



Agent

설치·운영 가이드 v1.3

KoreaSSL Certificate
Lifecycle Management

Linux
Windows IIS

목차

1 시작하기

Agent 선택	4
설치 전 준비	5
통신 환경과 호환성	6
자원 사용량	7

2 Linux

설치 환경 확인	8
간편 설치	9
직접 다운로드	10
압축 해제와 최초 설치	11
웹서버와 인증서 탐지	12
기타 서버의 설정 경로	13
인증서 선택과 반영 방식	14
설치와 반영 결과 확인	15
자동 점검과 실행 기록	16
기존 설치 업그레이드	17
언어 설정과 연결 해제	18

목차

3 Windows IIS

설치 준비와 다운로드	19
최초 설치와 서버 연결	20
설정과 IIS 바인딩	21
인증서 연결과 설치 확인	22
서비스와 트레이	23
내부 업데이트와 제거	24

4 KCLM 웹

웹에서 연결 관리	25
세 가지 상태 구분	26

5 운영 점검

Linux 문제 해결	27
통신·동기화 문제 해결	28
설치 완료 확인	29

Agent 선택

1.1 Linux·Windows IIS Agent

KCLM은 코리아SSL에서 발급한 인증서의 연결 상태를 확인하고, 갱신된 인증서를 서버에 반영하도록 돕습니다. 코리아SSL에서 발급한 모든 인증서는 KCLM을 무료로 이용할 수 있습니다.

Agent	설치 위치와 관리 대상
KCLM for Linux	인증서가 설치된 Linux 서버 Nginx, Apache, Tomcat 등의 파일·키스토어
KCLM Agent for IIS	Windows IIS 서버 HTTPS 바인딩과 Windows 인증서 저장소

1.2 실행 방식

Linux는 인증서가 설치된 서버에서 예약 시각에 점검한 뒤 종료합니다. Windows IIS는 IIS 서버에 설치하며 Windows 서비스가 자동 점검을 수행합니다.

이 가이드의 예시 버전: Linux 1.2.6 · IIS 1.2.7
다운로드할 때는 배포된 최신 버전과 CPU 구조를 확인하세요.

설치 전 준비

1.3 계정·인증서·작업 권한

준비 항목	확인 내용
코리아SSL 계정	KCLM 웹에 로그인할 계정과 연결할 발급 인증서
Agent Key	키 사용 가능 상태와 Agent 서버의 IP 제한
작업 권한	Linux: sudo 또는 root Windows IIS: 관리자 권한
운영 정보	도메인, 인증서 경로 또는 IIS 바인딩, 점검 주기
백업	현재 인증서·개인키와 웹서버 설정을 안전하게 보관

1.4 Agent Key 확인

01 KCLM 웹 로그인

<https://kclm.koreassl.com/>에 로그인하고 키 관리에서 Agent Key를 확인합니다.
키가 없으면 발급하거나 관리자에게 요청합니다.

02 사용 상태·허용 IP 확인

IP 제한을 사용한다면 Agent가 외부로 통신할 때 사용하는 IP를 허용 목록에 등록합니다.

Agent Key, 비밀번호, 개인키를 명령행 인수나 공유 문서에 기록하지 마세요.

통신 환경과 호환성

1.5 필요한 네트워크 연결

목적	나가는 HTTPS 연결
KCLM 서버	kclm-api.koreassl.com:443
배포 파일 다운로드	kclm.koreassl.com:443

DNS가 정상적으로 해석되고 서버 시각이 정확해야 합니다. TLS 1.2 이상과 신뢰할 수 있는 인증서를 사용합니다. 연결 오류를 피하려고 TLS 인증서 검증을 끄지 마세요.

1.6 설치 환경 확인

Agent 원격 관리용 수신 포트를 새로 열 필요는 없습니다. 웹사이트 운영에 필요한 80·443 등의 포트는 별도로 관리합니다.

커스텀 경로에 설치한 웹서버는 실행파일과 실제 설정 경로를 확인합니다. 기본 경로를 벗어나는 구성은 경로를 직접 지정해야 할 수 있습니다.

