Dell Security Management Server
설치 및 마이그레이션 가이드 v10.2.12

August 2020
개정 A01

참고, 주의 및 경고

노트: 참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

주의: 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

경고: 경고는 재산 손실, 신체적 상해 또는 사망 위험이 있음을 알려줍니다.

목차

1

소개

Security Management Server 정보

Security Management Server의 특징은 다음과 같습니다.

- 장치, 사용자 및 보안 정책의 중앙 집중식 관리
- 중앙 집중화된 준수 감사 및 보고
- 관리 임무 구분
- 역할 기반의 보안 정책 생성 및 관리
- 클라이언트가 연결된 경우 보안 정책 배포
- 관리자 지원 장치 복구
- 구성 요소 간 통신 시 신뢰할 수 있는 경로
- 고유한 암호화 키 생성 및 자동 보안 키 에스크로

Dell ProSupport에 문의

877-459-7304(내선번호 4310039)로 전화하면 연중무휴 하루 24시간 Dell 제품에 대한 전화 지원을 받을 수 있습니다.

또한, dell.com/support에서 Dell 제품에 대한 온라인 지원도 가능합니다. 온라인 지원에는 드라이버, 매뉴얼, 기술 자문, FAQ 및 최근에 나타나는 문제도 포함됩니다.

올바른 기술 전문가에게 신속히 연결될 수 있도록 전화할 때 서비스 태그 또는 익스프레스 서비스 코드를 준비하십시오.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

요구 사항 및 아키텍처

이 섹션은 Dell Security Management Server 구현에 관한 하드웨어 및 소프트웨어 요구 사항 및 아키텍처 디자인 권장사항에 대해 설명합니다.

Security Management Server 아키텍처 디자인

Encryption Enterprise 및 Endpoint Security Suite Enterprise 솔루션은 확장성이 뛰어난 제품으로서, 조직이 암호화할 엔드포인트 수를 기반으로 합니다.

아키텍처 구성요소

아래에 환경에 가장 적합한 하드웨어 구성이 제시되어 있습니다.

Security Management Server

- 운영 체제: Windows Server 2012 R2(Standard, Datacenter 64비트), Windows Server 2016(Standard, Datacenter 64비트), Windows Server 2019(Standard, Datacenter)
- 가상/실제 시스템
- CPU: 4개 코어
- RAM: 16.00GB
- 드라이브 C: 로그 및 애플리케이션 데이터베이스를 위한 30GB의 사용 가능한 디스크 공간

  노트: PostgreSQL 내에 저장된 로컬 이벤트 데이터베이스에 최대 10GB의 용량 사용.

프록시 서버

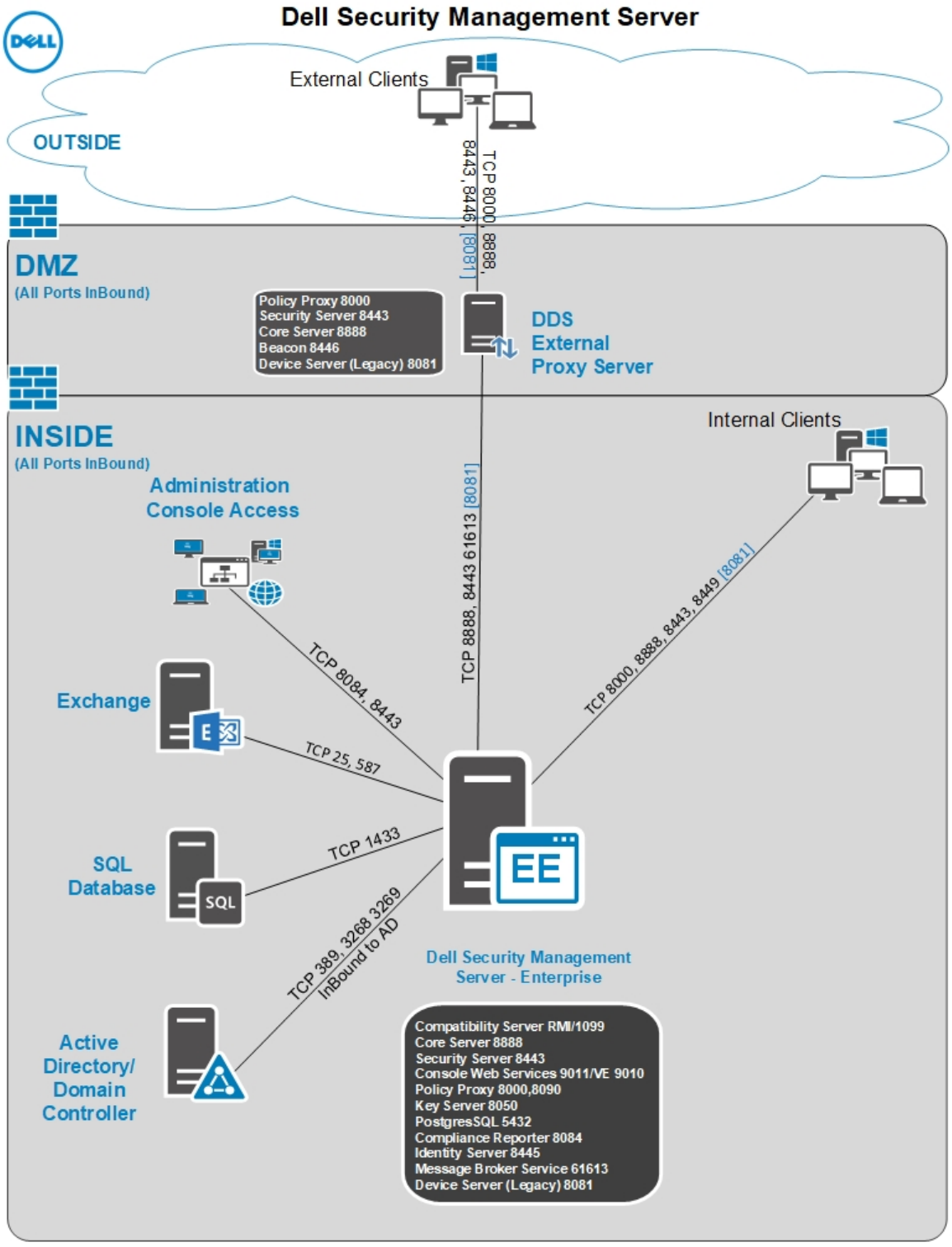
- 운영 체제: Windows Server 2012 R2(Standard, Datacenter 64비트), Windows Server 2016(Standard, Datacenter 64비트), Windows Server 2019(Standard, Datacenter)
- 가상/실제 시스템
- CPU: 2개 코어
- RAM: 8.00GB
- 드라이브 C: 로그를 위한 20GB의 사용 가능한 디스크 공간

SQL Server 하드웨어 사양

- CPU: 4개 코어
- RAM: 24.00GB
- 데이터 드라이브: 100~150GB의 사용 가능한 디스크 공간(환경에 따라 달라질 수 있음)
- 로그 드라이브: 50GB의 사용 가능한 디스크 공간(환경에 따라 달라질 수 있음)

  노트: 위의 정보가 대부분의 환경을 포함하지만 SQL Server 모범 사례를 따르는 것이 좋습니다.

아래는 Dell Security Management Server의 기본 배포입니다.



노트: 기업의 엔드포인트 수가 20,000개 이상일 경우에는 Dell ProSupport에 문의하십시오.

요구 사항

Security Management Server 소프트웨어 설치를 위한 하드웨어 및 소프트웨어 사전 요구 사항이 아래에 포함되어 있습니다.

설치를 시작하기 전에 설치에 사용되는 서버에 모든 패치와 업데이트가 적용되었는지 확인하십시오.

하드웨어

다음 표는 Security Management Server에 대한 *최소* 하드웨어 요구 사항을 자세히 설명합니다. 배포 크기에 따른 확장에 대한 추가 정보는 Security Management Server 아키텍처 디자인을 참조하십시오.

하드웨어 요구 사항
프로세서 Modern Quad-Core CPU(1.5GHz+)
RAM 16GB
사용 가능한 디스크 공간 20GB의 사용 가능한 디스크 공간 **노트:** PostgreSQL 내에 저장된 로컬 이벤트 데이터베이스에 최대 10GB의 용량 사용
네트워크 카드 10/100/1000 이상
기타 IPv4 또는 IPv6 또는 하이브리드 IPv4/IPv6 환경 필요

다음 표에는 Security Management Server 프런트엔드/프록시 서버의 *최소* 하드웨어 요구 사항이 자세히 나와 있습니다.

하드웨어 요구 사항
프로세서 최신 듀얼 코어 CPU
RAM 8GB
사용 가능한 디스크 공간 로그 파일을 위한 20GB의 사용 가능한 디스크 공간
네트워크 카드 10/100/1000 이상
기타 IPv4 또는 IPv6 또는 하이브리드 IPv4/IPv6 환경 필요

가상화

Security Management Server는 가상 환경에서 설치가 가능합니다. 다음과 같은 환경만 사용하는 것이 좋습니다.

Security Management Server v10.2.11은 다음과 같은 플랫폼에서 검증되었습니다.

Hyper-V Server는 전체 또는 코어 설치로 설치되었거나 Windows Server 2012, Windows Server 2016, Windows Server 2019에서 역할로 설치되었습니다.

- Hyper-V Server
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장

- 하드웨어가 최소 Hyper-V 요구 사항을 충족해야 함
- 전용 이미지 리소스를 위한 4GB 이상의 RAM
- 1세대 가상 시스템으로 실행되어야 함
- 자세한 내용은 https://technet.microsoft.com/en-us/library/hh923062.aspx를 참조하십시오.

Security Management Server v10.2.11은 VMware ESXi 6.0, VMware ESXi 6.5, VMware ESXi 6.5를 통해 검증되었습니다.

노트: VMware ESXi 및 Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019를 사용하는 경우 VMXNET3 이더넷 어댑터를 권장합니다.

- VMware ESXi 6.0
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-60/index.jsp를 참조하십시오.
- VMware ESXi 6.5
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php 참조
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-65/index.jsp를 참조하십시오.
- VMware ESXi 6.7
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php 참조
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-65/index.jsp를 참조하십시오.

노트: 성능상의 이유로 Security Management Server를 호스팅하는 SQL Server 데이터베이스는 별도의 컴퓨터에서 실행되어야 합니다.

SQL Server

대부분 환경에서 SQL Database 서버를 사용하면서 가용성 및 데이터 연속성을 보장하려면 SQL Cluster 같이 중복 시스템에서 실행하는 것이 가장 좋습니다. 또한 트랜잭션 로깅을 활성화하여 매일 전체 백업을 실행해야만 사용자/장치 활성화를 통해 새로 생성된 키를 복구할 수 있습니다.

데이터베이스를 유지 보수할 때는 데이터베이스 인덱스를 재작성하고 통계도 수집해야 합니다.

소프트웨어

다음 표에는 Security Management Server 및 프록시 서버의 소프트웨어 요구 사항이 자세히 나와 있습니다.

노트: Security Management Server에 보관된 민감한 데이터로 인해 Security Management Server를 전용 운영 체제에 설치해 최소 권한 규칙에 맞춰 조정하거나 환경을 안전하게 보호하도록 제한된 역할 및 권리가 있는 애플리케이션 서버에 포함할 것을 권장합니다. 이러한 권장 사항에는 권한이 있는 인프라스트럭처 서버에 Security Management Server를 설치하지 않는 내용을 포함합니다. 최소 권한 규칙 구현에 대한 자세한 내용은 https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models를 참조하십시오.

노트: UAC(Universal Account Control)가 보호된 디렉토리에 설치될 때 반드시 비활성화 상태여야 합니다. UAC를 비활성화한 후에는 서버를 재부팅해야 변경 사항이 적용됩니다.

노트: Policy Proxy의 레지스트리 위치(설치된 경우): HKLM\SOFTWARE\Wow6432Node\Dell

노트: Windows Server의 레지스트리 위치: HKLM\SOFTWARE\Dell

사전 요구 사항
• **Visual C++ 2010 재배포 가능 패키지** 설치되지 않은 경우 설치 프로그램이 자동으로 설치합니다. • **Visual C++ 2013 재배포 가능 패키지** 설치되지 않은 경우 설치 프로그램이 자동으로 설치합니다. • **Visual C++ 2015 재배포 가능 패키지** 설치되지 않은 경우 설치 프로그램이 자동으로 설치합니다. • **.NET Framework 버전 4.6.1** • **.NET Framework 버전 4.5** Microsoft는 .NET Framework 버전 4.6.1 및 4.5용 보안 업데이트를 게시했습니다. • **.NET Framework 버전 3.5 SP1** • **SQL Native Client 2012** SQL Server 2012 또는 SQL Server 2016을 사용하는 경우. 설치되지 않은 경우 설치 프로그램이 자동으로 설치합니다.

Security Management Server - 백엔드 서버 및 Dell 프런트엔드 서버
• **Windows Server 2012 R2** - Standard Edition - Datacenter Edition • **Windows Server 2016** - Standard Edition - Datacenter Edition • **Windows Server 2019** - Standard Edition - Datacenter Edition **노트:** 백엔드 구성 또는 프런트엔드 구성에 설치된 Dell의 Security Management Server는 현재 Windows Server 운영 체제의 운영 체제 업그레이드를 지원하지 않습니다.
LDAP 리포지토리
• Active Directory 2008 R2 • Active Directory 2012 R2 • Active Directory 2016 **노트:** Security Management Server은 Active Directory를 사용 중일 때 LDAP 채널 바인딩 및 LDAP 서명을 위한 Microsoft 요구 사항과 호환됩니다.
Management Console 및 Compliance Reporter
• Mozilla Firefox 41.x 이상 • Google Chrome 46.x 이상 • Microsoft Edge(Chromium)

- Microsoft Edge

  노트: 브라우저에서 쿠키를 허용해야 합니다.

