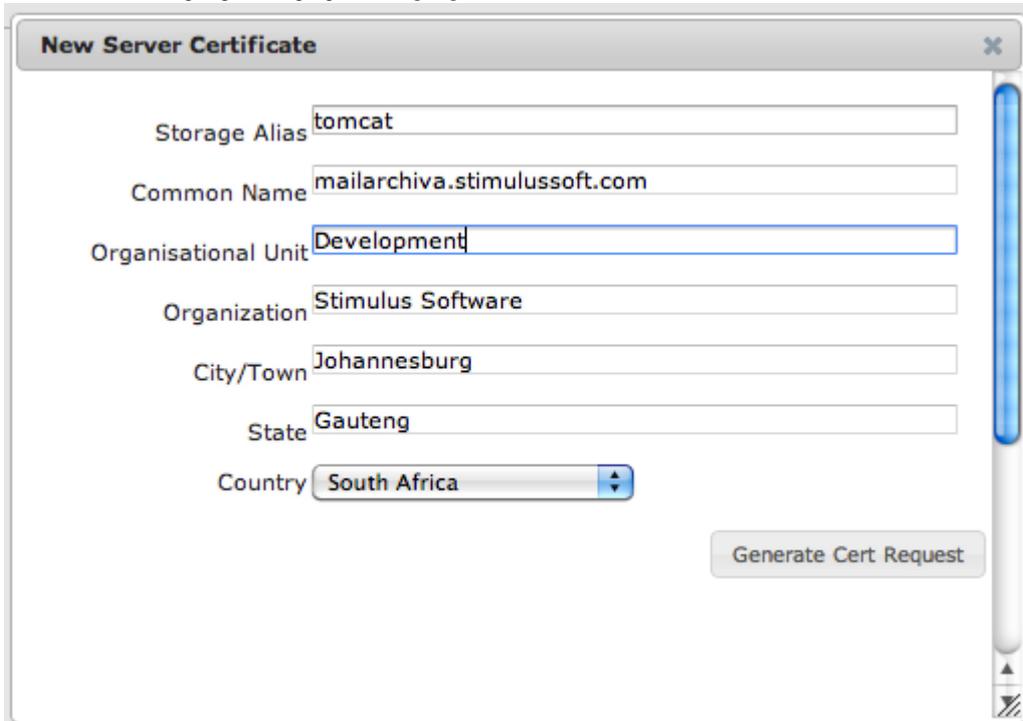


# Сертификаты

В этом разделе описывается, как создать и установить серверный и доверенный сертификат. Сертификаты используются для безопасного доступа к Архива по 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