IIS는 Windows 11과 Windows Server 2016에서 검증했습니다. 그 밖의 OS·웹서버 조합은 적용 전에 별도 확인이 필요합니다.

자원 사용량

1.7 참고 실측값

이전 버전의 참고 실측입니다. 최신 버전의 최대 사용량이나 최소 사양을 보장하지 않습니다.

Agent·측정 조건	메모리	CPU
Linux v1.1.17 10개 인증서 모의 조회	최대 RSS 13.7 MiB	조회 1회 평균 0.085초
IIS v1.1.19 GUI 대기	평균 실제 RAM 32.2 MiB	PC 전체 평균 0.103%

측정 환경과 범위

Linux는 Ubuntu 22.04 ARM64에서 측정했습니다. IIS는 Windows 11·논리 CPU 4개에서 약 30초간 GUI 대기 상태를 측정했으며 자동 점검 서비스는 중지했습니다.

실제 운영 부하

인증서 수와 점검 주기, 키스토어 변환·서버 반영에 따라 부하가 달라집니다. 인증서 다운로드·교체, 웹서버 검사·재반영과 IIS 서비스의 부하는 위 수치에 포함되지 않았습니다.

1 MiB = 1,048,576바이트입니다. CPU 소비 시간(초)과 CPU 사용률(%)은 서로 다른 지표입니다. Linux 최대 RSS와 Windows 평균 실제 RAM도 측정 기준이 다릅니다.

설치 환경 확인

2.1 CPU 구조와 기존 설치

```
uname -m
/usr/local/lib/kclm-agent/kclm-agent -version
```

조회 결과	사용할 배포본
x86_64 또는 amd64	linux-amd64
aarch64 또는 arm64	linux-arm64
설치 경로에 Agent가 있음	신규 설치 대신 upgrade.sh 사용

필수 도구

curl 또는 GNU wget, tar, sha256sum과 표준 셸 도구가 필요합니다. 예약 점검에는 실행 가능한 systemd 또는 cron이 필요합니다. 설치 스크립트는 apt·yum 등의 OS 패키지를 자동 설치하지 않습니다.

기본 설치와 인증서 연결

v1.2.5부터는 초기 인증서 검색·연결을 중단해도 기본 실행파일과 kclm-agent 명령이 유지됩니다. 다시 kclm-agent를 실행해 연결을 이어갈 수 있습니다. 인증서를 연결하기 전에는 해당 인증서의 자동 점검이 시작되지 않습니다.

간편 설치

2.2 curl로 최신 버전 설치

```
curl -q -fsS -o agent.sh \  
https://kclm.koreassl.com/agent.sh && sudo sh agent.sh
```

CPU 구조를 확인한 뒤 공개된 최신 배포본을 다운로드합니다. SHA-256, 압축 구성과 실행파일 버전을 검사하고 신규 설치 또는 업그레이드로 진행합니다.

GNU wget 사용

```
wget --no-config -O agent.sh \  
https://kclm.koreassl.com/agent.sh && sudo sh agent.sh
```

설치 전 검사만 실행

```
sudo sh agent.sh --check-only
```

처음 설치할 때는 대화형 터미널에서 Agent Key와 인증서 연결을 확인해야 합니다. 스크립트를 다운로드하는 것만으로 설치되지는 않습니다. GNU wget의 옵션 지원 여부도 확인하세요.

직접 다운로드

2.3 버전·CPU 구조 지정

아래는 Linux v1.2.6 amd64 예시입니다. ARM64 서버는 ARCH=arm64로 바꿉니다. 지정한 버전의 배포본이 공개되어 있어야 합니다.

```
VERSION=1.2.6
ARCH=amd64
FILE="kclm-agent-${VERSION}-linux-${ARCH}.tar.gz"
BASE="https://kclm.koreassl.com/download"
curl -q -fsS -o "$FILE" "$BASE/$FILE"
```

배포 파일 SHA-256 확인

```
sha256sum "$FILE"
```

공식 배포 체크섬과 일치할 때만 압축을 풉니다. 다른 버전이나 CPU 구조의 체크섬을 비교하면 안 됩니다.

