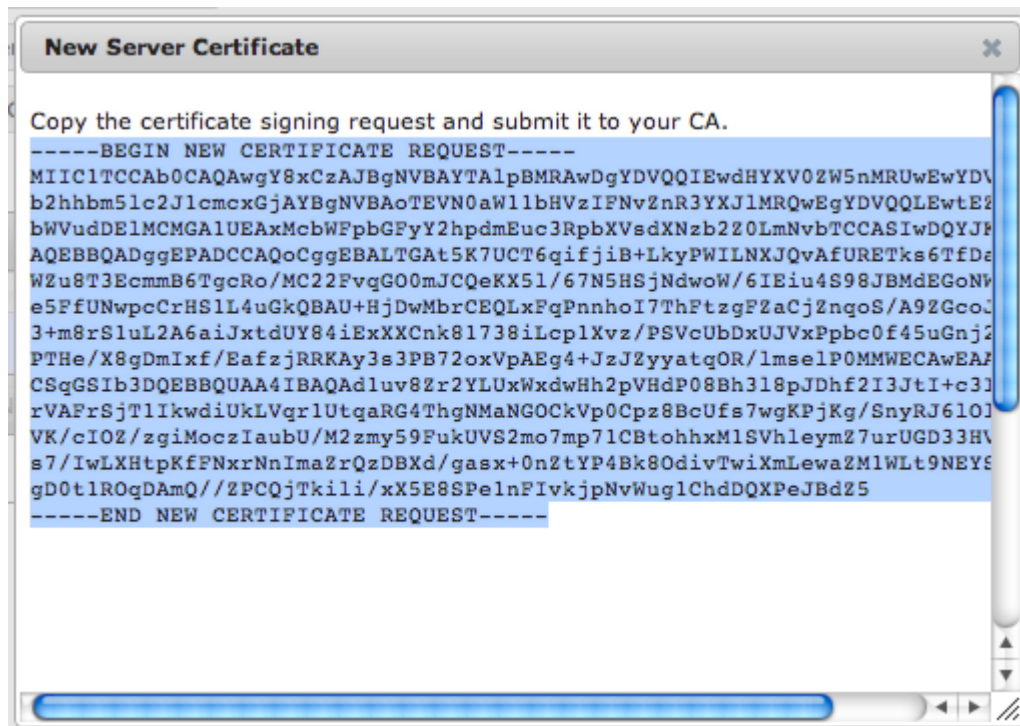
4. Введите common name сертификата

 если устанавливаете HTTPS, common name должен быть FQDN сервера (т.к. archiva.data-ocean.ru)

5. Заполните оставшиеся поля

 Избегайте ввода сокращенных наименований для города и государства, так как многие компании CA не будет принимать запрос на подпись.

6. Нажмите кнопку «Сгенерировать запрос сертификата»
7. Выделите и скопируйте запрос на подпись сертификата в буфер обмена. Закройте диалоговое окно.



- 8.
9. Вы должны увидеть псевдоним для подписания сертификата в списке сертификатов сервера на вкладке Сертификаты.

Получение сертификатов от центра сертификации (CA)

1. Получите бесплатную 15 дневную пробную версию SSL сертификат / приобретите сертификат от центра сертификации, таких как VeriSign.
2. Вставьте в запрос на подпись сертификата (CSR), созданный ранее.

Enter Certificate Signing Request (CSR)

Server platform:

