

업무가 빨라지는 그룹웨어, 다우오피스

TMW SSL 인증서 적용 가이드

TEAM

다우오피스 운영팀



TMW SSL 인증서 적용 가이드

- 1) 인증서 적용 전 사전 준비사항
- 2) KeyStore Explorer 설치
- 3) 인증서 분해 방법
- 4) TMW 인증서 등록

1) 인증서 적용 전 사전 준비사항

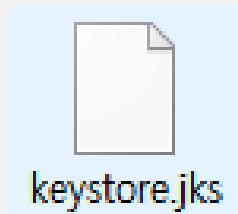
인증서 적용전 발급 기관을 통해 아파치용 인증서를 발급받아야 합니다.



SSL 인증서 적용 전 사전 준비 사항

인증서 발급 기관을 통해 아파치용 인증서를 발급

- jks확장자 파일 하나와 인증서 패스워드 준비



인증서 비밀번호: *****



jks 확장자 형태로 발급 받아야 툴을 이용하여 손쉽게 적용 가능한 형태로 변경 가능합니다.

KeyStore Explorer 툴을 다운로드 받습니다.

KeyStore Explorer 툴을 다운로드 받습니다.



- 1 <https://sourceforge.net/projects/keystore-explorer/> 접속
- 2 [Download] 버튼 클릭
- 3 다운로드 받은 파일 실행



2) KeyStore Explorer 설치 (2/3)

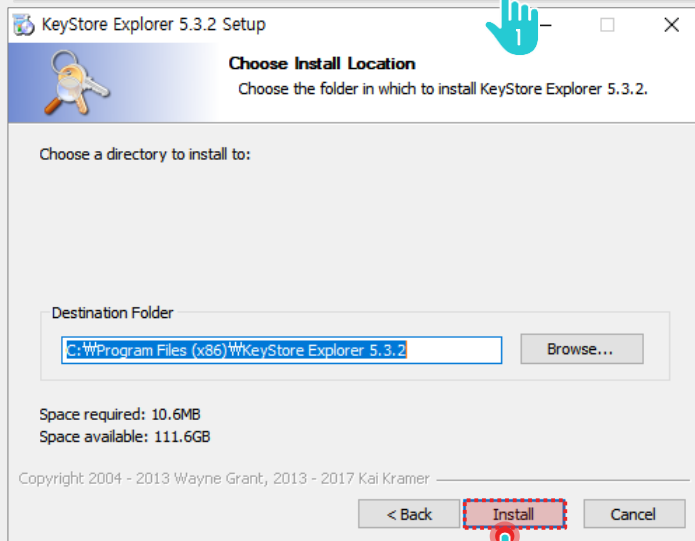
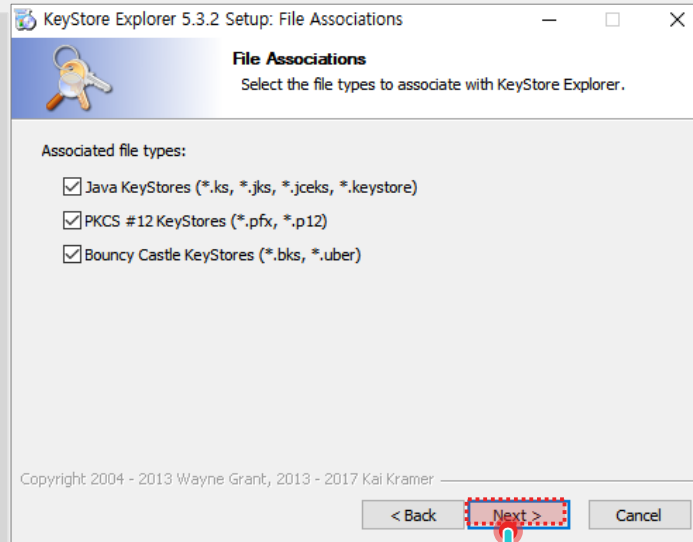
KeyStore Explorer 프로그램 설치 단계를 아래와 같이 수행합니다.