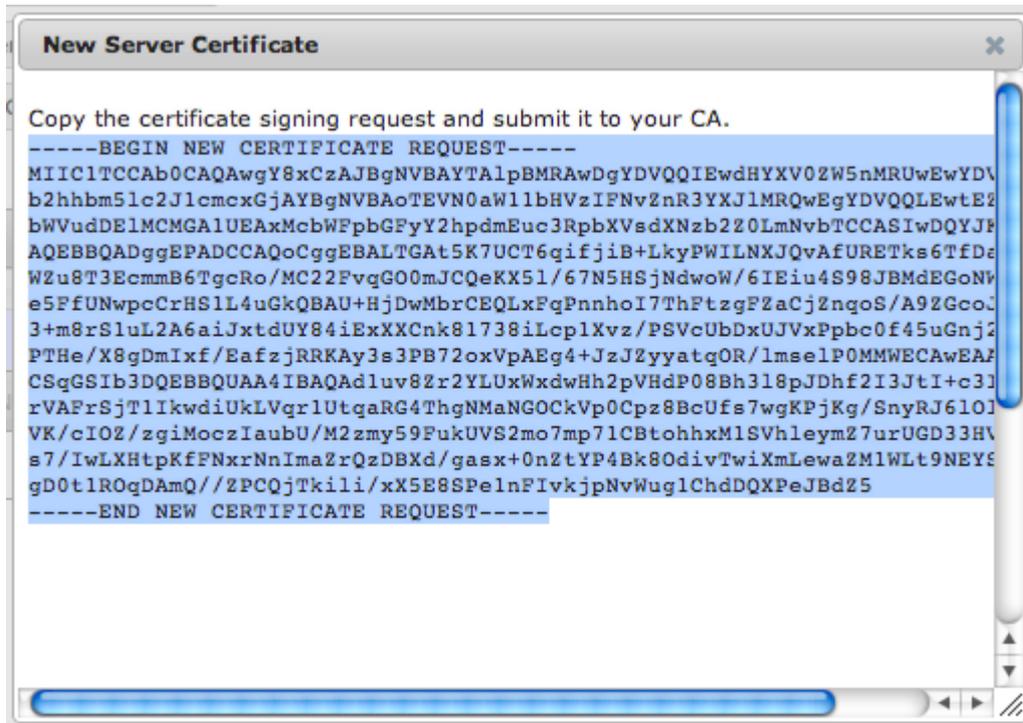
4. Введите common name сертификата

 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-----
MIIB2jCCAU MCAQAwZiorCzAJBgNVBAYTA1VTRCwvFQYDVQQIEw50b3J0aScBDYXJv
bGluYTEQMA4GA1UEBxMUMmFzZWlnaEdEdmBzGA1UEChMUVGhhd3RlIENvbnN1bH
RpbmcmY2MxGzAZBgNVBAsteiRlc3RpbmcmRjVWYXJ0bWVudDElMCMCEGA1UEEA
MadmIjdS9yaWFnbnVWZjwvLnRoYXZ0ZS55b20wgZ8wDQYJKoZIhvcNAQEBBQADgY0
AMGJAAoGBAMaHjIDvYjYnWZjwvEGUvbnKBA1HLh5H3YXifTq5oWc+beUzoG03L
a09ZScZUzMDJ4sTZQnQ7Tu7ZA0JhoefxyhMpe2FwH0NhPURPeEzRQFyajoOmqH
+wR9Jw5W4cEFOqGMxYtHdJAGCjlt9XReVz5YNPwhdqr36hx1Hrld7vAgMBAAGgADAN
BggqhkiG9w0BAQQAFAwOBQDErL49x/kgUusxzL1FwQR9KQZU6JlhEW1JzggugCya
l3buUYZbohNv99qHTaAUc+PccLM1Fw46GvH2EDF.tzvyzPHZwKkIBzxNGstKn55/O0
RhIT8F/P3tn7sqsc401D7gna8WVRZ9k2KMaQLJqdYInz5Ou27IV6EMFw==
-----END CERTIFICATE REQUEST-----

```

**Paste Certificate Signing Request (CSR):** ?