Security Management Server 구성 요소를 위한 권장 가상 환경

Security Management Server는 가상 환경에서 설치가 가능합니다.

Dell은 현재 Amazon Web Services, Azure 등 다양한 기타 공급업체와 같은 클라우드 호스팅된 IaaS(Infrastructure as a Service) 환경 내에서 Dell Security Management Server 또는 Dell Security Management Server Virtual을 호스팅하는 작업을 지원합니다. 이러한 환경을 위한 지원은 Security Management Server의 기능에만 한정됩니다. 이러한 가상 머신의 관리 및 보안은 IaaS 솔루션 관리자의 책임입니다.

추가 인프라 요구 사항. Active Directory 및 SQL Server와 같은 추가 인프라 요구 사항이 여전히 올바른 기능에 필요합니다.

노트: Security Management Server를 호스팅하는 SQL Server 데이터베이스는 별도의 컴퓨터에서 실행되어야 합니다.

데이터베이스

- **SQL Server 2012 -** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2014 -** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2016 -** Standard Edition/Enterprise Edition
- **SQL Server 2017 -** Standard Edition/Enterprise Edition
- **SQL Server 2019 -** Standard Edition/Enterprise Edition

노트: Express Edition은 제품 환경에 지원되지 않습니다. Express Edition은 POC 및 평가용으로만 사용할 수 있습니다.

SQL Server 버전에 따라 Security Management Server에 다음 중 하나를 활성화**해야** 합니다.

- 전체 텍스트 인덱싱
- 전체 텍스트 필터
- 검색을 위한 전체 테스트 및 의미 추출

사용 중인 SQL Server에 대해 위의 기능이 활성화되어 있지 않을 때 발생하는 오류에 대한 자세한 내용은 KB 문서 SLN308557을 참조하십시오.

Security Management Server에 대한 Microsoft SQL Server 사용 권한 및 기능을 구성하는 방법에 대한 자세한 내용은 이 KB 문서 SLN307771을 참조하십시오.

노트: 아래는 SQL 권한의 요구 사항입니다. 설치 및 서비스를 수행하는 사용자는 로컬 관리자 권한이 있어야 합니다. 또한 Dell Security Management Server의 서비스를 관리하는 서비스 계정에 대해 로컬 관리자 권한이 필요합니다.

유형	작업	시나리오	SQL 권한 필요
백엔드	업그레이드	기본적으로 업그레이드에 DB 및 로그인/사용자가 이미 설정됨	db_owner
백엔드	복원 설치	복원에는 기존 DB 및 로그인이 관련되어 있습니다.	db_owner
백엔드	새 설치	기존 DB 사용	db_owner
백엔드	새 설치	새 DB 생성	dbcreator, db_owner
백엔드	새 설치	기존 로그인 사용	db_owner
백엔드	새 설치	새 로그인 생성	securityadmin
백엔드	삭제	해당 없음	해당 없음
프록시 프런트엔드	모든	해당 없음	해당 없음

노트: 사용자 계정 컨트롤(UAC)이 활성화된 경우 `C:\Program Files`에 설치할 때 Windows Server 2012 R2에 설치하기 전에 비활성화해야 합니다. 서버를 재부팅해야만 변경 사항이 적용됩니다.

설치하는 동안 데이터베이스를 설정하려면 Windows 또는 SQL 인증 자격 증명이 필요합니다. 사용되는 자격 증명의 유형에 관계 없이, 계정에 수행 중인 작업에 대한 적절한 권한이 있어야 합니다. 이전 표에 각 유형의 설치에 필요한 권한이 설명되어 있습니다. 또한, 데이터베이스를 생성하고 설정하는 데 사용되는 계정에는 dbo로 설정된 기본 스키마가 있어야 합니다.

이러한 권한은 데이터베이스를 설정하기 위해 설치 동안에만 필요합니다. Security Management Server가 설치되고 나면 SQL 액세스를 관리하기 위해 사용되는 계정은 db_owner 및 public 역할에 제한될 수 있습니다.

액세스 권한이나 데이터베이스와의 연결에 대해 잘 모르는 경우에는 설치를 시작하기 전에 데이터베이스 관리자에게 문의하여 확인하시기 바랍니다.

Management Console을 위한 언어 지원

Management Console은 MUI(Multilingual User Interface)와 호환되며 다음 언어를 지원합니다.

언어 지원	
EN - 영어	JA - 일본어
ES - 스페인어	KO - 한국어
FR - 프랑스어	PT-BR - 포르투갈어, 브라질
IT - 이탈리아어	PT-PT - 포르투갈어, 포르투갈(이베리아)
DE - 독일어	

3

설치 전 구성

시작하기 전에 Security Management Server와 관련된 모든 최신 해결 방법이나 알려진 문제를 확인하려면 *Security Management Server 기술 권장 사항*을 읽으십시오.

Security Management Server를 설치하고자 할 경우 서버의 사전 설치 구성이 매우 중요합니다. 이 섹션을 특히 주목해서 Security Management Server를 원활하게 설치하십시오.

구성

Management Console 액세스

Internet Explorer가 더 이상 지원되지 않으므로 Management Console에 올바르게 액세스하려면 타사 브라우저를 설치해야 합니다.

Management Console의 유효성을 검사하는 데 Internet Explorer가 필요한 경우 로그인한 관리자에 해당하는 계정 유형에 대해 Internet Explorer 보안 구성 강화를 비활성화해야 합니다.

포트 및 방화벽 구성

공용 서버 및 클라이언트 통신(아웃바운드)

Dell Server가 관리되는 엔드포인트와 통신하려면 아래 서비스 및 포트가 필요합니다. 이러한 포트 및 서비스는 아웃바운드 통신을 지원해야 합니다. SSL 검사 및 프록시 서비스를 사용 중인 경우 URL에서 제외해야 합니다.

- 온 더 박스 소유 권한 검증
  - 대상 URL
    - cloud.dell.com
  - 포트
    - 443
  - 아웃바운드 디바이스
    - 백엔드 구성의 Security Management Server 또는 Security Management Server Virtual
  - 원래 서비스
    - Dell 보안 서버
  - 원래 포트
    - 8443
- Advanced Threat Prevention 클라이언트 통신
  - 대상 URL
    - 북미
      - login.cylance.com
      - protect.cylance.com
      - data.cylance.com
      - update.cylance.com
      - api.cylance.com
      - protect-api.cylance.com
      - download.cylance.com
    - 남미
      - login-sae1.cylance.com
      - protect-sae1.cylance.com
      - data-sae1.cylance.com
      - update-sae1.cylance.com
      - api-sae1.cylance.com
      - protect-api-sae1.cylance.com

        - download-sae1.cylance.com
    - 유럽
        - login-euc1.cylance.com
        - protect-euc1.cylance.com
        - data-euc1.cylance.com
        - update-euc1.cylance.com
        - api-euc1.cylance.com
        - protect-api-euc1.cylance.com
        - download-euc1.cylance.com
    - 중동 및 아시아
        - login-au.cylance.com
        - protect-au.cylance.com
        - data-au.cylance.com
        - update-au.cylance.com
        - api-au.cylance.com
        - protect-api-au.cylance.com
        - download-au.cylance.com
    - 일본, 호주 및 뉴질랜드
        - login-apne1.cylance.com
        - protect-apne1.cylance.com
        - data-apne1.cylance.com
        - update-apne1.cylance.com
        - api-apne1.cylance.com
        - protect-api-apne1.cylance.com
        - download-apne1.cylance.com
- 포트
    - 443
- 아웃바운드 디바이스
    - 관리되는 모든 엔드포인트
- 아웃바운드 서비스
    - CylanceSVC
- 원래 포트
    - 443

공용 프런트엔드 서버 통신(필요한 경우)

인터넷에서 프런트엔드 서버로 정보가 이동하는 것을 볼 수 있습니다. 방화벽 또는 라우팅 구성에는 공용 또는 인터넷 연결에서 하나 이상의 프런트엔드 서버 또는 로드 밸런서로 인바운드로 설정된 포트가 있어야 합니다.

- Dell Core Server Proxy: HTTPS/8888
- Dell Device Server: HTTPS/8081
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443

DMZ 또는 프런트엔드와 백엔드 서버 통신(필요한 경우)

아래 서비스 및 포트는 프런트엔드 모드로 구성된 Security Management Server에서 백엔드 모드로 구성된 Security Management Server로 통신합니다. 방화벽 또는 라우팅 구성에는 하나 이상의 프런트엔드 서버 또는 로드 밸런서에서 백엔드 서버로 인바운드로 설정된 포트가 있어야 합니다.

- 프런트엔드 Dell Policy Proxy 및 Dell Beacon Server - 백엔드 Dell Message Broker: STOMP/61613
- 프런트엔드 Dell Security Server Proxy - 백엔드 Dell Security Server: HTTPS/8443
- 프런트엔드 Dell Core Server Proxy - 백엔드 Dell Core Server: HTTPS/8888
- 프런트엔드 Dell Device Server - 백엔드 Dell Security Server: HTTPS/8443

백엔드 서버 - 내부 네트워크

아래 서비스 및 포트는 도메인 또는 VPN을 통해 연결된 클라이언트가 내부적으로 해당 서비스와 통신하는 데 사용됩니다. Dell Technologies에서는 이러한 서비스 중 몇 가지를 네트워크 외부로 전달하지 않거나 프런트엔드 서버의 구성에서 서비스를 기본적으로 필터링할 것을 권장합니다. 방화벽 또는 라우팅 구성에는 이러한 포트가 내부 네트워크에서 백엔드 Security Management Server로 인바운드로 설정되어야 합니다.

- Dell Security Server에 호스팅된 Management Console: HTTPS/8443
- Dell Compliance Reporter를 통해 전달된 보고서: HTTP(S)/8084

  노트: 이 서비스는 기본적으로 비활성화되어 있습니다. 대신 Dell Security Server에서 호스팅하는 Management Console에서 사용할 수 있는 관리 보고서를 사용합니다. 내역 보고를 위해 Dell Compliance Reporter를 활성화하는 것에 대한 자세한 내용은 KB 문서 SLN314792를 참조하십시오.
- Dell Core Server: HTTPS/8888
- Dell Device Server: HTTP(S)/8081

  노트: 이 기존 서비스는 8.x 이전 Dell Encryption 클라이언트에만 필요합니다. 환경 내의 모든 클라이언트가 8.0 이상인 경우 이 서비스를 안전하게 비활성화할 수 있습니다.
- Key Server: TCP/8050
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443
- 인증서 기반 인증, Dell Security Server를 통해 호스팅됨: HTTPS/8449

  노트: Windows Server 운영 체제에 설치된 Dell Encryption 클라이언트 또는 서버 모드로 설치된 클라이언트는 이 기능을 사용합니다. 이 서버 모드에서 클라이언트를 설치하는 방법에 대한 자세한 내용은 Encryption Enterprise 고급 설치 가이드를 참조하십시오.

인프라 통신

- Active Directory, Dell Encryption TCP/389/636(로컬 도메인 컨트롤러)에서 사용자 인증에 활용, TCP/3268/3269(글로벌 카탈로그), TCP/135/49125+(RPC)
- 이메일 통신(선택 사항): 25/587
- Microsoft SQL Server: 1433(기본 포트)

Microsoft SQL 데이터베이스 생성 및 관리

Dell Server 데이터베이스 생성:

이 지침은 선택적입니다. 데이터베이스가 없는 경우 설치 프로그램은 기본적으로 데이터베이스를 만듭니다. Security Management Server를 설치하기 전에 데이터베이스를 설정하고 싶은 경우 아래의 지침에 따라 SQL Management Studio에서 SQL 데이터베이스와 SQL 사용자를 생성합니다. Security Management Server를 설치하는 동안 자동으로 생성되지 않는 SQL 데이터베이스에 대해 적절한 사용 권한이 설정되어 있는지 확인합니다. 필요한 권한 목록을 보려면 소프트웨어 요구 사항을 참조하십시오.

데이터베이스를 사전에 생성하는 경우 기존 데이터베이스와 함께 백엔드 서버 설치의 지침을 따릅니다.

Security Management Server는 SQL 및 Windows 인증용으로 구성되어 있습니다.

노트: SQL 데이터베이스 또는 SQL 인스턴스를 위해 지원되는 예상된 비기본 데이터 정렬은 "SQL_Latin1_General_CP1_CI_AS" 데이터 정렬입니다. 데이터 정렬은 대/소문자를 구분하고 액센트 문자를 인식해야 합니다.

설치 필수 요소

필수 구성 요소는 Windows Server 운영 체제에서 Security Management Server를 설치하는 동안 기본으로 설치됩니다. 재부팅 요구 사항을 무시하려면 Security Management Server를 설치하기 전에 아래 필수 구성 요소를 선택적으로 설치하면 됩니다.

Visual C++ 재배포 가능 패키지 설치

아직 설치하지 않은 경우 Visual C++ 2010, 2013 및 2015(이상) 재배포 가능 패키지를 설치합니다. 또는 Security Management Server 설치 프로그램이 이 구성 요소를 설치하게 할 수 있습니다.

노트: Microsoft Visual C++ 재배포 가능 패키지를 설치하려면 재부팅해야 할 수 있습니다.

Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019 - https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads

.NET Framework 4.5 설치

.NET Framework 4.5는 Windows Server 2012 R2 이상에서 서버 관리자의 기능으로 사전 설치되어 있습니다.

SQL Native Client 2012 설치

SQL Server 2012 또는 SQL Server 2016을 사용하는 경우 SQL Native Client 2012를 설치합니다. 또는 Security Management Server 설치 프로그램이 이 구성 요소를 설치하게 할 수 있습니다. http://www.microsoft.com/en-us/download/details.aspx?id=35580

서버 설치 라이선스 가져오기

신규 설치의 경우 – 사용자의 제품 키(파일 이름: *EnterpriseServerInstallKey.ini*)를 `C:\Windows`에 복사하면 32자로 구성된 Product Key가 Security Management Server 설치 프로그램에 자동으로 입력됩니다.

노트: EnterpriseServerInstallKey.ini는 Security Management Server의 다운로드 패키지에 있으며 여기에서 확인할 수 있습니다.

서버의 사전 설치 구성이 완료되었습니다. 계속해서 설치 또는 업그레이드/마이그레이션합니다.

4

설치 또는 업그레이드/마이그레이션

이 장에서는 다음과 같은 작업을 위한 지침을 제공합니다.

- 새 설치 - Security Management Server를 새로 설치합니다.
- 업그레이드/마이그레이션 - 작동 중인 기존의 Enterprise Server v9.2 이상에서 업그레이드합니다.
- Security Management Server 제거 - 필요한 경우 현재 설치를 제거합니다.

  서버 설치에 기본 서버(백엔드)를 둘 이상 포함해야 하는 경우에는 Dell ProSupport에게 문의하십시오.

설치 또는 업그레이드/마이그레이션을 시작하기 전에

시작하기 전에 해당하는 설치 전 구성 단계를 수행해야 합니다.

Security Management Server 설치와 관련된 모든 최신 해결 방법이나 알려진 문제는 *Security Management Server 기술 권고사항*을 읽어 보십시오.

Microsoft C++ 런타임 설치 프로그램, Java 활동(인증서 생성 및 조작), PostgreSQL 생성 및 수정에 영향을 미치지 않도록 Security Management Server를 설치 또는 업그레이드하는 동안 바이러스 백신 및 맬웨어 방지를 비활성화해야 합니다. 이러한 모든 항목은 실행 파일 또는 스크립트에 의해 트리거됩니다.

해결 방법으로 다음을 제외합니다.

- [설치 경로]:\Dell\Enterprise Edition
- C:\Windows\Installer
- 설치 프로그램이 실행된 파일 경로입니다.

Dell Server 데이터베이스에 데이터베이스 모범 사례를 사용하고 조직의 재해 복구 계획에 Dell 소프트웨어를 포함시킬 것을 권장합니다.

DMZ에 Dell 구성요소를 배포하려면, 구성요소가 공격으로부터 적절히 보호를 받을 수 있는지 확인해야 합니다.

프로덕션 환경의 경우, SQL Server를 전용 서버에 설치할 것을 강력히 권장합니다.

프론트 엔드 서버를 설치 및 구성하기 전 백엔드 서버를 설치하는 것이 좋습니다.

설치 로그 파일은 다음 디렉토리에 있습니다.`C:\Users\<LoggedOnUser>\AppData\Local\Temp`

신규 설치

백엔드 서버를 설치할 때 다음 두 옵션 중 하나를 선택하십시오.

- 백엔드 서버 및 새 데이터베이스 설치 - 새 Security Management Server와 새 데이터베이스를 설치합니다.
- 기존 데이터베이스와 함께 백엔드 서버 설치 - 스키마 버전이 설치할 Security Management Server 버전과 일치하는 경우 Security Management Server를 새로 설치하고 사전 설치 구성 도중에 생성된 SQL 데이터베이스에 연결하거나 v9.x 이상인 기존 SQL 데이터베이스에 연결할 수 있습니다. v9.2 이상의 데이터베이스는 최신 버전의 Server 구성 도구를 사용하여 최신 스키마로 마이그레이션해야 합니다. Server 구성 도구로 데이터베이스 마이그레이션의 지침을 보려면 데이터베이스 마이그레이션을 참조하십시오. 최신 Server 구성 도구를 가져오거나 v9.2 이전의 데이터베이스를 마이그레이션하려면 Dell ProSupport에 문의하십시오.

노트:

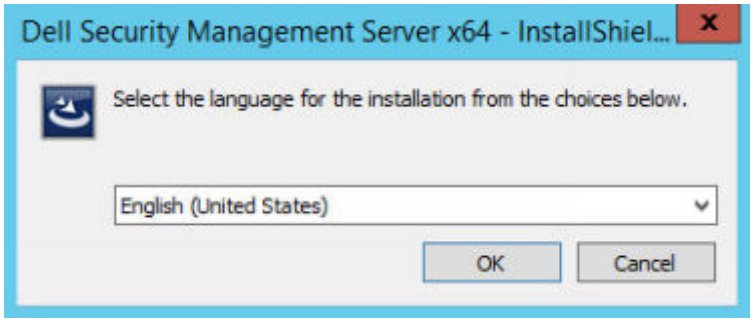
Enterprise Server v9.2 이상을 사용하고 있는 경우 **백엔드 서버 업그레이드/마이그레이션**의 지침을 참조하십시오.

프론트 엔드 서버를 설치하는 경우에는 백엔드 서버를 설치한 후에 이 설치를 수행하십시오.

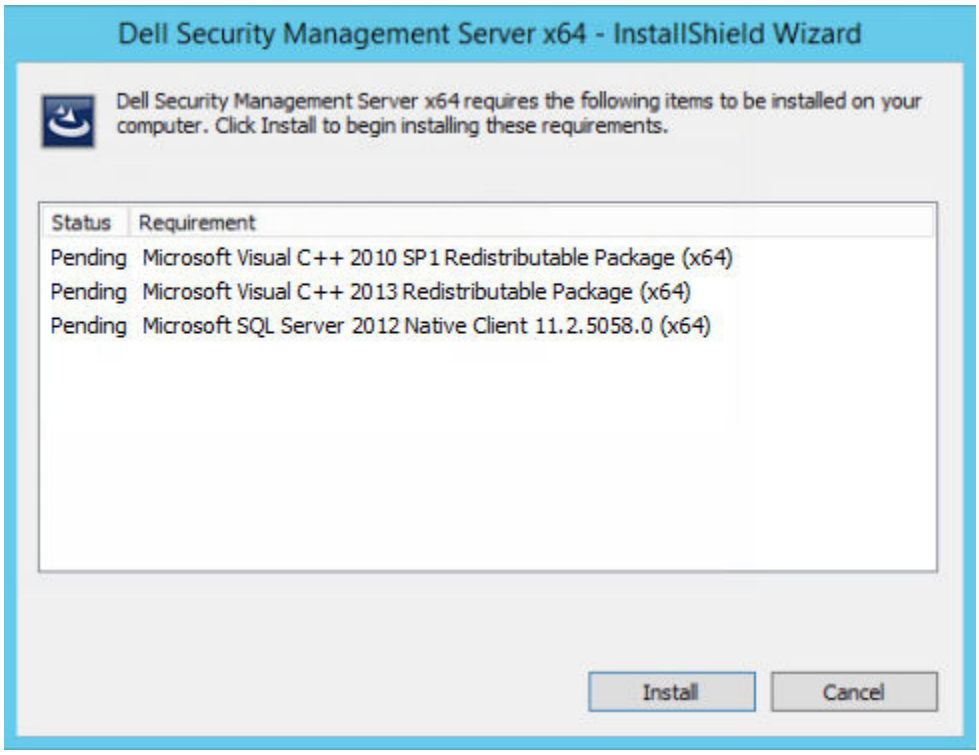
- 프론트 엔드 서버 설치 - 백엔드 서버와 통신할 프론트 엔드 서버를 설치합니다.

백엔드 서버 및 새 데이터베이스 설치

1. Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server에 설치할 서버의 루트 디렉토리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. 설치할 언어를 선택하고 **확인**을 클릭합니다.

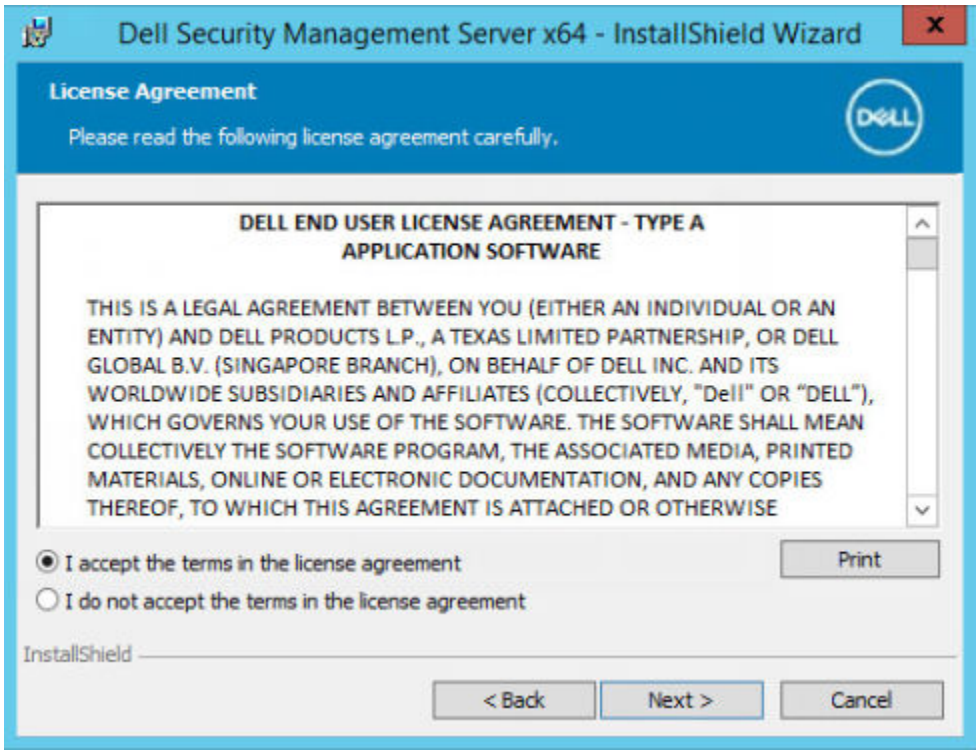


4. 사전 요구 사항이 아직 설치되어 있지 않으면, 사전 요구 사항이 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.

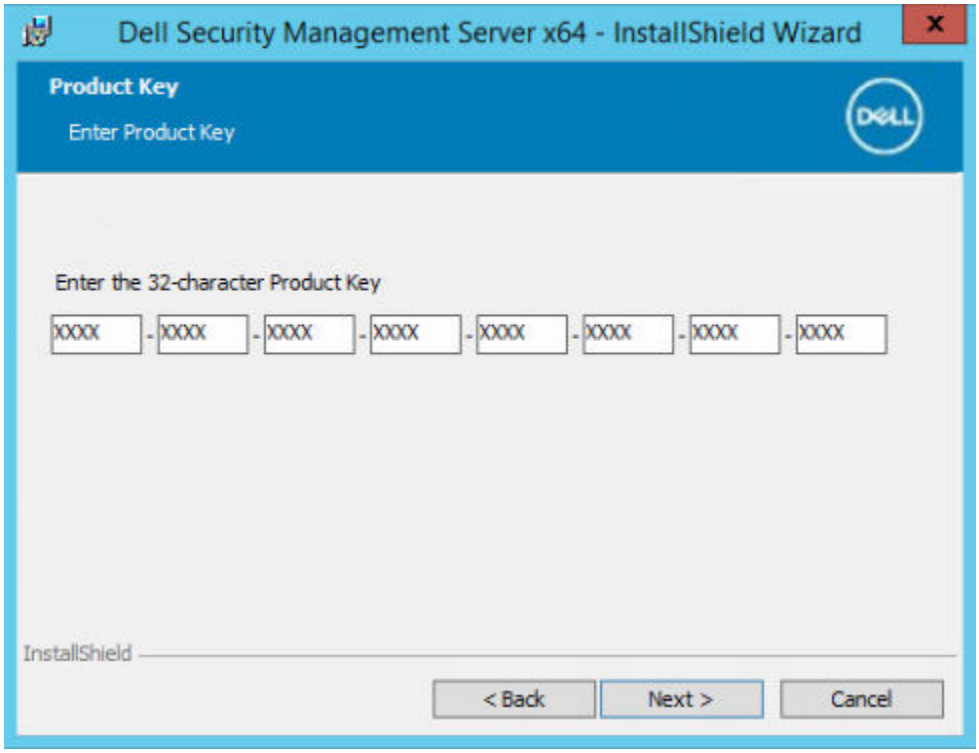


5. *시작* 대화상자에서 **다음**을 클릭합니다.