Server not listed

Server not listed

mailarchiva

Sample CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2jCCAUCAQAwZ2R0LmNvbTCCASlwdQYJ
bGluYTEEQMA4GA1UEBxMHU1bHVzIFNvZnR3YXJlMRQwEgYDVQQLEwtE2bWVudDElMCMGA1UEAxBmcbWFpbGZyY2hpdmcuc3RpbXVsdXNzb2Z0LmNvbTCCASlwdQYJ
KQZlHvcN
AQEBBQADggEPADCCAQoCggEBALTGAt5K7UCT6qifjiB+LkyPWILNXJQvAfURETks6TfDz
WZu8T3Ecmmb6TgcRo/MC22FvqGO0mJCQeKX5l/67N5HSjNdwoW/6IEiu4S98JBMdEGoNv
e5PfUNwpcCrHS1L4uGkQBAU+HjDwMbrCEQLxPqPnnhoI7ThFtzgFZaCjZnqoS/A9ZGco3
3+m8rS1uL2A6aiJxtduY84iExXXCnk81738iLcp1Xvz/PSVcUbDxUJVxPpb0f45uGnj2
PThE/X8gDmIxf/EafzjRRKAy3s3PB72oxVpAEg4+JzJZyyatqOR/lmselP0MMWECAwEA
AAAMA0G
CSqGSIB3DQEBBQUAA4IBAQAduv8Zr2YLUXWxdwHh2pVHdP08Bh3l8pJDhf2I3JtI+c3l
rVAFrSjt1IkwdiUkLVqr1UtqARG4ThgNMaNGOCKVp0Cpz8BcUfs7wgKPjKg/SnyRJ6lOI
MupHkqt
VK/cIOZ/zgiMoczIaubU/M2zmy59FukUVS2mo7mp71CBtohhtM1SVhleyM27urUGD33HV
UmaPgZj
s7/IwLXHtpKfFNxrNnImaZrQzDBXd/gasx+0nZtYP4Bk8OdivTwIXmLewaZM1WLt9NEYS
D9n91Vj
gD0t1ROqDAmQ//ZPCQjTkili/xX5E8SPe1nFlvkjpnVwuglChdDQXPeJBdZ5
-----END CERTIFICATE REQUEST-----
```

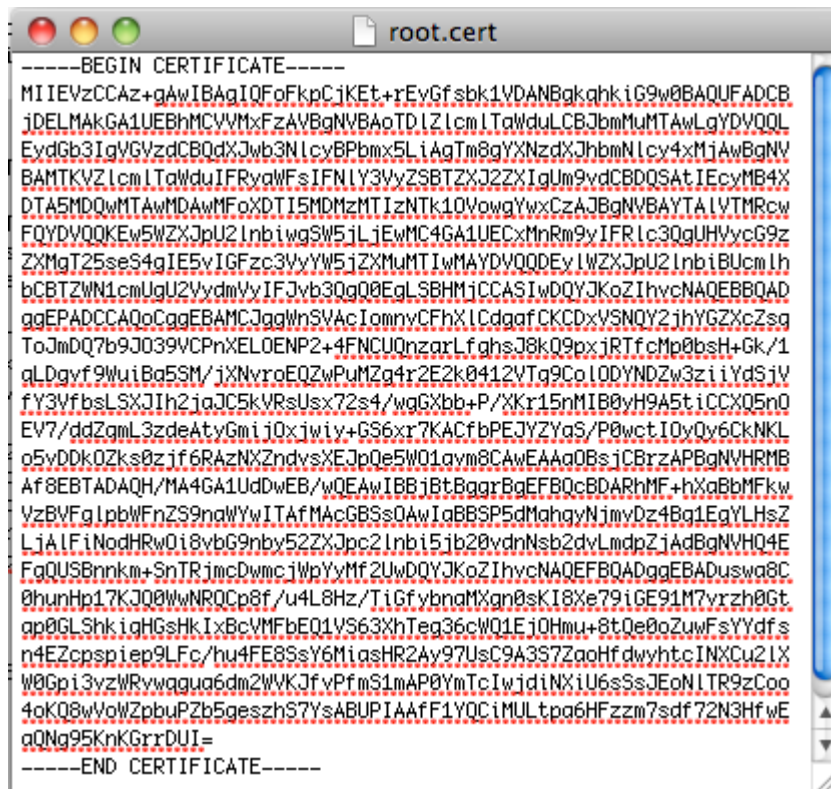
Paste Certificate Signing Request (CSR):

MIIC1TCCAb0CAQAwY8xCzAJBgNVBAYTA1pBMRAwDgYDVQQIEwdHYXV0ZW5nMRUwEwYDVQQHEwXK
b2hhbm5lc2J1cmcxGjAYBgNVBAoTEVN0aW11bHVzIFNvZnR3YXJlMRQwEgYDVQQLEwtE2bWVudDElMCMGA1UEAxBmcbWFpbGZyY2hpdmcuc3RpbXVsdXNzb2Z0LmNvbTCCASlwdQYJ
KQZlHvcN
AQEBBQADggEPADCCAQoCggEBALTGAt5K7UCT6qifjiB+LkyPWILNXJQvAfURETks6TfDz
WZu8T3Ecmmb6TgcRo/MC22FvqGO0mJCQeKX5l/67N5HSjNdwoW/6IEiu4S98JBMdEGoNv
e5PfUNwpcCrHS1L4uGkQBAU+HjDwMbrCEQLxPqPnnhoI7ThFtzgFZaCjZnqoS/A9ZGco3
3+m8rS1uL2A6aiJxtduY84iExXXCnk81738iLcp1Xvz/PSVcUbDxUJVxPpb0f45uGnj2
PThE/X8gDmIxf/EafzjRRKAy3s3PB72oxVpAEg4+JzJZyyatqOR/lmselP0MMWECAwEA
AAAMA0G
CSqGSIB3DQEBBQUAA4IBAQAduv8Zr2YLUXWxdwHh2pVHdP08Bh3l8pJDhf2I3JtI+c3l
rVAFrSjt1IkwdiUkLVqr1UtqARG4ThgNMaNGOCKVp0Cpz8BcUfs7wgKPjKg/SnyRJ6lOI