사용자 권한이
필요한 페이지입니다.

Description

- 1 [Next] 버튼 클릭
- 2 [Next] 버튼 클릭
- 3 [Install] 버튼 클릭
(다음장에 계속)





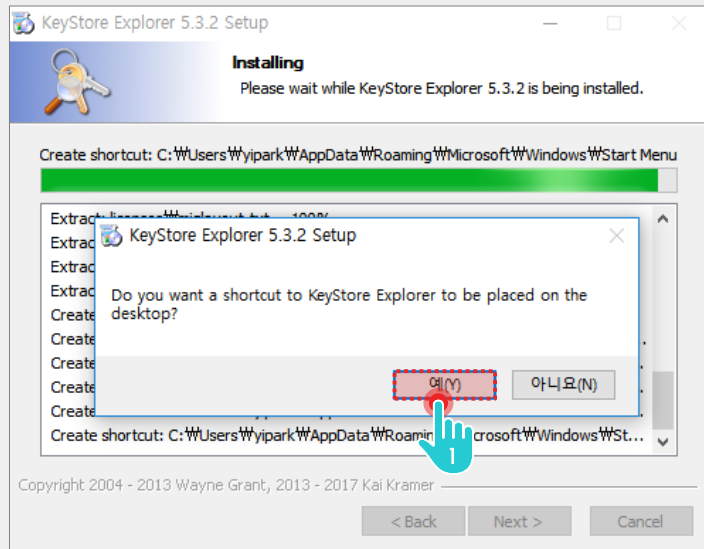
사용자 권한이
필요한 페이지입니다.

2) KeyStore Explorer 설치 (3/3)

KeyStore Explorer 프로그램 설치 단계를 아래와 같이 수행합니다.

Description

- 1 [예(Y)] 버튼 클릭
- 2 [Finish] 버튼 클릭





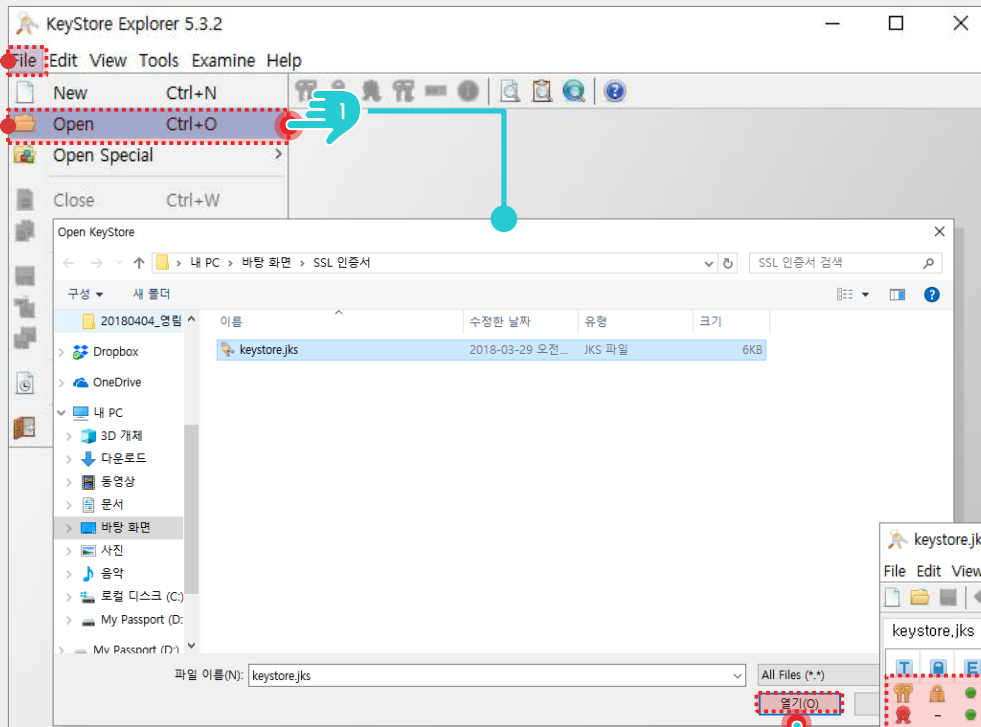
사용자 권한이
필요한 페이지입니다.

