

업무가 빨라지는 그룹웨어, 다우오피스

[TMSe] SSL 인증서 적용 가이드

TEAM
다우오피스 운영팀



[TMSe] SSL 인증서 적용 가이드

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

1) 인증서 적용 전 사전 준비사항

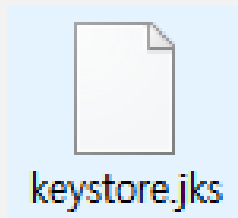
인증서 적용전 발급 기관을 통해 아파치용 인증서를 발급받아야 합니다.



SSL 인증서 적용 전 사전 준비 사항

인증서 발급 기관을 통해 아파치용 인증서를 발급

- jks확장자 파일 하나와 인증서 비밀번호 준비



인증서 비밀번호: *****



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

2) KeyStore Explorer 설치 (1/3)

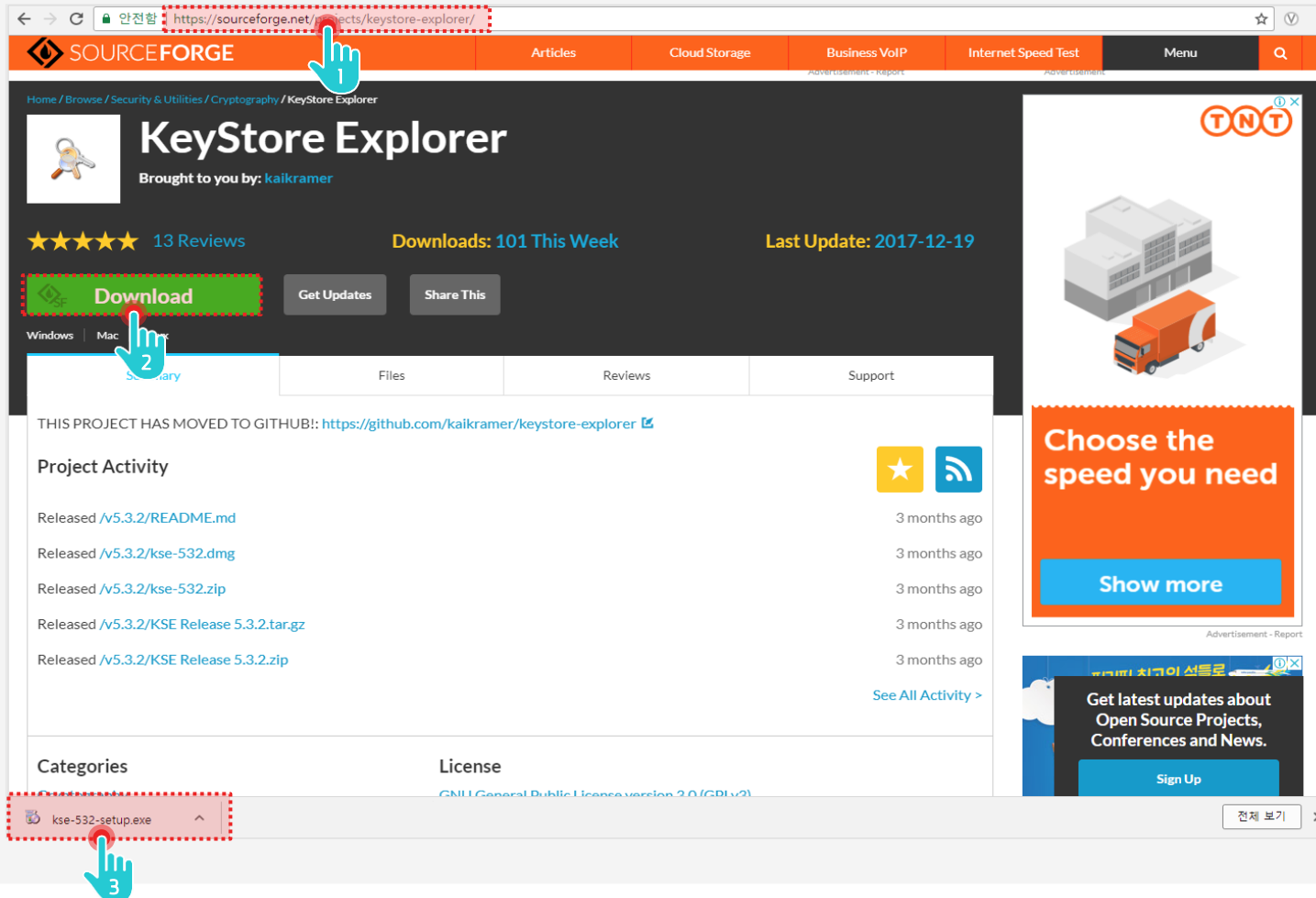
KeyStore Explorer 툴을 다운로드 받습니다.