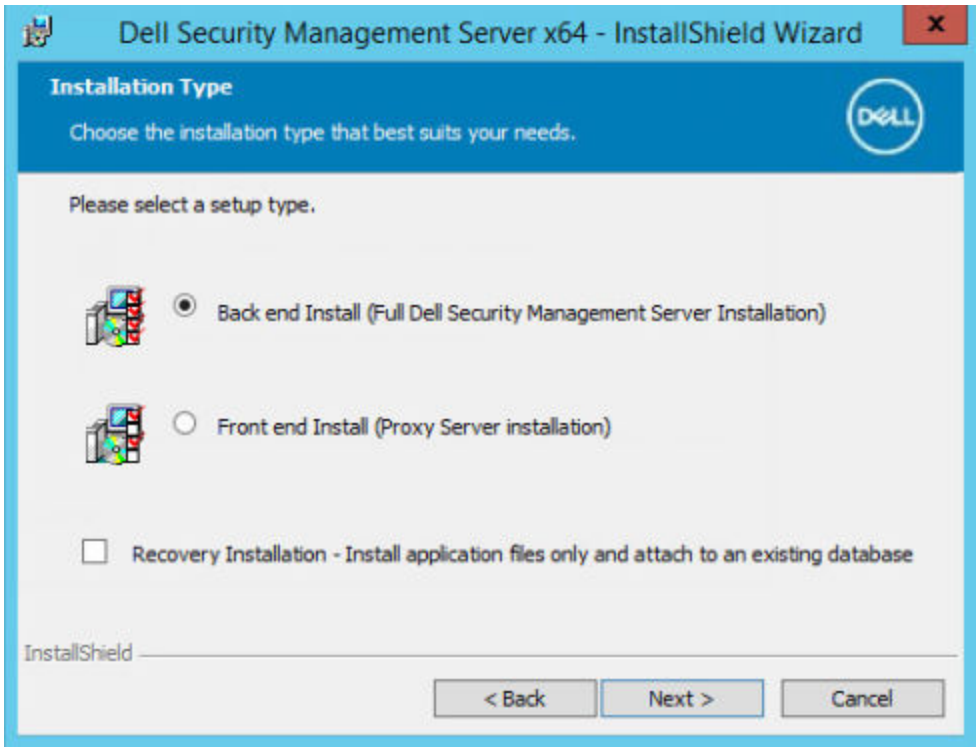
6. 라이센스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.



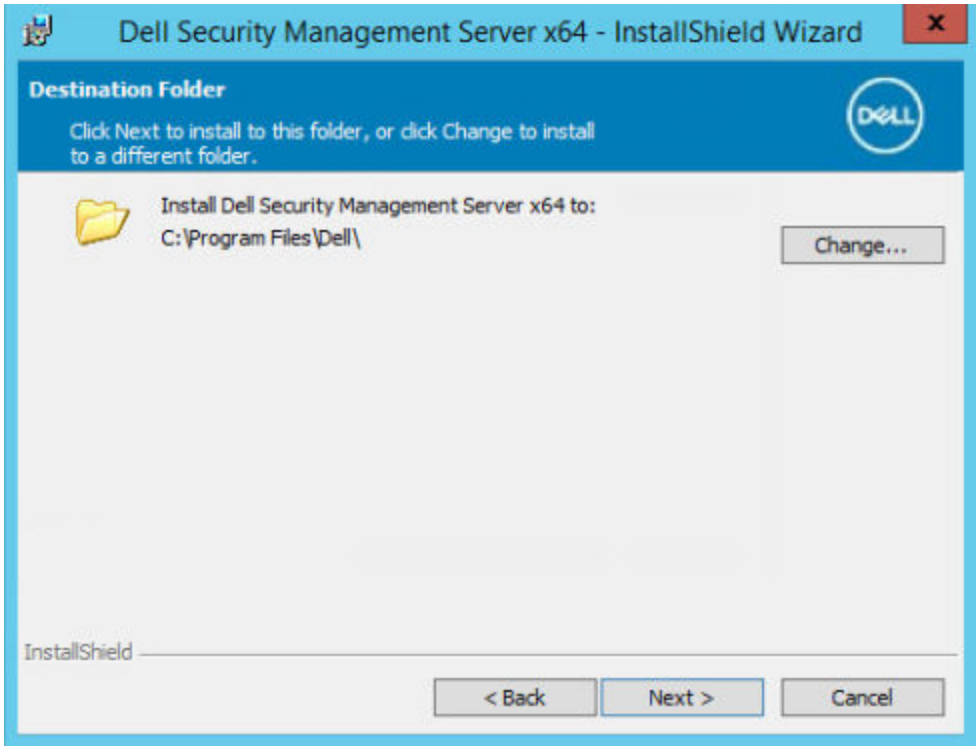
7. 선택 사항으로 사전 설치 구성의 설명에 따라 `EnterpriseServerInstallKey.ini` 파일을 `C:\Windows`에 복사한 경우 **다음**을 클릭합니다. 32자리 제품 키를 입력한 후 **다음**을 클릭합니다. 제품 키는 "`EnterpriseServerInstallKey.ini` 파일에 있습니다.



8. **백엔드 설치**를 선택하고 **다음**을 클릭합니다.

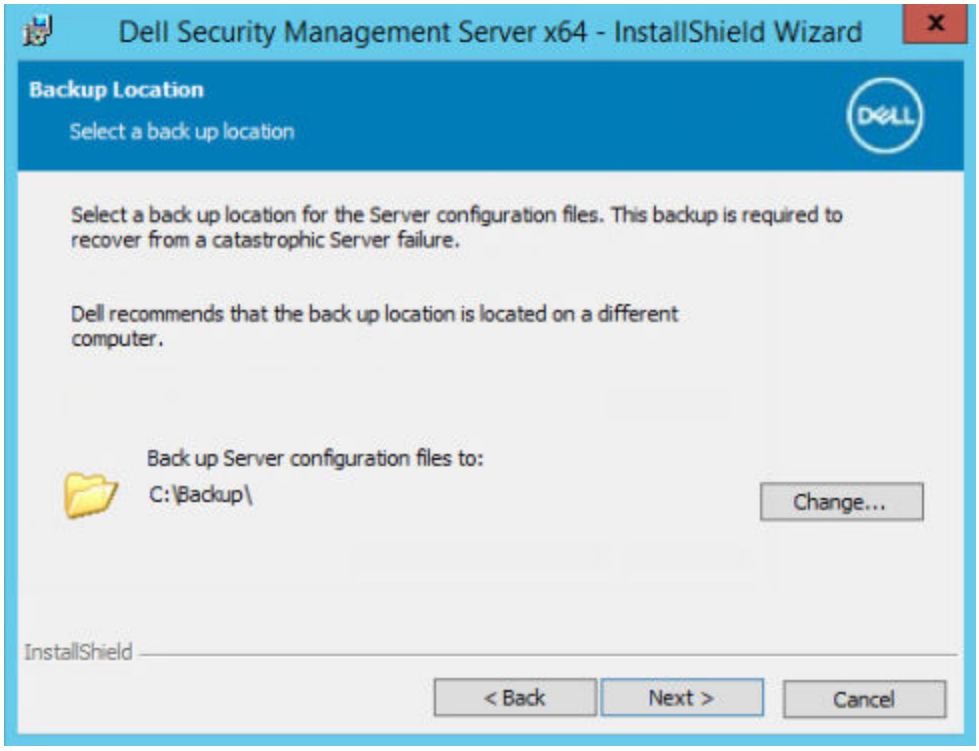


9. Security Management Server를 기본 위치인 `C:\Program Files\Dell`에 설치하려면 **다음**을 클릭합니다. 그렇지 않은 경우, **변경**을 클릭하여 다른 위치를 선택한 후 **다음**을 클릭합니다.



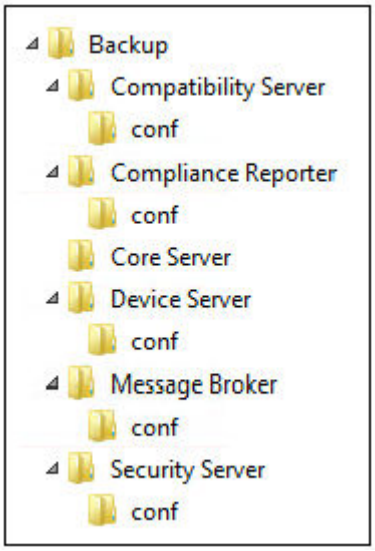
10. 백업 구성 파일을 저장할 위치를 선택하려면, **변경**을 클릭하여 원하는 폴더로 이동하고 **다음**을 클릭합니다.

    원격 네트워크 위치 또는 외부 드라이브를 백업 위치로 선택하는 것이 좋습니다.



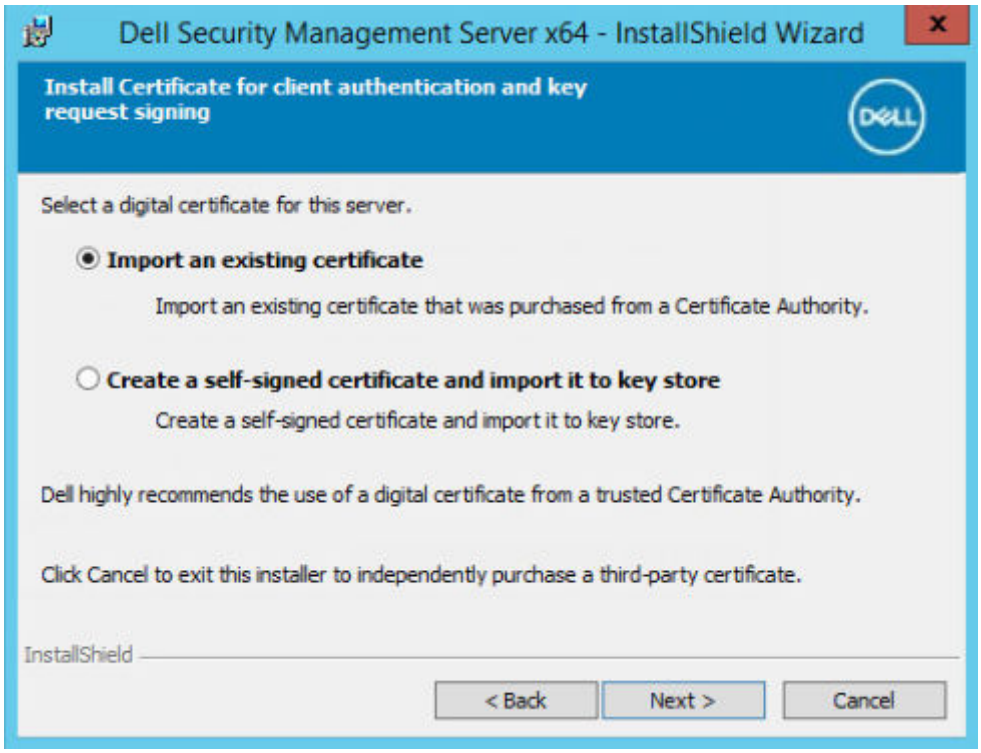
설치를 마친 후, 모든 구성 파일에 대한 변경 사항(Server 구성 도구를 통한 변경 사항 포함)은 Backup 폴더에 수동으로 저장해야 합니다. 구성 파일은 필요한 경우 수동으로 Dell Server를 복원하는 데 필요한 전체 정보에서 중요한 역할을 합니다.

노트: 이 설치 단계 중에는 설치 프로그램에서 생성된 폴더 구조(아래 예제 참조)를 그대로 유지해야 합니다.



11. 사용할 디지털 인증서 유형을 선택할 수 있습니다. **신뢰할 수 있는 인증 기관의 디지털 인증서를 사용할 것을 권장합니다.** 아래에서 옵션 "a" 또는 "b"를 선택하십시오.

    a. CA 기관에서 구입한 기존 인증서를 사용하려면 **기존 인증서 가져오기**를 선택하고 **다음**을 클릭합니다.



    찾아보기를 클릭하여 인증서 경로를 입력합니다.

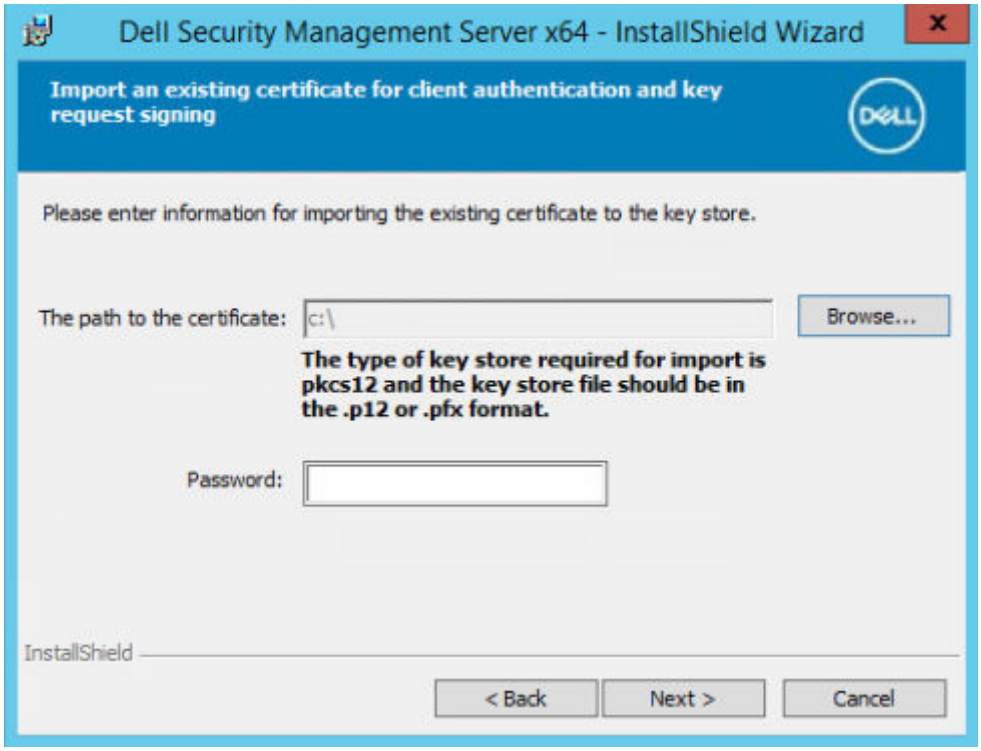
    이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 Certificate Management Console을 사용하여 PFX에 인증서 내보내기를 참조하십시오.