Linux v1.2.6 amd64

1d7b7da9f43acf33e97ac75fb694e838402b8f5ca60c38c4146d905a4429d753

Linux v1.2.6 arm64

e1d3727b77f58c686d13f16289d05f8dbe3798ec96c5fb51ca5bec1fe66baae1

압축 해제와 최초 설치

2.4 배포 폴더에서 실행

앞 페이지와 같은 터미널에서 진행합니다. VERSION, ARCH, FILE을 다시 지정해야 하는 경우에는 다운로드한 파일명에 맞춥니다.

```
tar -xzf "$FILE" && \
  cd "kclm-agent-${VERSION}-linux-${ARCH}" && \
  sha256sum -c SHA256SUMS && sudo sh install.sh
```

01 내부 파일 검사

SHA256SUMS의 모든 항목이 OK인지 확인합니다. 실패한 파일이 있으면 실행하지 말고 다시 다운로드합니다.

02 Agent Key 인증

연결 설정에서 Agent Key를 입력하고 KCLM 서버와의 인증 결과를 확인합니다.

03 서버 인증서 연결

서버 인증서와 KCLM 발급 인증서를 선택하고 반영 방식·점검 주기를 확인한 뒤 저장합니다.

기존 설치가 있으면 install.sh는 교체를 거부합니다. upgrade.sh 또는 간편 설치 스크립트의 업그레이드 절차를 사용하세요.

웹서버와 인증서 탐지

2.5 설치 위치에 맞는 검색

```
sudo kclm-agent discover
```

일반 Apache와 Bitnami의 apache·apache2 경로를 함께 검사하며, 각 설정에 맞는 실행파일을 사용합니다.

커스텀 Apache 경로 지정

```
sudo kclm-agent discover \
  --apache-conf /custom/apache/conf/httpd.conf \
  --apache-bin /custom/apache/bin/httpd
```

Bitnami Apache 예시

```
sudo kclm-agent discover \
  --apache-conf /opt/bitnami/apache2/conf/httpd.conf \
  --apache-bin /opt/bitnami/apache2/bin/httpd
```

discover는 조회 명령이며 인증서를 설치하지 않습니다. 모든 커스텀 구성을 자동으로 찾는 것은 아니므로 조회된 경로와 도메인을 확인하세요.

기타 서버의 설정 경로

Nginx 커스텀 설치 예시

```
sudo kclm-agent discover \
  --nginx-conf /custom/nginx/conf/nginx.conf \
  --nginx-bin /custom/nginx/sbin/nginx
```

설정 파일 직접 지정

서버	검색 옵션
Tomcat	--tomcat-conf /path/to/server.xml
Spring Boot	--spring-conf /path/to/application.properties
JBoss/WildFly	--jboss-conf /path/to/standalone.xml
WebtoB	--webtob-conf /path/to/http.m
JEUS	--jeus-conf /path/to/domain.xml

경로는 현재 서버가 사용하는 실제 설정 파일로 바꿉니다. 기본 경로 밖에 설치한 서버는 조회 결과의 도메인·인증서 경로와 설정 검사 명령을 대조합니다.

키스토어는 형식·별칭·비밀번호 설정에 따라 추가 연결 설정이 필요할 수 있습니다. 조회된 목록에 나타난다는 사실만으로 교체 가능한 구성이 확정되는 것은 아닙니다.

인증서 선택과 반영 방식

2.6 서버 인증서와 KCLM 인증서 연결

01 관리 메뉴에서 인증서 추가

웹서버 버전, 도메인, 현재 인증서 유효기간과 파일 경로를 확인하고 대상을 선택합니다.

02 추천 인증서 확인

선택한 도메인의 CN/SAN과 정상 구독을 기준으로 추천 목록을 확인합니다. 필요한 경우 전체 인증서 목록으로 전환합니다.

