



Managing OnCommand Workflow Automation SSL certificate

OnCommand Workflow Automation 5.1

NetApp
August 30, 2024

Table of Contents

- Managing OnCommand Workflow Automation SSL certificate 1
 - Replace the default Workflow Automation SSL certificate 1
 - Create a certificate signing request for Workflow Automation 2

Managing OnCommand Workflow Automation SSL certificate

You can replace the default OnCommand Workflow Automation (WFA) SSL certificate with a self-signed certificate or a certificate signed by a Certificate Authority (CA).

The default self-signed WFA SSL certificate is generated during the installation of WFA. When you are upgrading, the certificate for the previous installation is replaced with the new certificate. If you are using a non-default self-signed certificate or a certificate signed by a CA, you must replace the default WFA SSL certificate with your certificate.

Replace the default Workflow Automation SSL certificate

You can replace the default Workflow Automation (WFA) SSL certificate if the certificate has expired or if you want to increase the validity period of the certificate.

You must have root privileges for the Linux system on which you have installed WFA.

The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the custom WFA installation path.

Steps

1. Log in as a root user on the WFA host machine.
2. At the shell prompt, navigate to the following directory on the WFA server: `WFA_install_location/wfa/bin`
3. Stop the WFA database and server services:

```
./wfa --stop=WFA
```

```
./wfa --stop=DB
```

4. Delete the `wfa.keystore` file from the following location:
`WFA_install_location/wfa/jboss/standalone/configuration/keystore`.
5. Open a shell prompt on the WFA server, and then change directories to the following location:
`<OpenJDK_install_location>/bin`
6. Obtain the database key:

```
keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore  
"WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore  
" -validity xxxx
```

xxxx is the number of days for the validity of the new certificate.

7. When prompted, provide the password (default or new).

The default password is a randomly generated encrypted password.

To obtain and decrypt the default password, follow the steps in the Knowledge Base article [How to renew the self-signed certificate on WFA 5.1.1.0.4](#)

To use a new password, follow the steps in the Knowledge Base article [How to update a new password for the keystore in WFA](#).

8. Enter the required details for the certificate.
9. Review the displayed information, and then enter `Yes`.
10. Press **Enter** when prompted by the following message: Enter key password for <SSL keystore> <RETURN if same as keystore password>.
11. Restart the WFA services:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Create a certificate signing request for Workflow Automation

You can create a certificate signing request (CSR) in Linux so that you can use the SSL certificate that is signed by a Certificate Authority (CA) instead of the default SSL certificate for Workflow Automation (WFA).

- You must have root privileges for the Linux system on which you have installed WFA.
- You must have replaced the default SSL certificate that is provided by WFA.

The default WFA installation path is used in this procedure. If you have changed the default path during installation, then you must use the custom WFA installation path.

Steps

1. Log in as a root user on the WFA host machine.
2. Open a shell prompt on the WFA server, and then change directories to the following location:
<OpenJDK_install_location>/bin
3. Create a CSR file:

```
keytool -certreq -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore  
-alias "ssl keystore" -file /root/file_name.csr
```

`file_name` is the name of the CSR file.

4. When prompted, provide the password (default or new).

The default password is a randomly generated encrypted password.

To obtain and decrypt the default password, follow the steps in the Knowledge Base article [How to renew the self-signed certificate on WFA 5.1.1.0.4](#)

To use a new password, follow the steps in the Knowledge Base article [How to update a new password for the keystore in WFA](#).

5. Send the `file_name.csr` file to the CA to obtain a signed certificate.

See the CA web site for details.

6. Download a chain certificate from the CA, and then import the chain certificate to your keystore:

```
keytool -import -alias "ssl keystore CA certificate" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file chain_cert.cer
```

chain_cert.cer is the chain certificate file that is received from the CA. The file must be in the X.509 format.

7. Import the signed certificate that you received from the CA:

```
keytool -import -alias "ssl keystore" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file certificate.cer
```

certificate.cer is the chain certificate file that is received from the CA.

8. Start the WFA services:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.