MupHkqt
VK/cIOZ/zgiMoczIaubU/M2zmy59FukUVS2mo7mp71CBtohhtM1SVhleyM27urUGD33HV
UmaPgZj
s7/IwLXHtpKfFNxrNnImaZrQzDBXd/gasx+0nZtYP4Bk8OdivTwIXmLewaZM1WLt9NEYS
D9n91Vj
gD0t1ROqDAmQ//ZPCQjTkili/xX5E8SPe1nFlvkjpnVwuglChdDQXPeJBdZ5
-----END NEW CERTIFICATE REQUEST-----

Total: US \$0 (Free Trial)

< Back
Cancel
Continue

- 3.
4. В большинстве случаев, сертификат сервера и сертификат CA будет отправлен вам по почте.
5. Создайте папку на рабочем столе с именем Сертификаты
6. Откройте текстовый редактор и вставьте содержимое сертификата сервера. Назовите файл как "server.cert" и сохраните в папку Сертификаты.
7. Аналогично, скопируйте промежуточный сертификат в текстовый файл с именем intermediate.cert.
8. Наконец, скопируйте сертификат корневого центра сертификации в текстовый файл с именем root.cert.



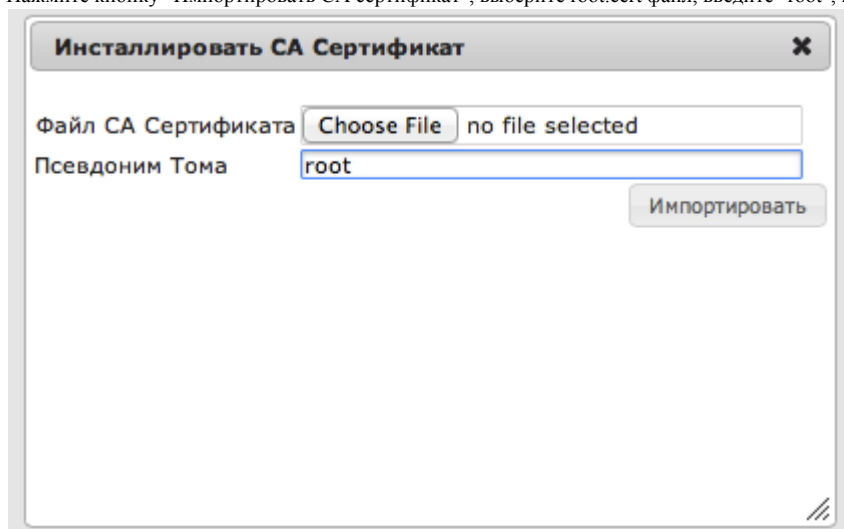
9.

Импорт сертификатов



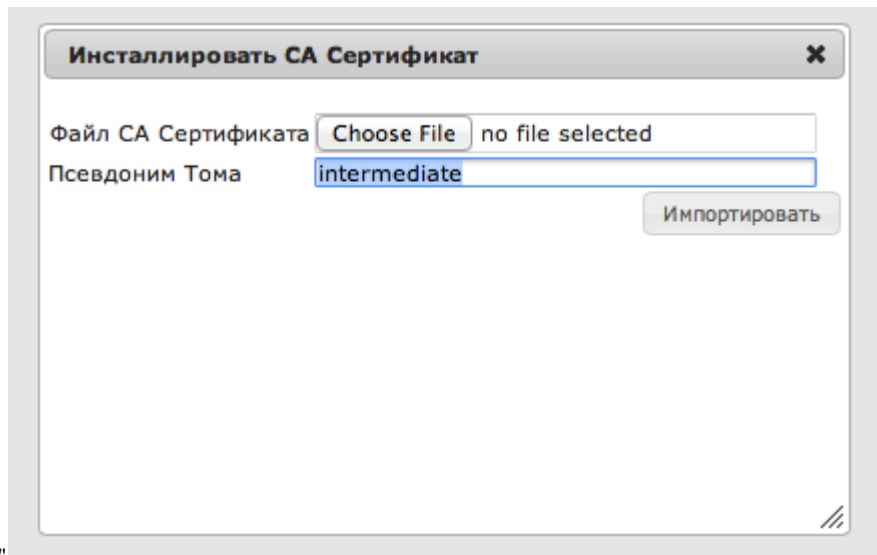
Порядок, в котором вы импортируете сертификаты важен. Сначала необходимо импортировать сертификат корневого центра сертификации, далее промежуточный сертификат и, наконец, сертификат сервера.

1. Нажмите кнопку "Импортировать CA сертификат", выберите root.cert файл, введите "root", как псевдоним и нажмите "Импортировать"



2.

3. Нажмите кнопку "Импортировать CA сертификат", выберите intermediate.cert файл, введите "intermediate", как псевдоним и нажмите



"Импортировать"

- Нажмите кнопку "Импортировать сертификат", выберите user.cert файл, введите аналогичный псевдоним, как вы вводили при генерации CSR "tomcat" и нажмите "Импортировать"
- Если все прошло хорошо, сертификат сервера и сертификат CA должен быть виден в списке сертификатов.

New Server Cert

Create certificate signing request or generate test certificate

Import Server Cert

Import server certificate obtained from a certificate authority