```

MIIC1TCCAAb0CAQAwY8xCzAJBgNVBAYTA1pBMRAwDgYDVQQIEwdHYXV0ZW5nMRUwEwYDV
b2hhbm5lc2J1cmcxGjAYBgNVBAoTEVN0aW11bHVzIFNvZnR3YXJlMRQwEgYDVQQLEwtEz
bWVudDElMCMGA1UEAxMcbWVpY2hpdmc3RpbXVsdXNzb2Z0LmNvbTCCASlwdQYJKoZIh
vncNAQEBBQADggEPADCCAQoCggEBALTGAt5K7UCT6qifjiB+LkyPWILNXJQvAfURETks6TfD
DamqIj/mWZu8T3Ecmmb6TgcRo/MC22FvqGO0mJCQeKX5l/67N5HSjNdwoW/6IEiu4S98J
BMdEGoNwBeFZRY1e5FFUNwpcCrHS1L4uGkQBAU+HjDwMbrCEQLxFqPnnhoI7ThFtzgFZa
CjZnqoS/A9ZGcoJO0Qq8Tu3+m8rS1uL2A6aiJxtduY84iExXXCnk81738iLcp1Xvz/PSVc
UbDxUJVxPpb0f45uGnj2CqSOJn+PThE/X8gDmIxf/EafzjRRKAy3s3PB72oxVpAEg4+JzJZyyatq
OR/lmselP0MMWECAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IBAQAduv8Zr2YLUXWxdwHh2pV
hdP08Bh3l8pJDhf2I3JtI+c3lhO6vd5x rVAFrSjT1IkwdiUkLVqr1UtqarG4ThgNMaNG
OCKVp0Cpz8BcUfs7wgKPjKg/SnyRJ6l0IOMupHkqtVK/cIOZ/zgiMoczIaubU/M2zmy59
FukUVS2mo7mp71CBtohhxM1SVhleyMz7urUGD33HVUmaPgZjs7/IwLXHtpKfPNxrNnIma
ZrQzDBXd/gasx+0nZtYP4Bk8OdivTwiXmLewaZM1WLt9NEYSd9n91VjgD0t1ROqDAmQ//
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.

```

-----BEGIN CERTIFICATE-----
MIIEVzCCAz+gAwIBAgIQFokFkpcJKet+rEvGfsbk1VDANBgkqhkiG9w0BAQUFADCB
jDELMAKGA1UEBhMCVVMxLjZlcm1TaWduLCBjb20uMTAwLjYyLjYyLjYyLjYyLjYy
EydGbz3IqVGVzdCB0dXJwb3NlcyBpbm5lIjAgTm8gYXNzdXJhbW50cy4xMjAwBgNV
BAMTKVZlcm1TaWduIFRvaWVsIFNlY3VvZSB0ZXJ2ZXIqUm9vdCB00SAtIEcyMB4X
DTA5MDQwMTAwMDAwMFoXDTE1MDMzMTEzNTkxMDVowgYwCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW51LjEwMC4GA1UECmMhRm9yIFRlc3Q0UHVycG9z
ZXNlcnR5ZS4gIE5vIGFzc3VyYW51ZXMUMTIwMAYDVOQDEyLWZXJpU2lnbiBUcm1h
bCB0ZXNlcm1UgU2VydmlvYyIFJwb3Qg00EgLSBHMjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMCJggWnSVAcIomnyCFHXLcdaafCKCDxVSNQY2jhYGGZxcZsg
To3mDQ7b9J039VCPnxELOENP2+4FNCUQnzarLfghsJ8kQ9pxjRTfcMp0bsH+Gk/1
aLDgvyf9WuiBa5SM/jXNvroEQzWpUmZg4r2E2k0412VTg9Co10DYNDZw3ziiYdsjY
fY3VfbsLSXJIh2jaJC5kVRsUsx72s4/wgXbb+P/XKr15nMIB0vH9A5tiCCX05n0
EV7/ddZgml3zdeAtyGmij0xjwiY+GS6xr7KACfbPEJYZYaS/P0wctI0yQy6CkNKL
o5yDDk0Zks0zjf6RAzNXZndvsXEJp0e5W01qvm8CAwEAAQ0BSjCBrzAPBgNVHRMB
Af8EBTADAQH/MA4GA1UdWeB/wQEAWIBBjBTBggrBgEFBQcBDARhMF+hXaBbMFkw
VzBVFglpbWFnZS95bnYwITAfMAGBBSs0AwIaBBSF5dMahgynimvDz4Bq1EqYHsZ
LjAlFiNodHRwOi8vbG9nb352ZXJpc2lnbi51b20vdnNsb2dyLmdpZjAdBgNVHQ4E
FgQUSBnnkm+SnrjmcDwmcjWpYyMf2UwDQYJKoZIhvcNAQEFBQADggEBAduSwa8C
0hunHp17KJ00WwNR0Cp8f/u4L8Hz/TiGfybnaMxqn0sKI8Xe79iGE91M7vrzh0Gt
ap0GLShkigHGShkIxBcVMFbEQ1YS63XhTeg36cWQ1EjOHmu+8t0e0oZuwFsYYdfs
n4EZcpspiep9LFc/hu4FE8SsY6MiasHR2Ay97UsC9A3S7ZaoHfdwyhtcINXCu2lX
W0Gpi3vzWRwqgaa6dm2WVKJfvPfmSImAP0YmTcIwjdlNXiU6sSsJEoNlTR9zCoo
4oK08wVowZpbuPZb5geszS7YsABUPIAAfF1YQCIMULtpa6HFzzm7sdf72N3HfWE
aQNg95KnKGrDUI=
-----END CERTIFICATE-----

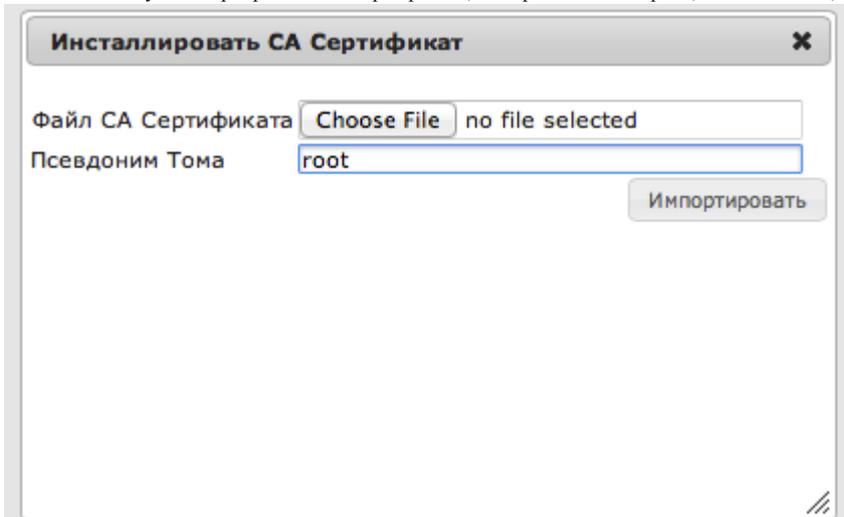
```

