

Доступ по HTTPS

Так-как Архива часто содержит строго конфиденциальную информацию, настоятельно рекомендуется защита доступа к веб-консоли с помощью HTTPS (HTTP / TLS).

Есть два способа настроить защищенный доступ к консоли:

1. [Управление сертификатами Архива](#) - Используйте встроенные в Архива функции управления сертификатами (Enterprise Edition только)
2. [Используйте утилиты командной строки](#) - Используйте встроенные в Java утилиты командной строки (Enterprise Edition и ISP Edition)

Управление сертификатами Архива



Можно использовать только для Архива

1. Следуйте инструкциям в [Сертификаты](#) получите и установите сертификат сервера и соответствующие сертификаты CA.
2. Запустите утилиту `getkeystoresecret`, как описано в [Сертификаты](#). Запомните пароль хранилища ключей паролем.
3. Измените файл `server.xml` расположен в [главный путь к приложению]\server\conf

a) Раскомментируйте строку:

```
<Connector port="443" allowUnsafeLegacyRenegotiation="false" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" keystoreAlias="tomcat" keystoreFile="/etc/opt/mailarchiva/ROOT/mailarchivacerts"
keystorePass="changeit">
```

b) измените значения поля `keystorePass` на значение полученное утилитой `getkeystoresecret`. Убедитесь в правильности ввода.

c) при желании, закомментируйте (небезопасные) соединение по умолчанию на порту 8090.

Отредактируйте `web.xml` расположенный в [главный путь к приложению]\server\webapps\ROOT\WEB-INF



Раскомментируйте строку:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Context</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

Перезапустите сервис Архива `server`, он должен быть доступен по адресу `https://you_server`

Java утилиты командной строки

При использовании командной строки используется утилита `keytool` включенная в дистрибутив JRE. Если Архива была установлена правильно и по умолчанию то данная утилита будет располагаться в директории `C:\Program Files\MailArchiva\jre64\bin` or `/opt/mailarchiva/jre64/bin`.

Среди прочего, утилита `keytool` предоставляет возможность генерировать запросы на сертификат и устанавливать сертификаты в файл хранилища ключей Java.



Приведенные ниже инструкции в значительной степени основана на [Tomcat SSL How To](#).

1. Создайте новое хранилище ключей



Вместо того чтобы вводить имя и фамилию, когда будет предложено сделать это, пожалуйста, введите полное доменное имя сервера Архива (например archiva.company.com)

Выберите надежный путь для хранилища закрытых ключей Tomcat.

```
keytool -genkey -alias tomcat -keyalg RSA -keystore \path\to\my\keystore
```

2. Создайте запрос:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore
```

3. Отправьте Ваш запрос в Ваш сертификационный центр или любой другой авторитетный центра сертификации

4. Сохраните цепь в формате Base64

5. Экпортируйте каждый сертификат в формате Base64

6. Импортируйте цепь сертификатов один сертификат за одним, начиная с root:

```
keytool -import -alias root -keystore -trustcacerts -file b. keytool -import -alias tomcat -keystore -trustcacerts -file
```

7. Настройте TLS соединение встроенное в сервер Tomcat Архива в файле server.xml. server.xml файл находится в папке C:\Program Files \ Архива \ Server \ Conf \ server.xml (Windows) или /opt/ Архива/server/conf/server.xml (Linux)

8. Отредактируйте server.xml и раскомментируйте соединение TLS прослушивающее порт 443. Измените соединение обозначив правильное хранилище ключей и пароль.

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol" port="443" minSpareThreads="5"
maxSpareThreads="75" enableLookups="true" disableUploadTimeout="true" acceptCount="100"
maxThreads="200" scheme="https" secure="true" SSLEnabled="true" keystoreFile="<path\to\keystore>"
keystorePass="changeit" clientAuth="false" sslProtocol="TLS"/>
```

9. Для предотвращения небезопасного трафика, закомментируйте порт 80 соединения в файле server.xml.

10. Если вы хотите автоматически перенаправить обращение к порту 80 на порт 443, отредактируйте web.xml в C:\Program Files\MailArchiva\Server\webapps\ROOT\WEB-INF\web.xml (Windows) или /opt/mailarchiva/server/webapps/ROOT/WEB-INF/web.xml (Linux) дабавьте следующие линии перед закрывающим тегом </web-app>:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Context</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  auth-constraint goes here if you require authentication
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

Перезапустите сервис Архива, он должен быть доступен по адресу https://you_server или http://you_server вы будете автоматически направлены на безопасное соединение https