    다음을 클릭합니다.

    노트:

    이 설정을 사용하려면, 내보내진 CA 인증서 중 가져올 CA 인증서에 최대의 신뢰 체인이 수립되어 있어야 합니다. 확실하지 않을 경우, CA 인증서를 다시 내보내고 "인증서 내보내기 마법사"에서 다음 옵션이 선택되었는지 확인하십시오.

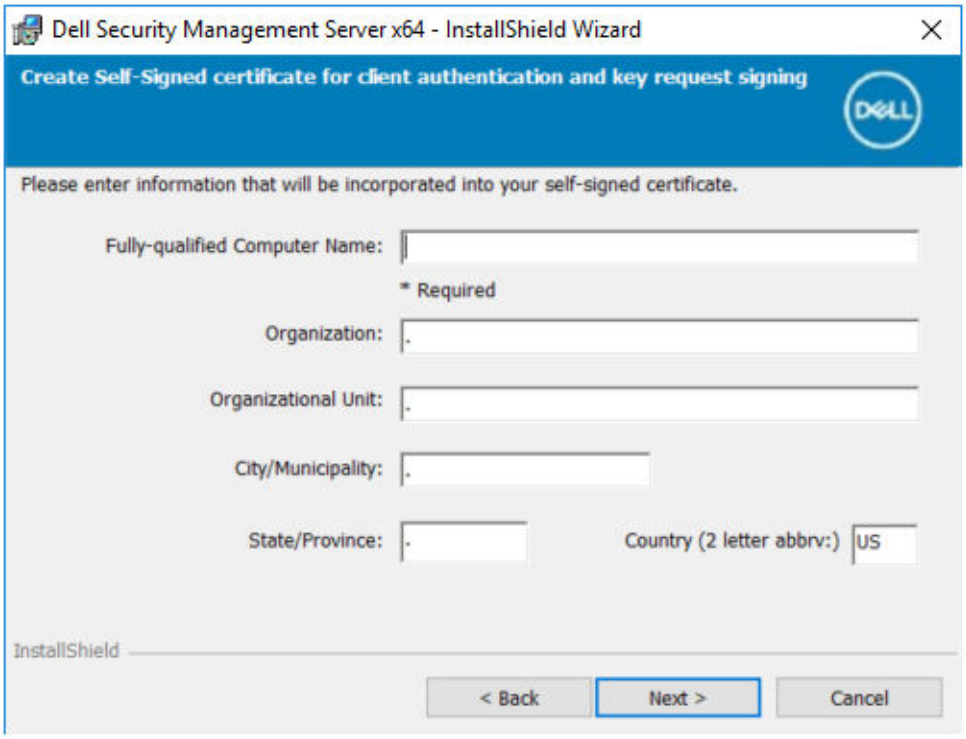
    - 개인 정보 교환 - PKCS#12(.PFX)
    - 가능한 한 모든 인증서를 인증서 경로에 포함
    - 모든 확장 속성을 내보냄



또는

b. 자체 서명된 인증서를 만들려면 **자체 서명된 인증서를 생성하여 키 스토리지에 가져오기**를 선택하고 **다음**을 클릭합니다.
자체 서명 인증 대화상자에 다음 정보를 입력합니다.
정규화된 컴퓨터 이름(예: computername.domain.com)
조직
조직 단위(예: 보안 팀)
시
도(전체 이름)
국가: 알파벳 두 글자로 된 국가 약어
다음을 클릭합니다.

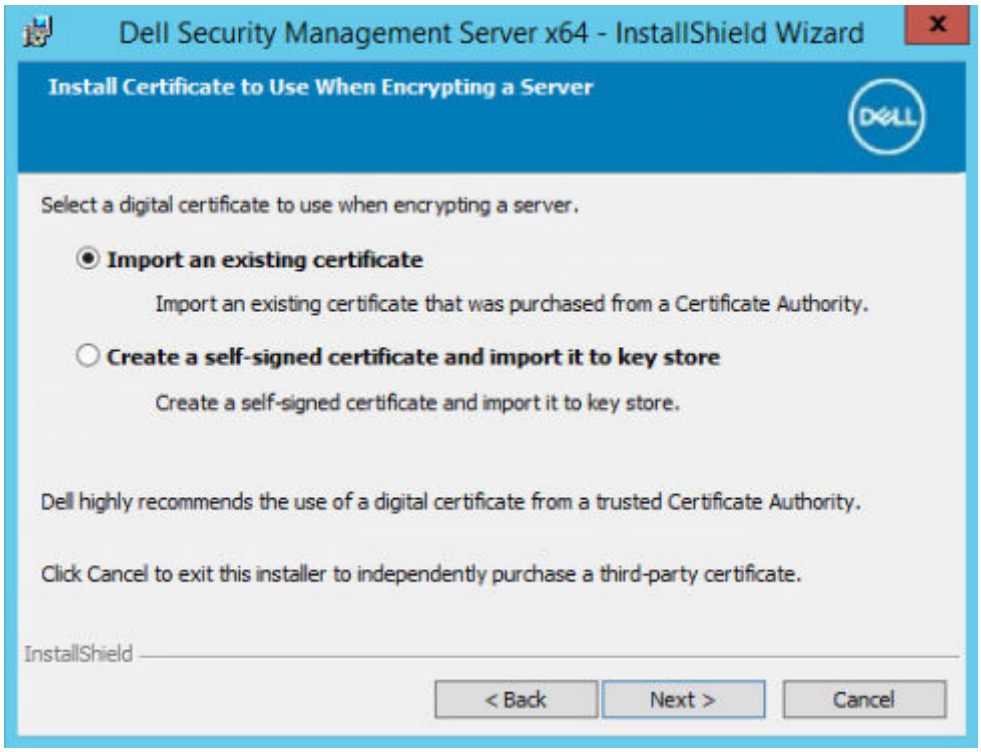
노트: 기본적으로 인증서 유효 기간은 10년입니다.



12. Server Encryption에서, 사용할 디지털 인증서 유형을 선택할 수 있습니다. 신뢰할 수 있는 인증 기관의 디지털 인증서를 사용할 것을 권장합니다.

    아래에서 옵션 "a" 또는 "b"를 선택하십시오.

    a. CA 기관에서 구입한 기존 인증서를 사용하려면 **기존 인증서 가져오기**를 선택하고 **다음**을 클릭합니다.



    찾아보기를 클릭하여 인증서 경로를 입력합니다.

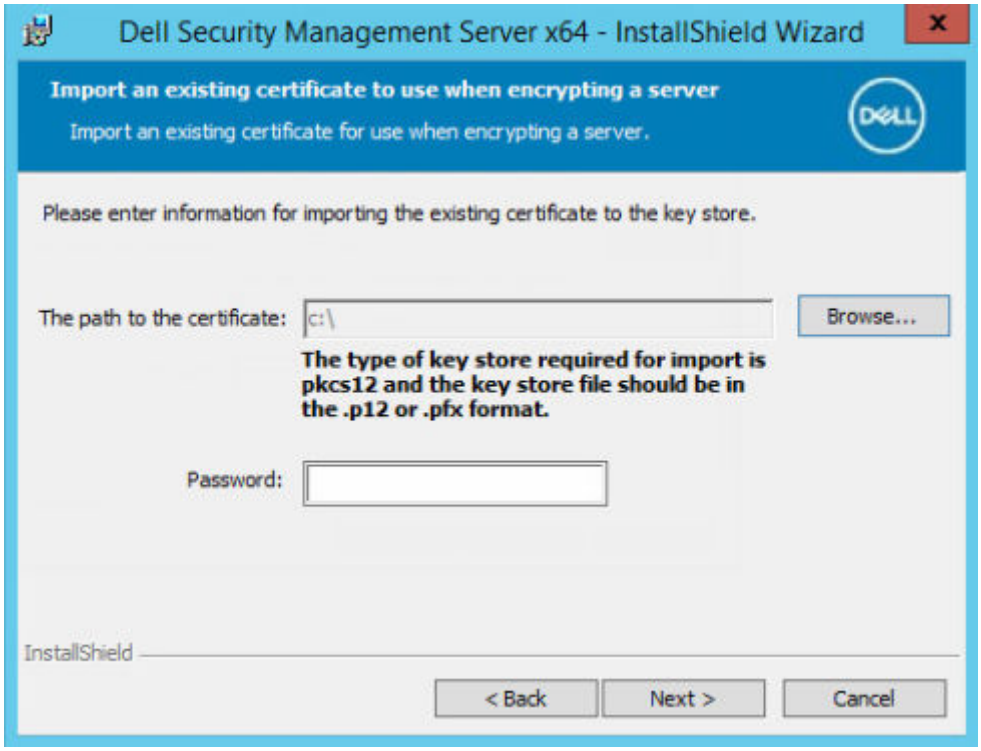
    이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 Certificate Management Console을 사용하여 PFX에 인증서 내보내기를 참조하십시오.

    다음을 클릭합니다.

노트:

이 설정을 사용하려면, 내보내진 CA 인증서 중 가져올 CA 인증서에 최대의 신뢰 체인이 수립되어 있어야 합니다. 확실하지 않을 경우, CA 인증서를 다시 내보내고 "인증서 내보내기 마법사"에서 다음 옵션이 선택되었는지 확인하십시오.

- 개인 정보 교환 - PKCS#12(.PFX)
- 가능한 한 모든 인증서를 인증서 경로에 포함
- 모든 확장 속성을 내보냄



또는

b. 자체 서명된 인증서를 만들려면 **자체 서명된 인증서를 생성하여 키 스토리지에 가져오기를 선택하고 다음을 클릭합니다.**

자체 서명 인증 대화상자에 다음 정보를 입력합니다.

정규화된 컴퓨터 이름(예: computername.domain.com)

조직

조직 단위(예: 보안 팀)

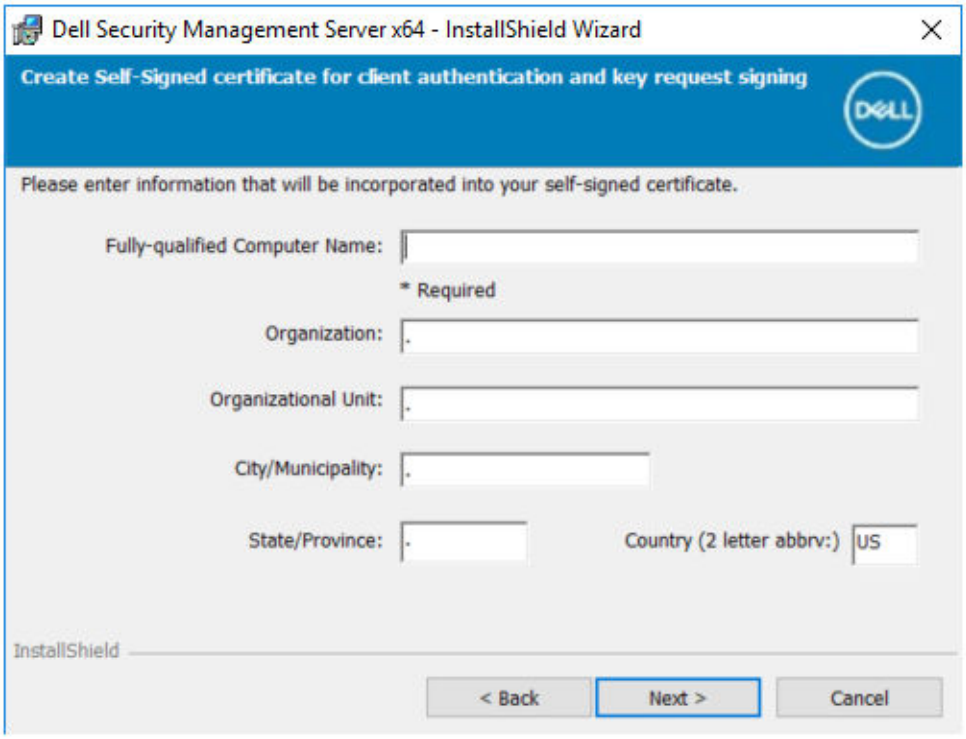
시

도(전체 이름)

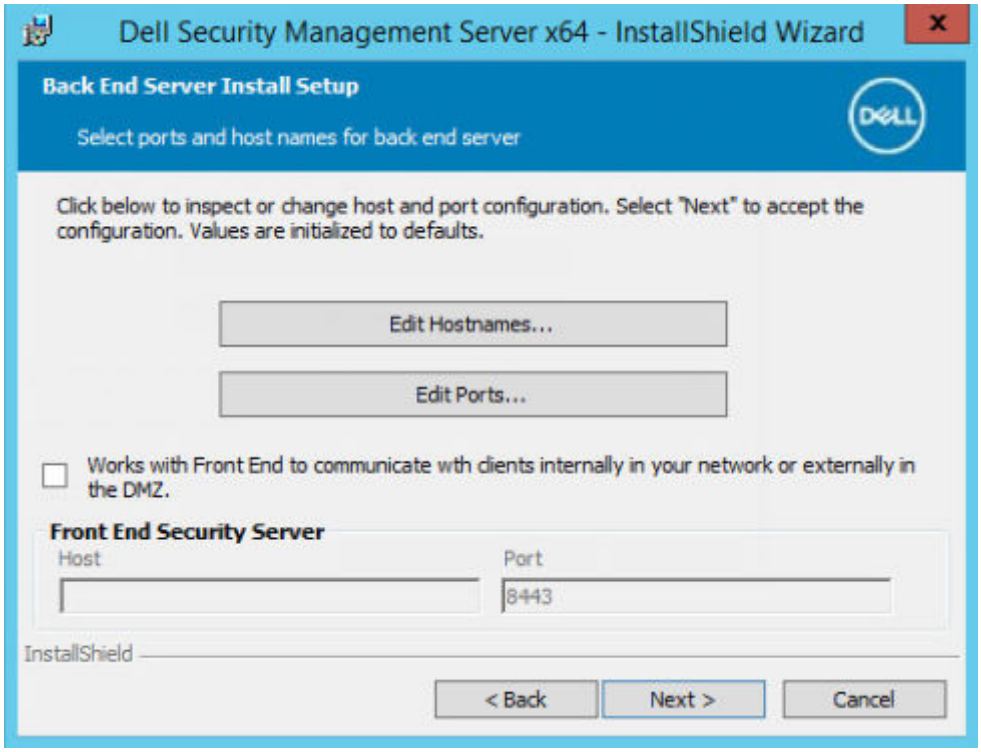
국가: 알파벳 두 글자로 된 국가 약어

다음을 클릭합니다.