Import CA Cert

Import trusted certificate authority certificate

Server Certificate/s

Show entries

Search:

Alias	Issuer	Subject	Serial No.	Valid From	Valid To	Actions
	C=US,O=VeriSign..	C=US,O=VeriSign..	167792795180741..	2009-04-01	2019-04-01	
	C=US,O=VeriSign..	C=US,O=VeriSign..	299148634490218..	2009-04-01	2029-04-01	
tomcat	C=ZA,ST=Gauteng..	C=US,O=VeriSign..	383556443838423..	2012-08-14	2012-09-14	Delete

First Previous 1 Next Last

Showing 1 to 3 of 3 entries

Trusted Certificate/s

Show entries

Search:

Alias	Issuer	Subject	Serial No.	Valid From	Valid To	Actions
intermediate	C=US,O=VeriSign..	C=US,O=VeriSign..	167792795180741..	2009-04-01	2019-04-01	Delete
root	C=US,O=VeriSign..	C=US,O=VeriSign..	299148634490218..	2009-04-01	2029-04-01	Delete

First Previous 1 Next Last

Showing 1 to 2 of 2 entries

Хранилище ключей

Закрытый ключ и сертификат хранится в стандартном файле хранилища ключей Java. Этот файл называется mailarchivacerts и находится в каталоге конфигурации.

Для дополнительных функций управления сертификатами, таких как ключ и сертификат экспорта, пожалуйста, обратитесь к keystore утилите, включенную в среду выполнения Java.

Для получения кода доступа к хранилищу, запустите в командной строке команду getkeystoresecret. Эта утилита находится в папке server в основной папке приложения.

GetKeyStoreSecret

Retrieve key store password for insertion into Apache Tomcat's server.xml

```
salt [enter=feadf944dd4d62a5] :
encryption password:test
```

```
keystore passphrase:p8qf7M9sBZnW8XALepzKRrMyJ5Y=
```

```
Press enter to continue.
```

Введите пароль шифрования Архива. Полученные Ключевая фраза является паролем к хранилище ключей mailarchivacerts. Если сертификаты в настоящее время используются для TLS, данный пароль может быть введен в Tomcat server.xml для [настройки HTTPS](#) соединения.