03 CA·제품명·만료일 비교

주문번호만으로 선택하지 말고 CA, 제품명, 인증 유형과 구독 최종 만료일을 함께 확인합니다.

2.7 자동 반영과 수동 반영

구분	운영 방식
자동 반영	설정된 점검에서 교체가 필요하면 검증 후 파일 교체·서버 반영
수동 반영	점검 결과를 확인하고 사용자가 서버 반영 작업 실행

설정 검사·재반영 명령을 임의로 바꾸지 마세요. Apache는 전체 httpd.conf 검사와 graceful 지원 여부를 확인합니다. 기존 인증서가 만료됐더라도 새 인증서의 유효성 검증은 유지됩니다.

설치와 반영 결과 확인

2.8 실제 설치된 버전 확인

```
/usr/local/lib/kclm-agent/kclm-agent -version
sudo kclm-agent --menu
sudo kclm-agent -dry-run
```

다운로드 폴더의 ./kclm-agent와 설치 경로의 버전은 다를 수 있습니다. 예약 실행은 설치 경로의 실행파일을 사용합니다.

확인할 인증서 정보

항목	판단 기준
서버 인증서	실제 로컬 파일·키스토어에 설치된 인증서
KCLM 인증서	현재 연결한 주문·인증서 ID와 CA·제품명
설치 일치	선택한 인증서와 설치된 인증서의 SHA-256 지문
만료일	서버 인증서 만료일과 구독 최종 만료일을 구분

CA·제품명이 바뀌었다는 이유만으로 교체 완료를 판단하지 마세요. 실제 파일과 재반영 결과, 필요한 경우 접속 지문까지 확인합니다.

자동 점검과 실행 기록

2.9 systemd 예약 상태 확인

```
sudo systemctl status kclm-agent.timer
sudo systemctl list-timers kclm-agent.timer
sudo journalctl -u kclm-agent.service -n 50 --no-pager
```

점검 서비스는 실행 후 종료하는 방식입니다. 서비스가 계속 active 상태여야 하는 것은 아닙니다. timer의 활성 상태와 다음 예약, 서비스의 마지막 종료 결과를 함께 확인합니다.

인증서별 점검 시각

Agent에서 마지막 자동 점검 시각과 다음 예정 시각을 확인합니다. 설정된 주기가 있어도 실제 예약기가 멈춰 있으면 점검은 실행되지 않습니다.

예약을 기다리지 않고 점검

```
sudo kclm-agent --run
```

--run은 실제 점검입니다. 자동 반영으로 설정한 대상은 인증서 교체와 서버 반영이 진행될 수 있습니다. cron 환경은 /etc/cron.d/kclm-agent와 cron 데몬 상태를 확인합니다.

기존 설치 업그레이드

2.10 upgrade.sh 사용

새 배포본을 압축 해제한 폴더에서 실행합니다. 기존 Agent, CPU 구조, 실행파일 형식, 설정과 예약 상태를 먼저 검사합니다.

```
sudo sh upgrade.sh --check-only
sudo sh upgrade.sh
```

간편 설치 명령도 기존 설치를 발견하면 업그레이드 절차로 전환합니다. 교체 후에는 이전 설정을 유지하고 자동 점검 예약을 다시 활성화합니다.

교체 후 확인

```
/usr/local/lib/kclm-agent/kclm-agent -version
sudo systemctl status kclm-agent.timer
```

업그레이드가 중단됐다면

검사에서 중단된 경우 강제로 실행파일만 덮어쓰지 마세요. 교체 중 실패하면 이전 실행파일과 예약으로 복구를 시도합니다. 강제 종료 후 복구 기록이 남았다면 임의로 삭제하지 말고 오류와 백업 위치를 확인합니다.

Linux v1.2.6에는 systemd 219에서도 동작하도록 속성 조회 호환성 수정이 포함되어 있습니다. Agent Key와 기존 연결 설정은 업그레이드 과정에서 유지됩니다.