3) 인증서 분해 방법 (1/5)_인증서 분해

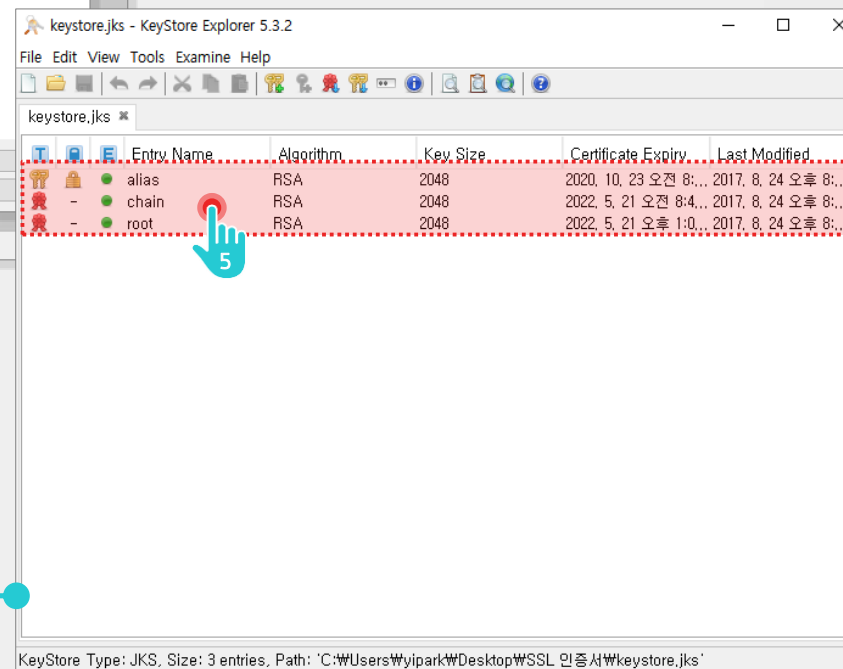
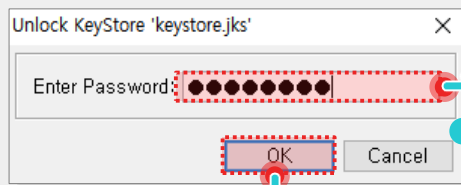
KeyStore Explorer 프로그램 실행 후 jks파일을 드래그하여 프로그램에 적재합니다.

Description

- 1 [파일 > Open] 클릭
- 2 다운로드 받은 jks파일 선택 후 [열기] 클릭
- 3 인증서 발급 시 할당받은 비밀번호 입력
- 4 [OK] 클릭
- 5 인증서 파일 목록 확인



Open an existing KeyStore from disk





3) 인증서 분해 방법 (2/5)_Root 인증서 생성

Root 인증서 파일을 아래와 같이 생성합니다.

keystore.jks - KeyStore Explorer 5.3.2

File Edit View Tools Examine Help

keystore.jks

Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
alias	RSA	2048	2020, 10, 23 오전 8:...	2017, 8, 24 오후 8:...
chain	RSA	2048	2022, 5, 21 오전 8:4...	2017, 8, 24 오후 8:...
root	RSA	2048	2022, 5, 21 오후 1:0...	2017, 8, 24 오후 8:...