9.

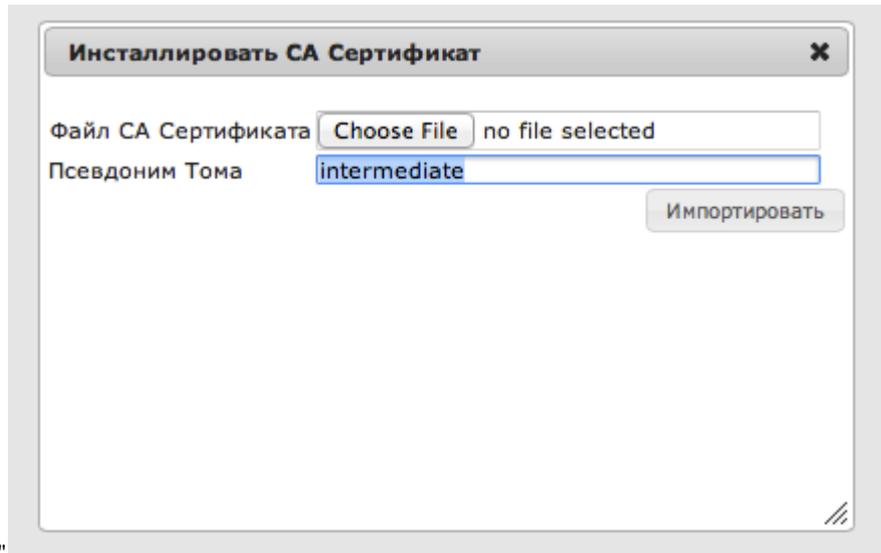
### Импорт сертификатов

**i** 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"

4. Нажмите кнопку "Импортировать сертификат", выберите user.cert файл, введите аналогичный псевдоним, как вы вводили при генерации CSR "tomcat" и нажмите "Импортировать"
5. 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.