언어 설정과 연결 해제

2.11 영어·한국어 선택

```
sudo kclm-agent --language en --menu
sudo kclm-agent --language ko --menu
```

기본 언어는 시스템 로케일로 판단하며 한국어 이외에는 영어를 사용합니다. 터미널에 한글 글꼴이 없으면 영어로 실행하세요. Agent가 원격 터미널의 글꼴을 설치하거나 바꾸지는 않습니다.

2.12 관리 대상 정리

01 관리 메뉴에서 연결 해제 선택

해제할 도메인과 연결 인증서를 다시 확인합니다.

02 Agent와 웹의 동기화 확인

KCLM 웹에서 관리 해제 요청과 완료 상태를 확인합니다. 이미 시작된 교체·복구 작업이 있다면 먼저 결과를 확인합니다.

연결 해제는 설치된 인증서 파일, 웹서버 사이트 또는 코리아SSL 주문을 삭제하는 작업이 아닙니다.

설치 준비와 다운로드

3.1 IIS 서버에서 준비할 항목

관리자 권한으로 작업합니다. IIS 사이트, HTTPS 호스트명, IP·포트와 현재 바인딩을 확인하고 IIS 설정과 인증서 저장소를 백업합니다.

공식 ZIP 다운로드

<https://kclm.koreassl.com/download/kclm-agent-1.2.7-windows-amd64.zip>

ZIP 전체를 같은 폴더에 압축 해제합니다. 실행파일만 따로 옮기지 마세요.

3.2 디지털 서명 확인

01 실행파일 속성 열기

디지털 서명 탭에서 서명 상태가 유효한지 확인합니다.

02 서명자 확인

Korea Digital Certificate Authority Inc.인지 확인합니다. 프로그램 및 기능에 표시되는 게시자는 한국디지털인증(주)입니다.

IIS Agent는 IIS 서버에 설치합니다. 운영 서버에 적용하기 전에는 해당 OS·IIS 구성에서 시험하는 것이 필요합니다.

최초 설치와 서버 연결

3.3 Setup 실행

01 KCLM-Agent-IIS-Setup.exe 실행

관리자 권한 요청과 설치 경로를 확인합니다. 설치 후 바로가기 또는 KCLM-Agent-IIS.exe를 실행합니다.

02 Agent Key 입력

신규 Setup 설치 시 Agent Key가 초기화됩니다. 사용할 키를 입력하고 KCLM 서버 연결 확인 후 저장합니다.

03 인증서 연결 후 서비스 확인

프로그램이 설치됐다는 이유만으로 자동 점검이 시작되지는 않습니다. 인증서 연결을 완료하고 서비스 화면에서 실행 상태를 확인합니다.

기본 연결 주소

```
https://kclm-api.koreassl.com/v1
```

일반 업데이트에는 도움말의 내부 업그레이드를 사용하세요. Setup 재실행과 내부 업그레이드는 Agent Key 보존 방식이 다릅니다.

설정과 IIS 바인딩

3.4 파일 → 설정

설정	동작
화면 언어	한국어 · 영어 · 일본어 · 중국어(간체)
KCLM 서버 주소	현재 주소는 읽기 전용으로 표시 변경 버튼과 확인 절차를 거쳐 수정
Agent Key	현재 키 표시 → 변경 확인 → 새 키 입력
연결 확인 및 저장	서버와 키의 검증이 성공한 뒤 저장

3.5 연결할 IIS 사이트 확인

인증서 연결에서 IIS 사이트와 HTTPS 바인딩을 선택합니다. 사이트명, 호스트명, IP·포트와 현재 인증서를 대조합니다. 목록이 비어 있으면 IIS 검색을 다시 실행합니다.

서버 주소나 계정을 바꾸면 기존 연결에 재연결이 필요할 수 있습니다. 설정 저장 후 연결 범위와 대상 계정을 다시 확인하세요.