사용자 권한이
필요한 페이지입니다.

Description

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



2) KeyStore Explorer 설치 (2/3)

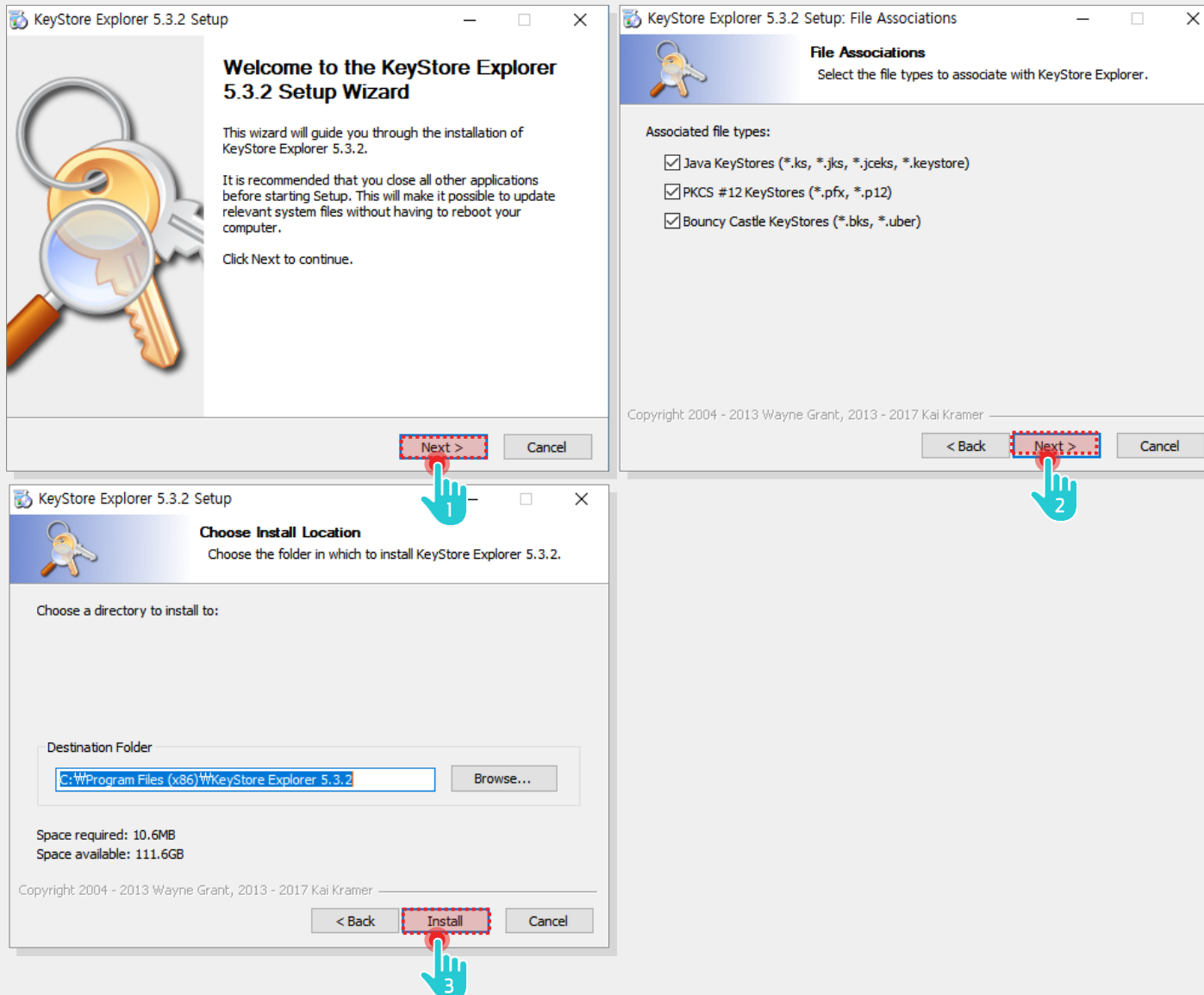
KeyStore Explorer 프로그램 설치 단계를 아래와 같이 수행합니다.