View Details >

Cut Ctrl+X

Copy Ctrl+C

Export > Export Certificate

Delete

Rename

Export Public Key

Export Certificate from entry 'root'

Export Format: ☒ X.509 ☐ PKCS #7 ☐ PKI Path ☐ SPC

PEM: ☒

Export File: C:\Users\Wypark\Desktop\SSL 인증서\root.cer

Browse

Export Cancel

Export Certificate

Export Certificate Successful.

확인

Description

- 1 root 인증서 선택 후 오른쪽 마우스 버튼 클릭
- 2 [Export > Export Certificate] 메뉴 클릭
- 3 저장경로 설정
- 4 [Export] 버튼 클릭
- 5 [확인] 버튼 클릭



3) 인증서 분해 방법 (3/5)_chain 인증서 생성

Chain 인증서 파일을 아래와 같이 생성합니다.

keystore.jks - KeyStore Explorer 5.3.2

File Edit View Tools Examine Help

keystore.jks

Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
alias	RSA	2048	2020, 10, 23 오전 8:...	2017, 8, 24 오후 8:...
chain	RSA	2048	2022, 5, 21 오전 8:4...	2017, 8, 24 오후 8:...
root	RSA	2048	2022, 5, 21 오후 1:0...	2017, 8, 24 오후 8:...

Export the Trusted Certificate entry as X.509, PKCS #7, PKI Path or SPC

Export Certificate from entry 'chain'

Export Format: ☒ X.509 ☐ PKCS #7 ☐ PKI Path ☐ SPC

PEM: ☒

Export File: C:\Users\vipark\Desktop\SSL 인증서\chain.cer

Export Cancel

Export Certificate

Export Certificate Successful.

확인

Description

- 1 chain 인증서 선택 후 오른쪽 마우스 버튼 클릭
- 2 [Export > Export Certificate] 메뉴 클릭
- 3 저장경로 설정
- 4 [Export] 버튼 클릭
- 5 [확인] 버튼 클릭



3) 인증서 분해 방법 (4/5)_신뢰받은 인증서 생성

신뢰받은 인증서 파일을 아래와 같이 생성합니다.

keystore.jks - KeyStore Explorer 5.3.2

File Edit View Tools Examine Help

keystore.jks *

Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
alias	IRSA	2048	[2020, 10, 23 오전 8:...] [2017, 8, 24 오후 8:...]	
chain		2048	2022, 5, 21 오전 8:4... 2017, 8, 24 오후 8:...	
root		2048	2022, 5, 21 오후 1:0... 2017, 8, 24 오후 8:...	

Export Certificate Chain from entry 'alias'

Export Length: ☒ Head Only ☐ Entire Chain

Export Format: ☒ X.509 ☐ PKCS #7 ☐ PKI Path ☐ SPC

PEM: ☒

Export File: C:\Users\wypark\Desktop\SSL 인증서\alias.cer

Export Cancel

Export Certificate Chain

Export Certificate Chain Successful.

확인

Description

- 1 회사 인증서 선택 후 오른쪽 마우스 버튼 클릭
- 2 [Export > Export Certificate Chain] 메뉴 클릭
- 3 저장경로 설정
- 4 [Export] 버튼 클릭
- 5 [확인] 버튼 클릭



3) 인증서 분해 방법 (5/5)_개인키 파일 생성

개인키 파일을 아래와 같이 생성합니다.

The screenshot illustrates the steps to export a private key from a Java KeyStore. The main application window, 'keystore.jks - KeyStore Explorer 5.3.2', displays a table of entries. The 'alias' entry is selected, and the 'Export' menu is open, with 'Export Private Key' chosen. This triggers a sequence of dialog boxes: 1. 'Unlock Entry 'alias'' for password entry. 2. 'Export Private Key Type' where 'PKCS #8' is selected. 3. 'Export Private Key as PKCS #8 from KeyStore Entry 'alias'' where the 'Encrypt' checkbox is unchecked and the output file path is specified. 4. A final success dialog with a confirmation button.