인증서 연결과 설치 확인

3.6 KCLM 인증서 선택

01 도메인·CA·제품명 비교

주문번호, 인증 유형, 유효기간과 구독 최종 만료일을 확인합니다. 연결할 호스트는 인증서의 CN/SAN 범위에 포함돼야 합니다.

02 점검 주기와 반영 방식 지정

자동 또는 수동 반영을 선택하고 연결을 저장합니다.

03 IIS 설치 결과 확인

현재 인증서와 선택한 인증서가 다르다면 반영 상태를 확인하고 실제 IIS 바인딩의 인증서를 대조합니다.

3.7 목록의 만료일 구분

열	의미
서버 인증서 만료	IIS에 설치된 인증서의 실제 만료일
구독 최종 만료일	연결한 인증서 상품의 구독 종료일
상태·상세정보	정상·반영 대기·확인 필요를 구분 행을 두 번 클릭해 상세 확인

서비스와 트레이

3.8 GUI와 자동 점검 서비스

조작	결과
서비스 화면	KCLMAgentIIS 서비스 설치·실행 상태 확인
창 닫기 X	트레이로 숨김 트레이에서 다시 열기 가능
파일 → 끝내기	GUI 완전 종료 실행 중인 점검 서비스는 계속 동작
서비스 중지	서비스에 의한 자동 점검 중단
웹에서 특정 연결 중지	해당 연결의 정책을 다음 Agent 통신에서 반영

점검이 실행되지 않을 때

서비스가 실행 중인지 확인한 뒤 인증서별 점검 주기와 마지막 점검 시각을 확인합니다. 화면의 KCLM 서버 연결 상태만으로 자동 점검 서비스가 정상이라고 판단하지 마세요.

서비스 중지나 관리 중지는 기존 IIS 사이트와 설치된 인증서를 제거하지 않습니다.

내부 업데이트와 제거

3.9 도움말 → 최신 버전 확인

01 현재·최신 버전 비교

업데이트가 제공되는지 확인하고 프로그램 안에서 다운로드를 시작합니다.

02 검증 후 업그레이드

다운로드 진행률을 확인합니다. 파일 무결성, 코드서명, 제품·게시자·버전을 검증한 뒤 교체합니다.

03 재실행 후 상태 확인

버전, Agent Key, 연결 목록과 서비스 상태를 확인합니다. 내부 업그레이드는 기존 설정을 유지합니다.

3.10 프로그램 제거

Windows 설정의 앱 또는 프로그램 및 기능에서 제거합니다. 프로그램 제거와 IIS 사이트·인증서 삭제는 서로 다른 작업입니다.

내부 업그레이드는 IIS 1.2.5부터 제공됩니다. 이전 버전은 설정 보존을 확인하고 업데이트 절차를 진행하세요. 일반 업데이트에 Setup을 다시 실행하면 Agent Key가 초기화됩니다.

웹에서 연결 관리

4.1 대시보드·연결 관리

KCLM 웹에서 서버·Agent·인증서 연결과 마지막 보고 시각을 확인합니다. OS·웹서버 버전, CA·제품명과 서버 그룹을 함께 확인할 수 있습니다.

4.2 원격 변경 요청

작업	처리 방식
인증서 변경	대상 도메인과 새 CA·제품명을 대조 화면의 도메인 재입력 등 확인 절차 완료
중지·재개	Agent의 다음 통신에서 정책 반영 기존 웹서버와 인증서는 유지
관리 해제	해제 요청과 Agent 동기화 완료를 확인 진행 중 작업이 있다면 결과를 확인

웹 새로고침과 Agent 통신

웹의 자동 갱신은 서버에 저장된 최신 보고를 조회합니다. 자동 갱신 카운트가 지났다고 Agent의 새 점검이나 보고가 즉시 발생하는 것은 아닙니다. 변경 요청 시각과 마지막 보고 시각을 함께 확인하세요.