사용자 권한이
필요한 페이지입니다.

Description

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





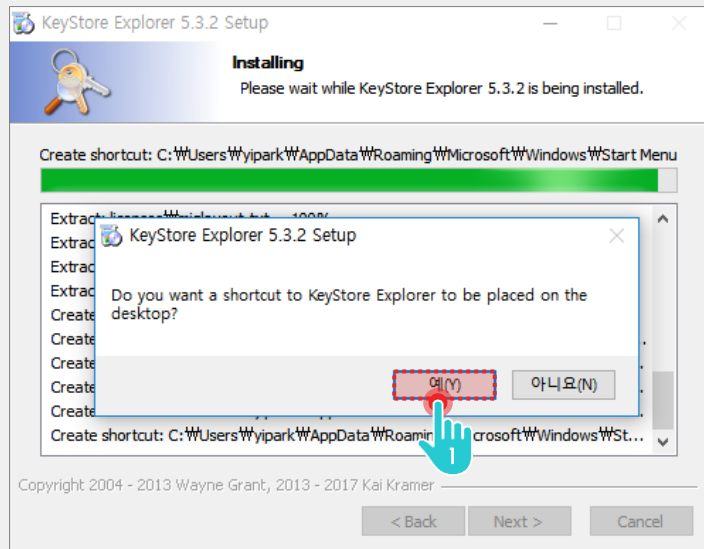
사용자 권한이
필요한 페이지입니다.

2) KeyStore Explorer 설치 (3/3)

KeyStore Explorer 프로그램 설치 단계를 아래와 같이 수행합니다.

Description

- 1 [예(Y)] 버튼 클릭
- 2 [Finish] 버튼 클릭





KeyStore Explorer 프로그램 실행 후 jks파일을 드래그하여 프로그램에 적재합니다.

KeyStore Explorer 프로그램 실행 후 jks파일을 드래그하여 프로그램에 적재합니다.

- 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





사용자 권한이
필요한 페이지입니다.

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



사용자 권한이
필요한 페이지입니다.

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\Wypark\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



사용자 권한이
필요한 페이지입니다.

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	RSA	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



사용자 권한이
필요한 페이지입니다.

3) 인증서 분해 방법 (5/5)_개인키 파일 생성

개인키 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			2022. 5. 21 오전 8:4...	2017. 8. 24 오후 8:...
root			2022. 5. 21 오후 1:0...	2017. 8. 24 오후 8:...

Export Private Key as PKCS #8 from KeyStore Entry 'alias'

Export Private Key as PKCS #8

Export Private Key as PKCS #8 Successful.

Export File: C:\Users\Wypark\Desktop\SSL 인증서\alias.pkcs8

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

4) TMSe 인증서 등록 (1/2)