노트: 기본적으로 인증서 유효 기간은 10년입니다.



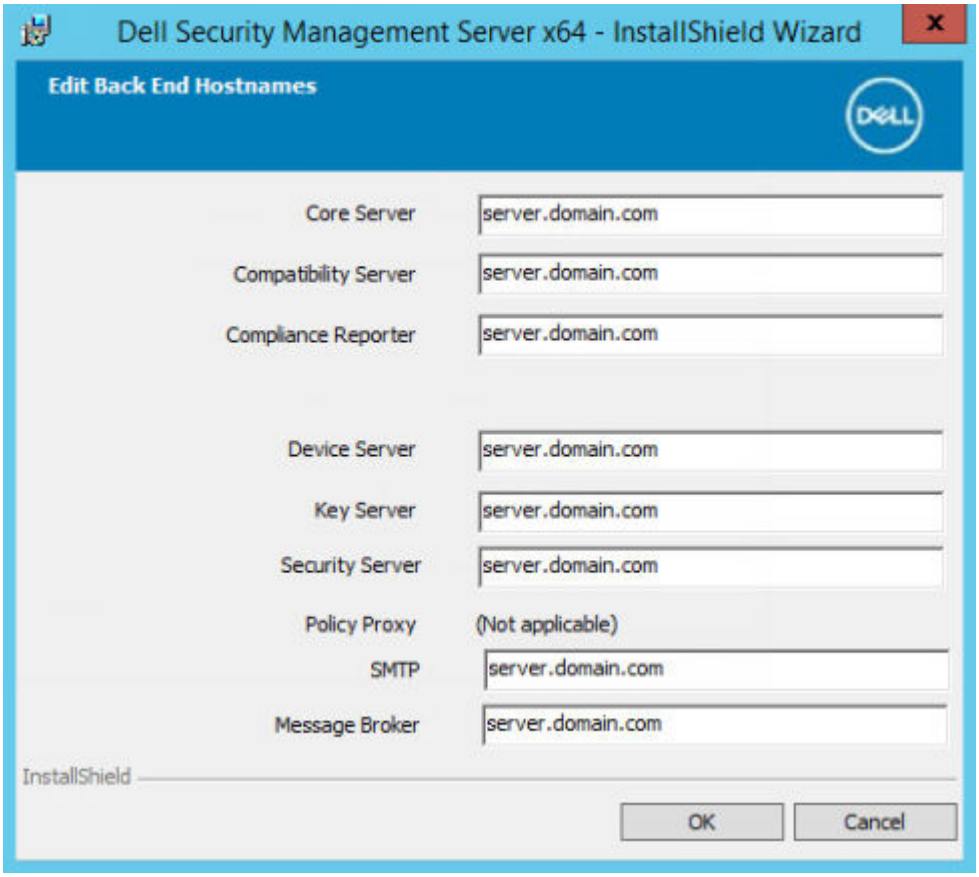
13. *백엔드 서버 설치 설정* 대화상자에서 호스트 이름 및 포트를 보거나 편집할 수 있습니다.
    - 기본 호스트 이름 및 포트를 수락하려면 *백엔드 서버 설치 설정* 대화상자에서 **다음**을 클릭합니다.
    - 프론트 엔드 서버를 사용하는 경우 **네트워크 내부 또는 DMZ 외부로 클라이언트와 통신하도록 프론트 엔드 작동**을 선택하고 프론트 엔드 보안 서버 호스트 이름(예: server.domain.com)을 입력합니다.



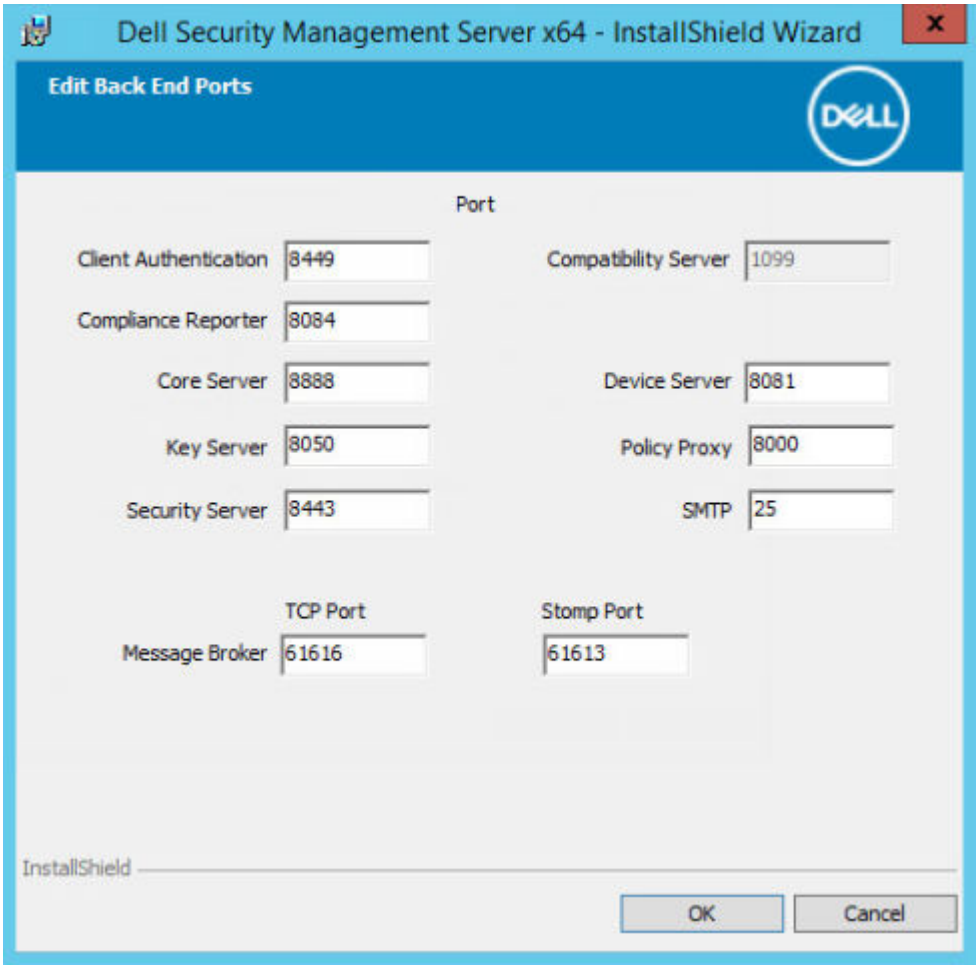
    - 호스트 이름을 보거나 편집하려면 **호스트 이름 편집**을 클릭합니다. 필요한 경우에만 호스트 이름을 편집합니다. 기본값 사용을 권장합니다.

      노트: 호스트 이름에는 밑줄("_")을 사용할 수 없습니다.

      작업을 마친 후 **확인**을 클릭합니다.

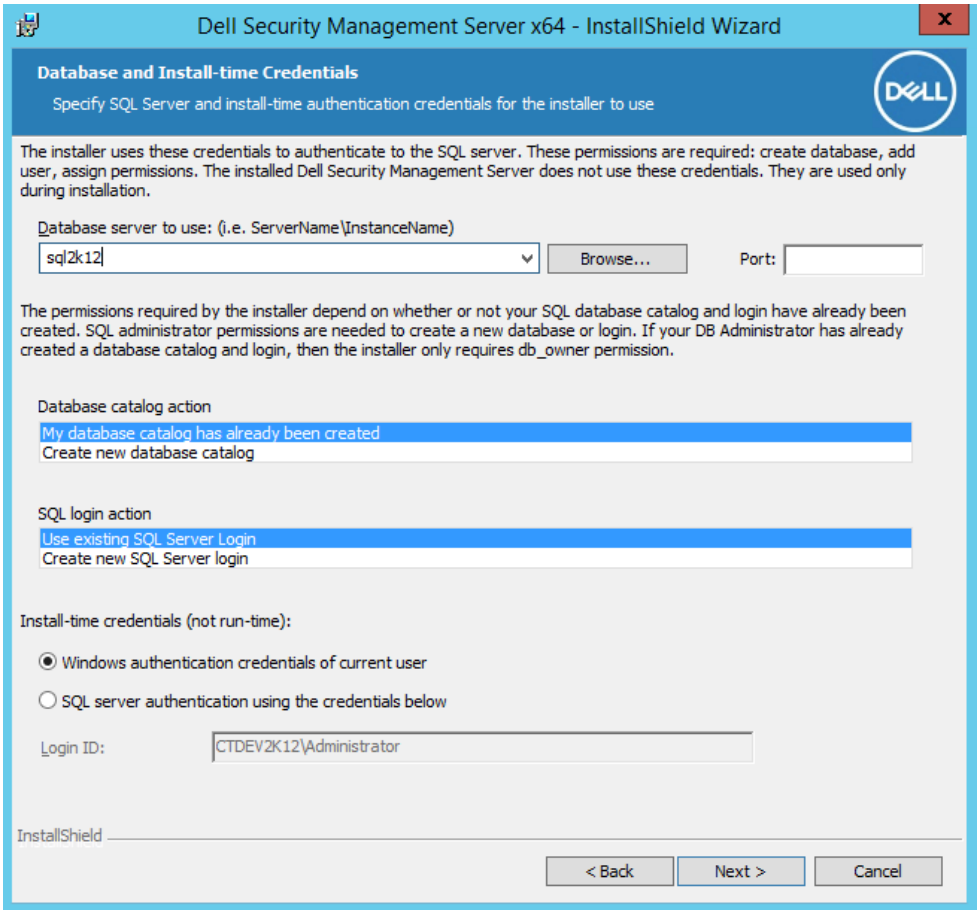


- 포트를 보거나 편집하려면 **포트 편집**을 클릭합니다. 필요한 경우에만 포트를 편집합니다. 기본값 사용을 권장합니다. 작업을 마친 후 **확인**을 클릭합니다.



14. 새 데이터베이스를 생성하려면 다음 단계를 수행하십시오.
    a. **찾아보기**를 클릭하여 데이터베이스를 설치할 서버를 선택합니다.
    b. Dell Server 데이터베이스를 설치하려면 사용할 설치 프로그램에 대한 인증 방법을 선택합니다. 설치한 이후, 설치된 제품은 여기에 특정된 자격 증명을 사용하지 않습니다.
        - **현재 사용자의 Windows 인증 자격 증명**

          Windows 인증을 선택하면 Windows에 로그인하는 데 사용한 자격 증명이 인증에 사용됩니다(*사용자 이름* 및 *암호*는 수정할 수 없음). 해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다.



또는

- **다음 자격 증명을 사용해 SQL 서버 인증**

  SQL 인증을 사용하려면 사용되는 SQL 계정에 SQL 서버에 대한 시스템 관리자 권한이 있어야 합니다.

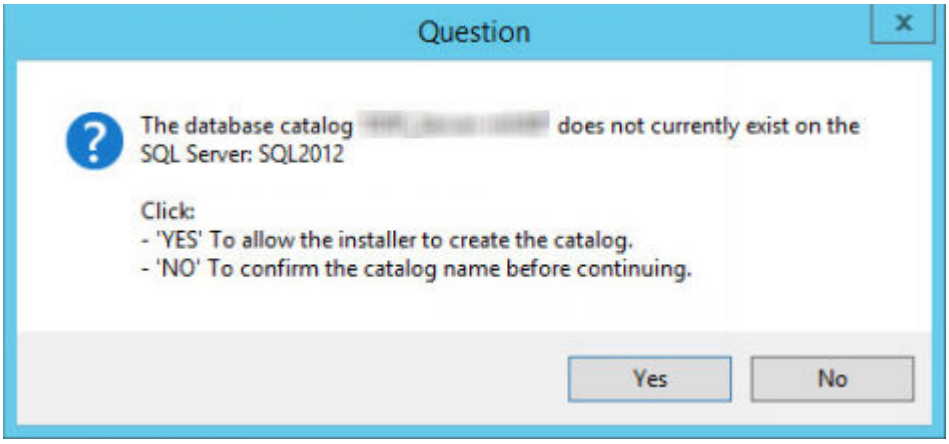
  설치 프로그램은 이 허가를 통해 SQL 서버에 인증해야 합니다: 데이터베이스 생성, 사용자 추가, 허용 할당.

c. 데이터베이스 카탈로그를 식별합니다.

   새 데이터베이스 카탈로그의 이름을 입력합니다. 새 카탈로그를 생성하라는 메시지가 다음 대화상자에 표시됩니다.

d. **다음**을 클릭합니다.

e. 설치 프로그램에서 데이터베이스를 만들도록 하려면 **예**를 클릭합니다. 이전 화면으로 돌아가 변경을 수행하려면 **아니오**를 클릭합니다.