세 가지 상태 구분

4.3 연결·설치·공개 HTTPS

정보	무엇을 확인하는가
Agent 연결 상태	마지막 생존 보고와 KCLM 서버 통신 상태
인증서 설치·일치	연결 인증서와 실제 설치 인증서의 지문 비교
공개 HTTPS 참고	접속 URL에서 응답한 인증서와 수집 시각

Linux·IIS의 내부망 서버는 공개 접속 정보가 없을 수 있습니다. 공개 HTTPS 정보가 없다는 사실만으로 인증서 설치 실패라고 판단하지 않습니다.

만료일도 구분해서 확인

서버 인증서 만료일은 현재 설치된 인증서의 유효기간입니다. 구독 최종 만료일은 상품의 구독 종료일이며, 둘은 같지 않을 수 있습니다.

제품명 변경과 실제 교체

화면의 제품명만 보고 설치 완료로 판단하지 마세요. 설치 지문과 재반영 결과를 확인합니다. 외부 접속 정보는 프록시·로드밸런서·다중 서버에 따라 로컬 인증서와 다를 수 있습니다.

Linux 문제 해결

5.1 증상별 확인 순서

증상	먼저 확인할 내용
명령을 찾을 수 없음	/usr/local/bin/kclm-agent와 설치 코어 확인 설치가 완료됐는지 확인
인증서가 검색되지 않음	discover 안내 → 실제 설정·실행파일 경로 인증서·개인키 파일 권한과 쌍 일치 확인
다른 제품으로 표시됨	연결 주문·인증서 ID → 로컬 지문 → 반영 결과
자동 점검 기록 없음	timer/cron → 마지막 서비스 종료 결과 연결 저장·인증서별 점검 주기 확인
업그레이드 검사 실패	오류를 확인하고 중단 원인 해결 실행파일 강제 덮어쓰기나 복구 기록 삭제 금지

Bitnami Apache의 명령 구성

```
/opt/bitnami/apache2/bin/httpd -t \  
-f /opt/bitnami/apache2/conf/httpd.conf  
/opt/bitnami/apache2/bin/httpd -k graceful \  
-f /opt/bitnami/apache2/conf/httpd.conf
```

위 명령의 두 번째는 실제 재반영입니다. 설정 검사 성공과 대상 경로를 확인한 뒤에만 사용합니다.
인증서 설정은 bitnami.conf에 있어도 최상위 httpd.conf를 검사합니다.

통신·동기화 문제 해결

5.2 KCLM 서버에 연결되지 않을 때

DNS와 TLS, 서버 시각을 확인한 뒤 서버 주소, Agent Key 사용 상태, IP 제한 순서로 확인합니다.

5.3 웹에 이전 상태가 남을 때

Agent 실행 여부와 서비스·예약 상태, 마지막 보고 시각을 확인합니다.

5.4 실제 접속 인증서가 다를 때

로컬 파일 또는 IIS 바인딩의 지문, 재반영 결과, 실제 TLS 응답을 차례로 확인합니다. 여러 IP나 프록시·로드밸런서가 있으면 각 접속 경로를 따로 확인합니다.

지원 요청에 필요한 정보

포함할 정보	제외할 정보
Agent 버전, OS·웹서버 버전 도메인, 발생 시각, 오류 문구	Agent Key, 비밀번호 개인키와 인증 토큰

설치 완료 확인

5.5 운영 시작 전 점검

점검 항목	완료 기준
서버 연결	Agent Key 인증 성공 올바른 계정과 대상 도메인
인증서	CA·제품명·유효기간 확인 실제 설치 지문과 반영 결과 확인
자동 운영	Linux: timer 또는 cron Windows IIS: Windows 서비스
웹 동기화	마지막 보고와 변경 요청 상태 확인
업데이트	다운로드 폴더가 아닌 설치 경로의 버전 확인

한국디지털인증 주식회사

tech@koreassl.com

1644-4308

가이드 수정 이력

- 2026-02-01 v1.0 최초 작성
- 2026-03-01 v1.1 설치전 준비 페이지 수정 5p
- 2026-08-15 v1.2 내부 업데이트와 제거 페이지 수정 24p
- 2026-10-30 v1.3 최신 Agent에 기능 및 내용 최신화