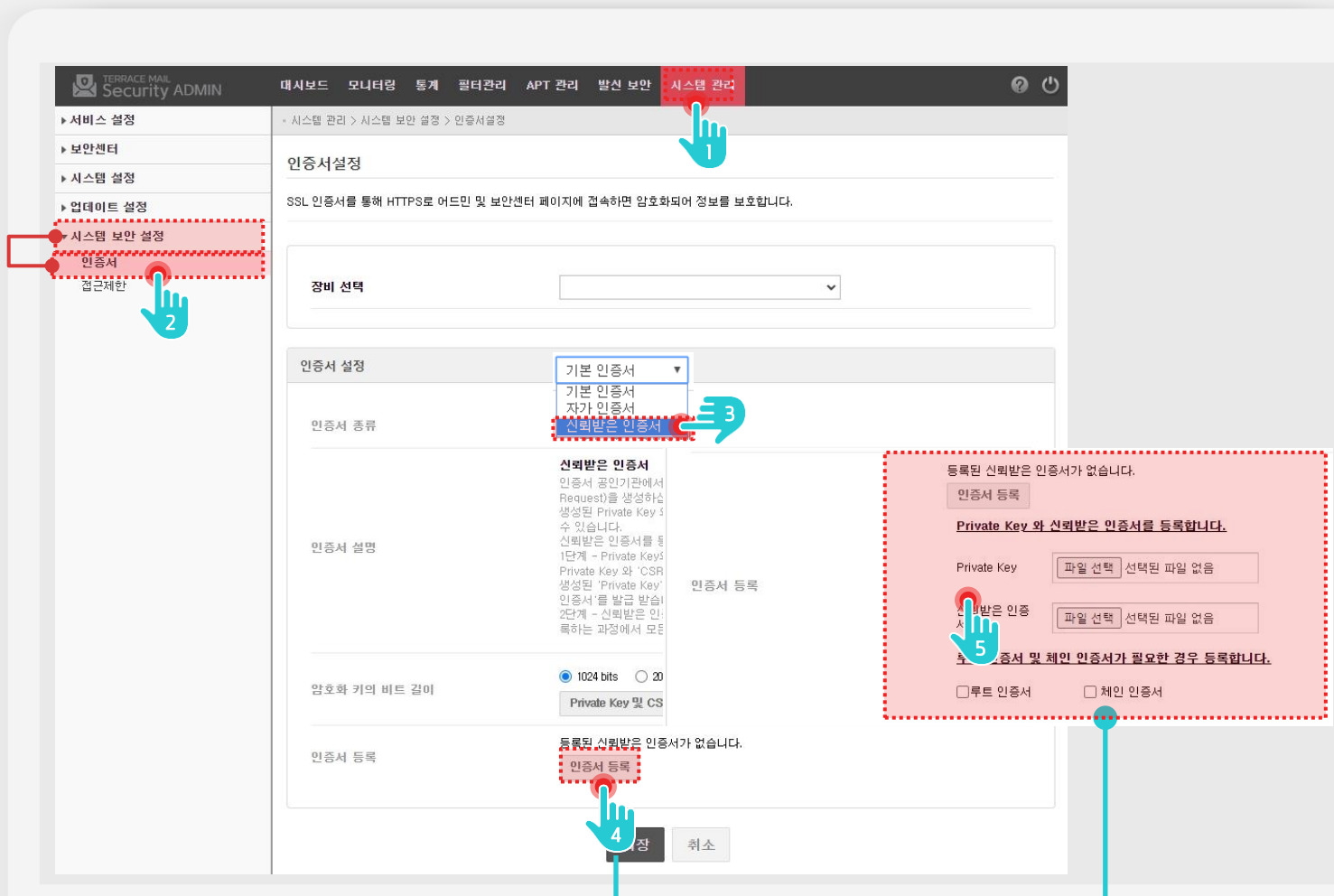
시스템 관리자로 접속하여 인증서 설정화면에 접속합니다.



관리자 권한이
필요한 페이지입니다.

Description

- 1 [시스템 관리] 클릭
- 2 [시스템 보안 설정 > 인증서] 클릭
- 3 인증서 종류 [신뢰받은 인증서] 클릭
- 4 변경된 인증서 설정 화면 하단 [인증서 등록] 클릭
- 5 인증서 등록 행이 파일등록 화면으로 변경





사용자 권한이
필요한 페이지입니다.

4) TMSe 인증서 등록 (2/2)

인증서 파일(개인키, 신뢰받은 인증서, 루트 인증서, 체인 인증서)을 등록 후 저장합니다.

Description

- 1 개인 키, 신뢰받은 인증서 파일 등록
- 2 [루트 인증서], [체인 인증서] 체크 박스 클릭
※ 루트/체인 등록메뉴 활성화
- 3 루트 인증서, 체인 인증서 등록
- 4 [저장] 버튼 클릭
- 5 서버 재기동 알림 메시지 확인 후 [확인] 버튼 클릭
- 6 서버 재기동 완료 후 [확인] 버튼 클릭

Thank you