



# **OnCommand Workflow Automation SSL**

## **인증서 관리**

### **OnCommand Workflow Automation 5.0**

NetApp  
April 19, 2024

This PDF was generated from <https://docs.netapp.com/ko-kr/workflow-automation-50/rhel-install/task-replace-the-default-workflow-automation-ssl-certificate-linux.html> on April 19, 2024. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# 목차

OnCommand Workflow Automation SSL 인증서 관리 .....	1
기본 Workflow Automation SSL 인증서를 교체합니다 .....	1
Workflow Automation에 대한 인증서 서명 요청을 생성합니다 .....	2

# OnCommand Workflow Automation SSL 인증서 관리

기본 WFA(OnCommand Workflow Automation) SSL 인증서를 자체 서명된 인증서 또는 CA(인증 기관)에서 서명한 인증서로 교체할 수 있습니다.

WFA를 설치하는 동안 자체 서명된 기본 WFA SSL 인증서가 생성됩니다. 업그레이드할 때 이전 설치의 인증서가 새 인증서로 바뀝니다. 기본값이 아닌 자체 서명된 인증서 또는 CA에서 서명한 인증서를 사용하는 경우 기본 WFA SSL 인증서를 인증서로 교체해야 합니다.

## 기본 Workflow Automation SSL 인증서를 교체합니다

인증서가 만료되었거나 인증서의 유효 기간을 늘리려면 기본 WFA(Workflow Automation) SSL 인증서를 교체할 수 있습니다.

### 필요한 것

WFA를 설치한 Linux 시스템에 대한 루트 권한이 있어야 합니다.

### 이 작업에 대해

기본 WFA 설치 경로가 이 절차에 사용됩니다. 설치 중에 기본 위치를 변경한 경우 사용자 지정 WFA 설치 경로를 사용해야 합니다.

### 단계

1. WFA 호스트 시스템에서 루트 사용자로 로그인합니다.
2. 셸 프롬프트에서 WFA 서버의 다음 디렉토리로 이동합니다.

```
'WFA_INSTALL_LOCATION/WFA/BIN
```

3. WFA 데이터베이스 및 서버 서비스를 중지합니다.

```
'./WFA- stop=WFA'
```

```
'./WFA - stop=DB'입니다
```

4. 'WFA.keystore' 파일을 다음 위치에서 삭제합니다.  
'WFA\_install\_location/WFA/jboss/standalone/configuration/keystore'
5. WFA 서버에서 셸 프롬프트를 열고 디렉토리를 다음 위치로 변경합니다.

```
'WFA_INSTALL_LOCATION/WFA/JRE/BIN
```

6. 데이터베이스 키 가져오기:

```
"keytool-keysize 2048-genkey-alias "SSL keystore"-keyalg rsa-keystore"  
WFA_install_location/WFA/jboss/standalone/configuration/keystore/WFA.keystore"-enity xxxx"입니다
```

xxxx는 새 인증서의 유효 기간(일)입니다.

7. 메시지가 표시되면 암호를 입력합니다(기본값 또는 새 암호).

기본 비밀번호는 'changit'입니다. 기본 암호를 사용하지 않으려면 'standalone-full.xml' 파일에서 ssl 요소의 password 특성을 'WFA\_install\_location/WFA/jboss/standalone/configuration'에서 변경해야 합니다

◦ 예 \*

```
<ssl name="ssl" password="new_password" certificate-key-  
file="${jboss.server.config.dir}/keystore/wfa.keystore"
```

8. 인증서에 필요한 세부 정보를 입력합니다.
9. 표시된 정보를 검토한 후 Yes를 입력합니다.
10. 다음 메시지가 나타나면 \* Enter \* 를 누릅니다. "Enter key password for <SSL keystore> <return if same as keystore password>".
11. WFA 서비스를 다시 시작합니다.

'./WFA—start=DB'입니다

'./WFA—start=WFA'

## Workflow Automation에 대한 인증서 서명 요청을 생성합니다

WFA(Workflow Automation)용 기본 SSL 인증서 대신 CA(인증 기관)에서 서명한 SSL 인증서를 사용할 수 있도록 Linux에서 CSR(인증서 서명 요청)을 생성할 수 있습니다.

필요한 것

- WFA를 설치한 Linux 시스템에 대한 루트 권한이 있어야 합니다.
- WFA에서 제공하는 기본 SSL 인증서를 교체해야 합니다.

이 작업에 대해

기본 WFA 설치 경로가 이 절차에 사용됩니다. 설치 중에 기본 경로를 변경한 경우 사용자 지정 WFA 설치 경로를 사용해야 합니다.

단계

1. WFA 호스트 시스템에서 루트 사용자로 로그인합니다.
2. WFA 서버에서 셸 프롬프트를 열고 디렉터리를 다음 위치로 변경합니다.

'WFA\_INSTALL\_LOCATION/WFA/JRE/BIN

3. CSR 파일 생성:

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

*FILE\_NAME* 은(는) CSR 파일의 이름입니다.

4. 메시지가 표시되면 암호를 입력합니다(기본값 또는 새 암호).

기본 암호는 \* changeit \* 입니다. 기본 암호를 사용하지 않으려면 'WFA\_install\_location/WFA/jboss/standalone/configuration' 위치에서 'tandalone-full.xml' 파일의 SSL 요소 암호 특성을 변경해야 합니다.

◦ 예 \*

```
<ssl name="ssl" password="new_password" certificate-key-  
file="${jboss.server.config.dir}/keystore/wfa.keystore"
```

5. 서명된 인증서를 얻으려면 \_file\_name.csr\_ 파일을 CA로 보냅니다.

자세한 내용은 CA 웹 사이트를 참조하십시오.

6. CA에서 체인 인증서를 다운로드한 다음 체인 인증서를 키 저장소로 가져옵니다.

```
'keytool-import-alias' ssl keystore CA certificate" -keystore  
WFA_install_location/WFA/jboss/standalone/configuration/keystore/WFA.keystore" -trustcacerts -file  
C:\chain_cert.cer"
```

C:\chain\_cert.cer는 CA로부터 받은 체인 인증서 파일입니다. 파일은 X.509 형식이어야 합니다.

7. CA에서 받은 서명된 인증서를 가져옵니다. 'keytool-import-alias "SSL keystore" -keystore  
WFA\_install\_location/WFA/jboss/standalone/configuration/keystore/WFA.keystore" -trustcacerts -file  
C:\certificate.cer'

C:\certificate.cer는 CA로부터 수신한 체인 인증서 파일입니다.

8. WFA 서비스를 시작합니다.

'./WFA—start=DB'입니다

'./WFA—start=WFA'

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.