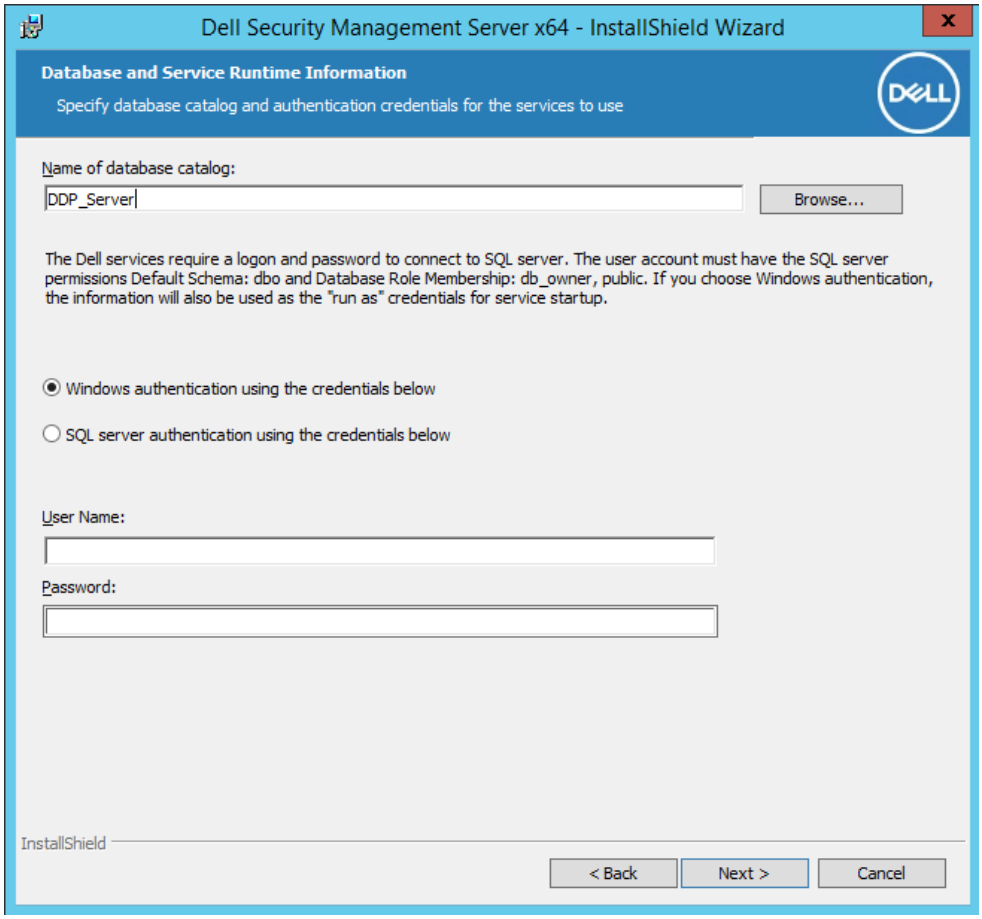
15. 사용할 제품에 대해 인증 방법을 선택합니다. 이 단계는 제품에 계정을 연결합니다.

- **Windows 인증**

아래의 자격 증명을 사용해 Windows 인증을 선택하고 **다음**을 클릭합니다.

해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.

또한 이 자격 증명은 Security Management Server에서 작업할 때 Dell 서비스에서 사용됩니다.

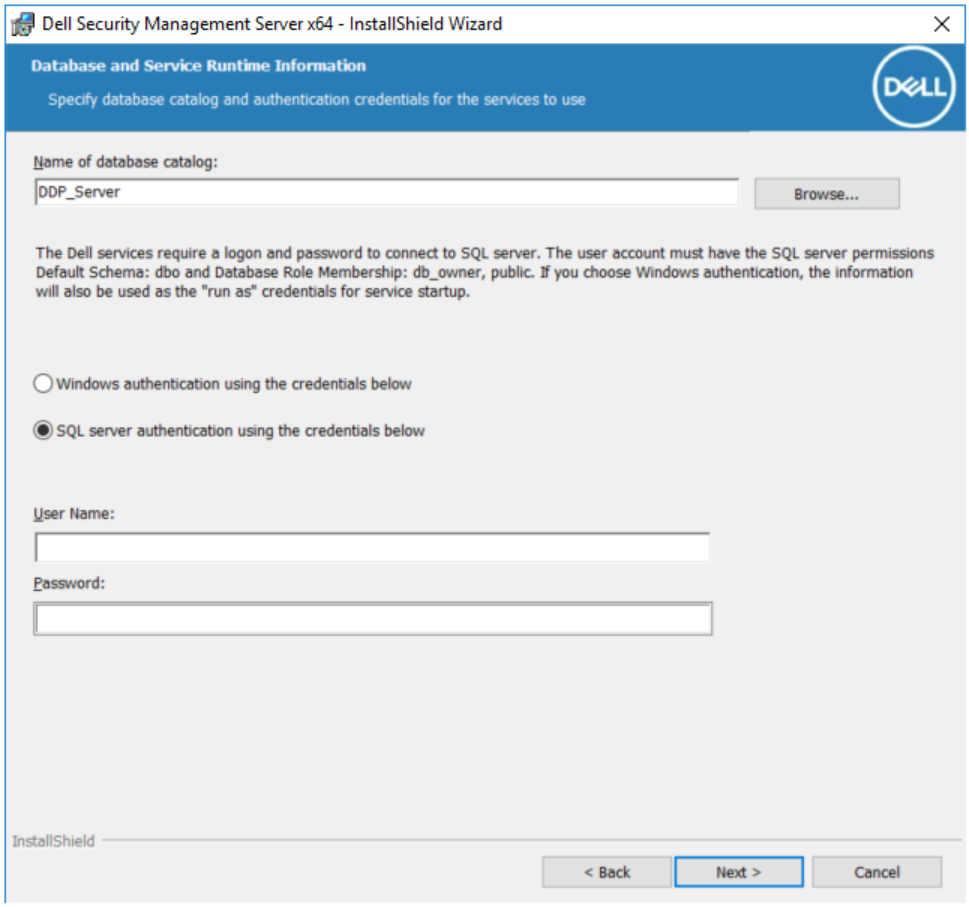


또는

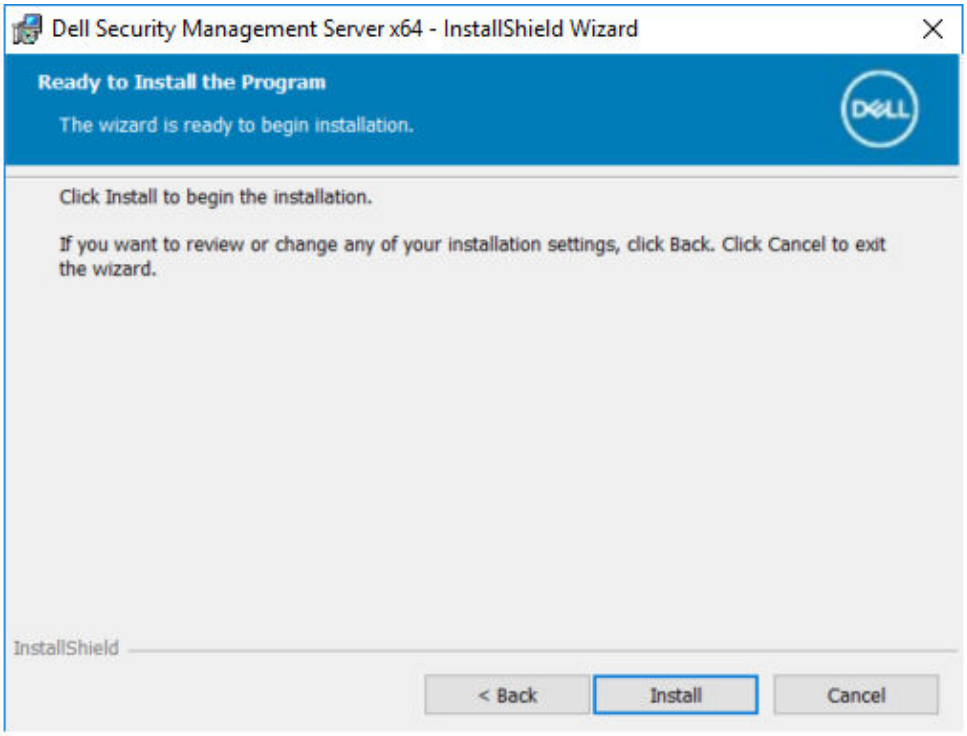
- **SQL 서버 인증**

  아래의 자격 증명을 사용해 SQL 서버 인증을 선택하고 Security Management Server에서 작업할 때 사용할 Dell 서비스에 대한 SQL 서버 자격 증명을 입력하고 **다음**을 클릭합니다.

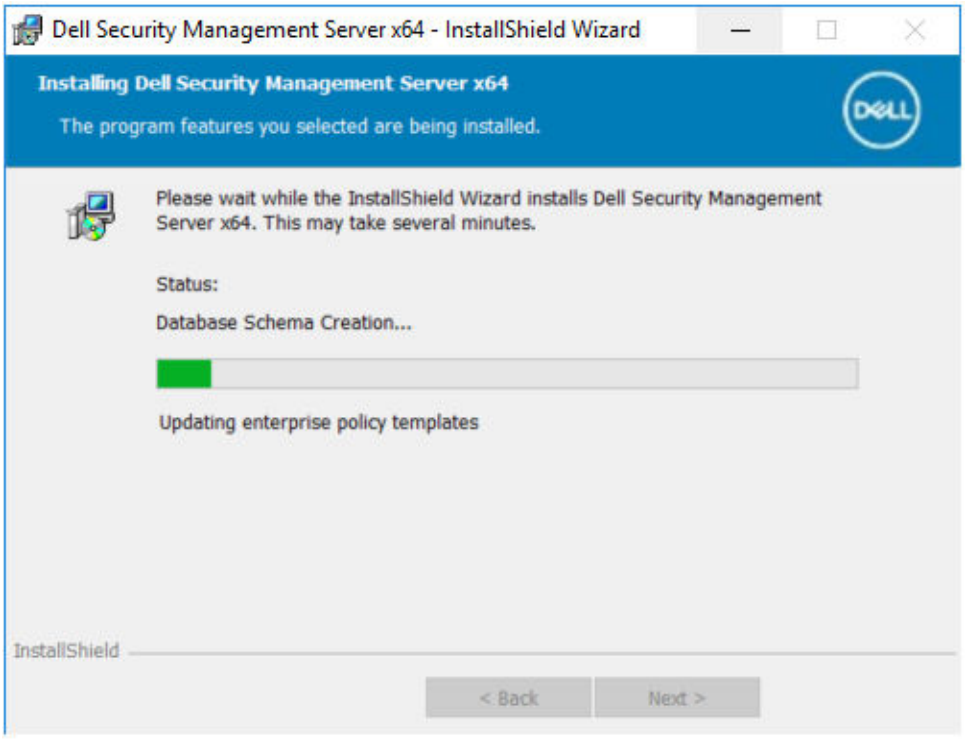
  사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.



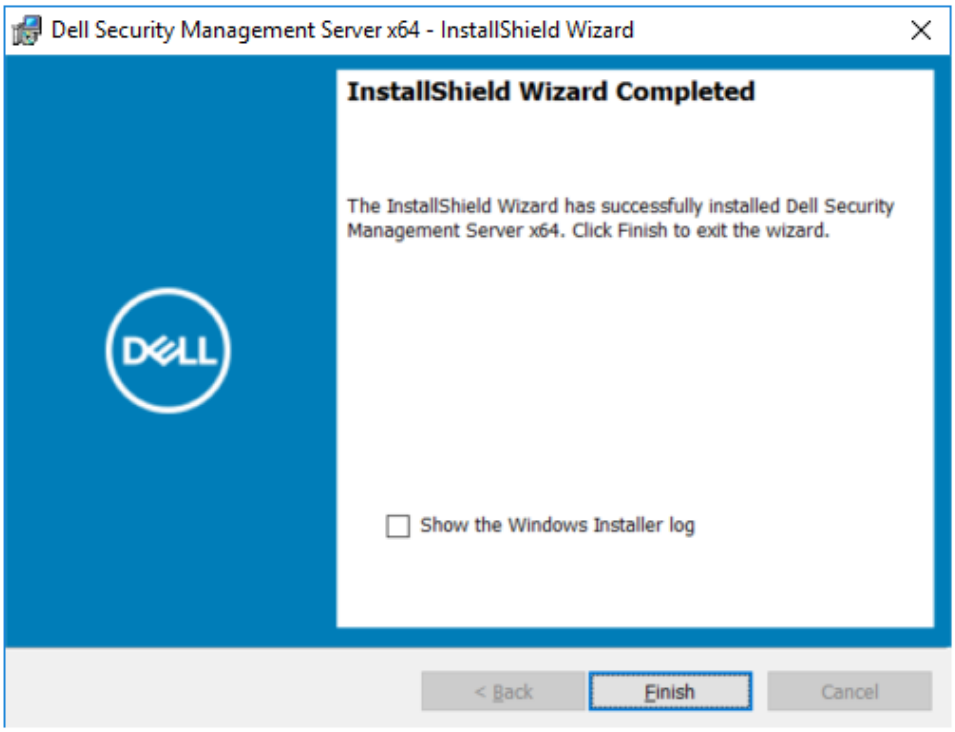
16. *프로그램 설치 준비 완료* 대화상자에서 **설치**를 클릭합니다



진행률 대화상자에 설치 과정 상태가 표시됩니다.