Description

- 1 회사 인증서 선택 후 오른쪽 마우스 버튼 클릭
- 2 [Export > Export Private Key] 메뉴 클릭
- 3 인증서 발급 시 할당받은 비밀번호 입력
- 4 [OK] 버튼 클릭
- 5 [OK] 버튼 클릭
- 6 [Encrypt] 체크 해제
- 7 저장경로 입력
- 8 [Export] 버튼 클릭
- 9 [확인] 버튼 클릭



관리자 권한이
필요한 페이지입니다.

4) TMW 인증서 등록 (1/2)

관리자 화면으로 접속하여 환경설정 상세메뉴에서 SSL 인증서를 등록합니다.

Description

- 1 [환경설정] 메뉴 클릭
- 2 [고급기능 > SSL/TLS] 메뉴 선택
- 3 [SSL 인증서] 탭 선택
- 4 [새로운 인증서 등록] 버튼 클릭
- 5 [루트 인증서], [체인 인증서] 체크

※ 루트/체인 등록하면 출력

The screenshot displays the TMW Mail Watcher web interface. At the top, the navigation bar includes '환경 설정' (Environment Settings), which is highlighted with a red dashed box and a hand icon labeled '1'. Below this, the breadcrumb trail shows 'admin님의 현재위치 : 환경 설정 > 고급 기능 > SSL/TLS', with 'SSL/TLS' highlighted and a hand icon labeled '2'. The left sidebar contains a menu where '고급 기능' (Advanced Features) is expanded, and 'SSL/TLS' is selected, indicated by a red dashed box and a hand icon labeled '3'. The main content area shows the 'SSL 인증서' (SSL Certificate) tab, which is also highlighted with a red dashed box and a hand icon labeled '3'. Within this tab, the '신뢰받은 인증서' (Trusted Certificate) dropdown is set to '신뢰받은 인증서' (Trusted Certificate), and the '새로운 인증서 등록' (Register New Certificate) button is highlighted with a red dashed box and a hand icon labeled '4'. A zoomed-in view of the '새로운 인증서 등록' dialog is shown below, with the 'Root 인증서' (Root Certificate) and '체인 인증서' (Chain Certificate) checkboxes checked, indicated by a red dashed box and a hand icon labeled '5'.

4) TMW 인증서 등록 (2/2)

인증서 파일을 아래와 같이 등록합니다.

180326_메일]0 > 내 PC > 바탕 화면 > SSL 인증서

SSL 인증서 검색

이름	수정된 날짜	유형	크기
alias.cer	2018-03-29 오후...	보안 인증서	3KB
alias.pkcs8	2018-03-29 오후...	PKCS8 파일	2KB
chain.cer	2018-03-29 오후...	보안 인증서	2KB
keystore.jks	2018-03-29 오전...	JKS 파일	6KB
root.cer	2018-03-29 오후...	보안 인증서	2KB

파일 이름(N): alias.cer

모든 파일

열기(O) 취소

신뢰받은 인증서

1. Private Key와 신뢰받은 인증서(SSL Certificate)를 등록합니다. (필수 항목)

Private Key: 파일 선택

신뢰받은 인증서: 파일 선택

2. Root 인증서 및 체인 인증서가 필요한 경우 등록을 합니다.(선택 항목)

인증서의 계층 구조에 맞게 등록을 합니다.

☒ Root 인증서 ☒ 체인 인증서

Root 인증서: 파일 선택

체인 인증서: 파일 선택

[O] 버튼 클릭

웹 서버가 재시작되고 있습니다.... 잠시 기다려 주세요.



관리자 권한이
필요한 페이지입니다.

Description

- 1 개인키 파일 등록
- 2 신뢰받은 인증서 파일 등록
- 3 Root 인증서 파일 등록
- 4 체인 인증서 파일 체크
- 5 [O] 버튼 클릭

Thank you