17. 설치가 완료되면 **마침**을 클릭합니다.



백엔드 서버 설치 작업이 완료됩니다.

설치가 끝나면 Dell 서비스가 다시 시작됩니다. Dell Server를 다시 부팅할 필요는 없습니다.

기존 데이터베이스와 함께 백엔드 서버 설치

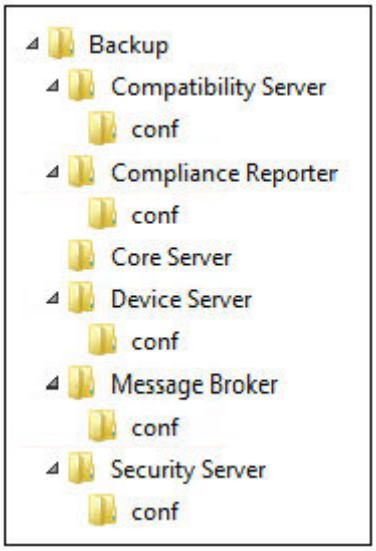
노트:

Dell Server v9.2 이상을 사용하고 있는 경우 백엔드 서버 업그레이드/마이그레이션의 지침을 참조하십시오.

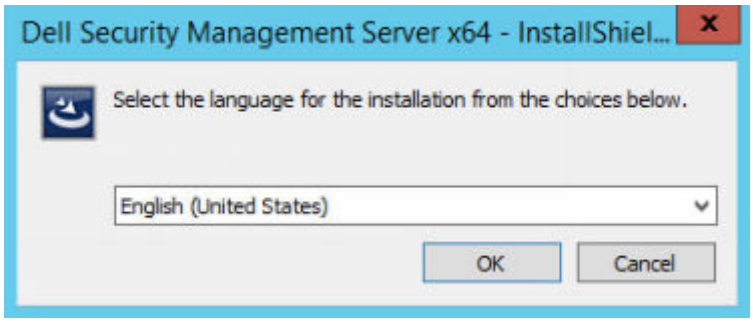
스키마 버전이 설치할 Security Management Server 버전과 일치하는 경우 Security Management Server를 새로 설치하고 사전 설치 구성 도중에 생성된 SQL 데이터베이스에 연결하거나 v9.x 이상인 기존 SQL 데이터베이스에 연결할 수 있습니다.

설치가 수행되는 사용자 계정에는 SQL 데이터베이스에 대해 데이터베이스 소유자 권한이 있어야 합니다. 액세스 권한이나 데이터베이스와의 연결에 대해 잘 모르는 경우에는 설치를 시작하기 전에 데이터베이스 관리자에게 문의하여 확인하시기 바랍니다.

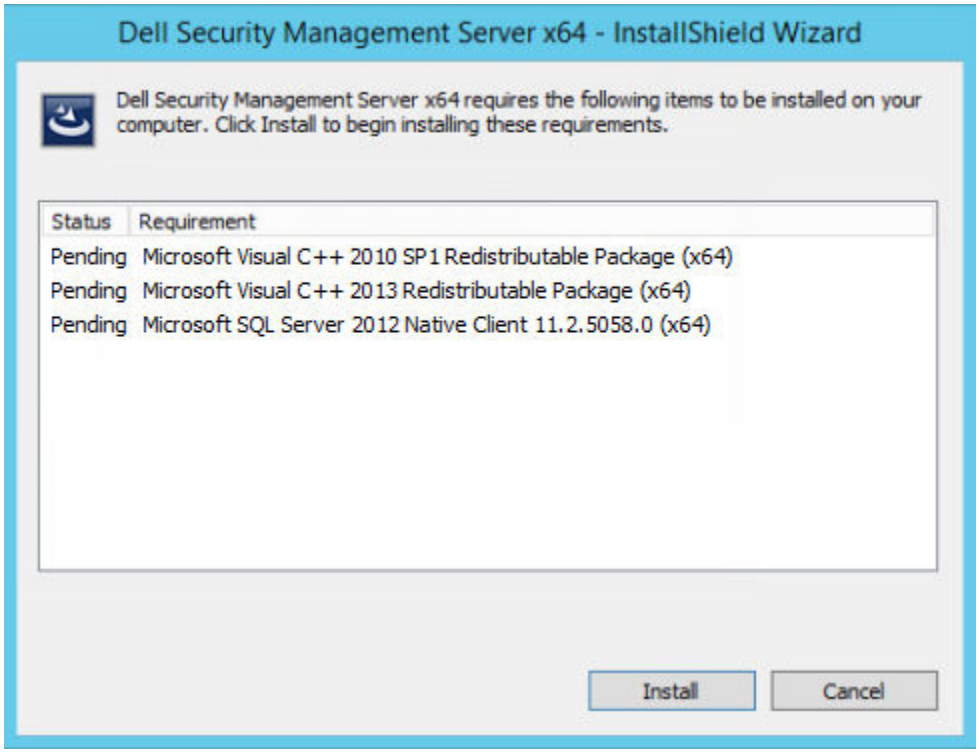
이전에 Security Management Server와 함께 기존의 데이터베이스를 설치한 경우 설치를 시작하기 전에 데이터베이스, 구성 파일, secretKeyStore를 백업했고 Security Management Server를 설치하는 서버에서 액세스할 수 있는지 확인하십시오. Security Management Server와 기존 데이터베이스를 구성하려면 이러한 파일에 액세스해야 합니다. 설치 시에 설치 프로그램에서 생성된 폴더 구조(아래 예제 참조)는 그대로 유지해야 합니다.



1. Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server에 설치할 서버의 루트 디렉토리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. 설치할 언어를 선택하고 **확인**을 클릭합니다.



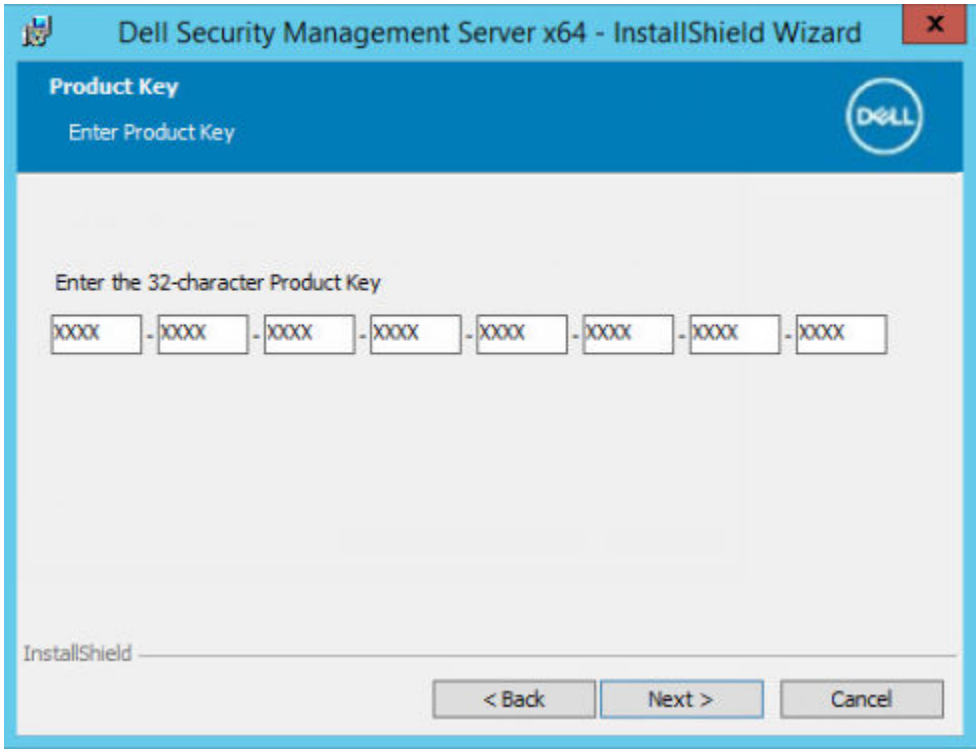
4. 사전 요구 사항이 아직 설치되어 있지 않으면, 사전 요구 사항이 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.



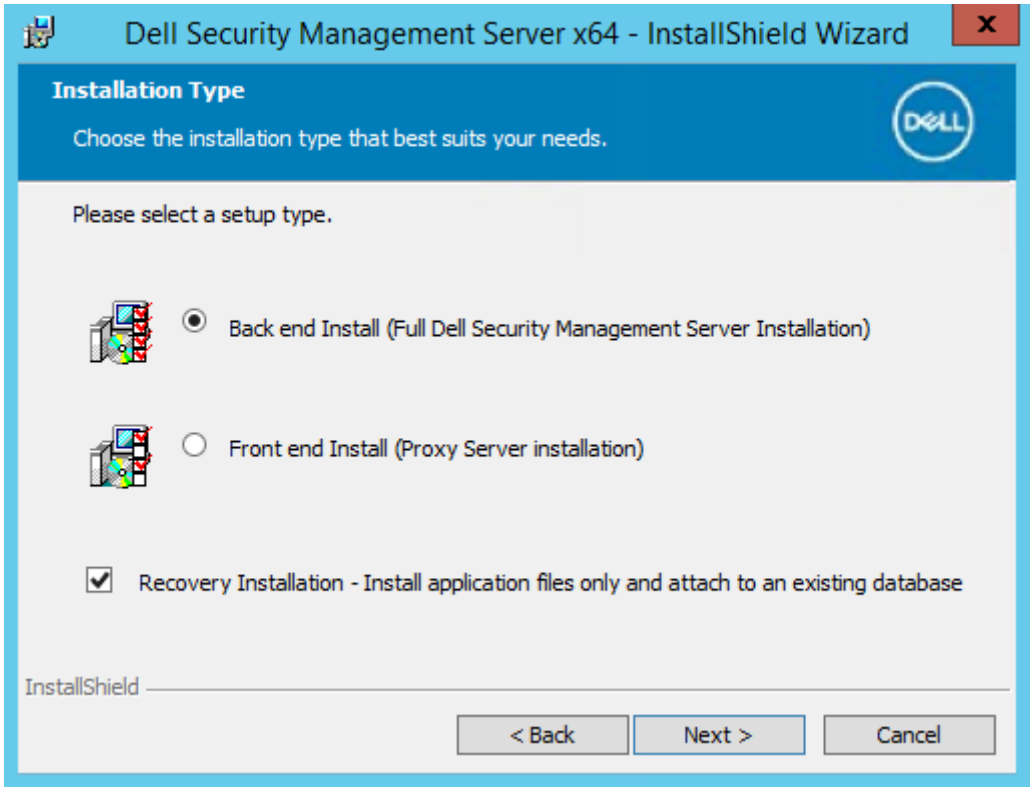
5. *시작* 대화상자에서 **다음**을 클릭합니다.

6. 라이센스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.

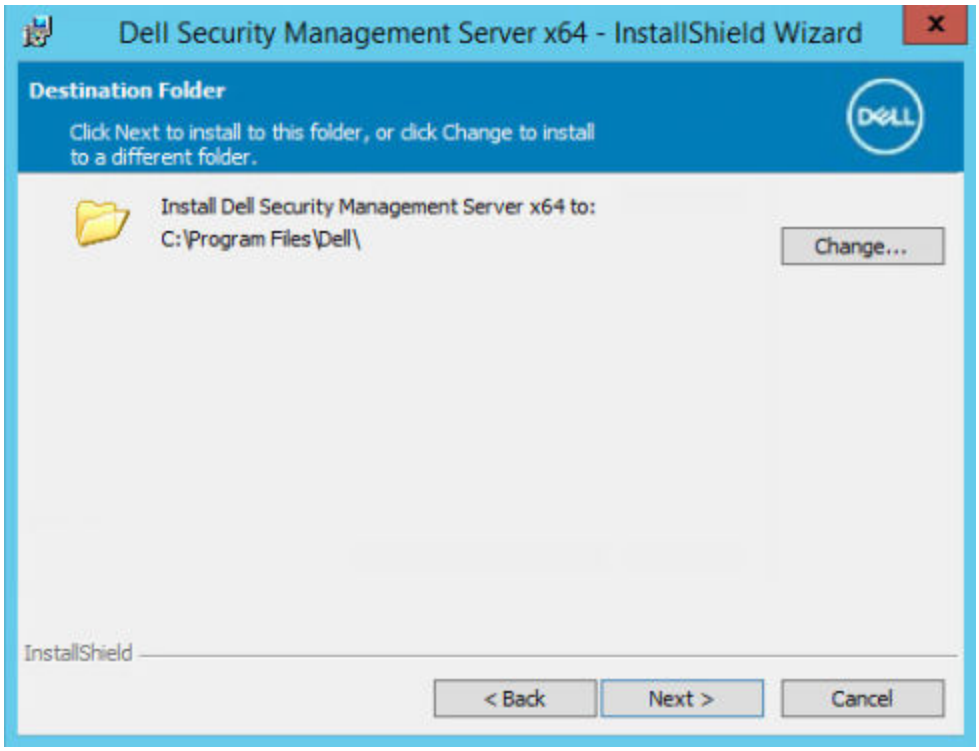
7. 선택 사항으로 사전 설치 구성의 설명에 따라 `EnterpriseServerInstallKey.ini` 파일을 `C:\Windows`에 복사한 경우 **다음**을 클릭합니다. 32자리 제품 키를 입력한 후 **다음**을 클릭합니다. 제품 키는 "`EnterpriseServerInstallKey.ini` 파일에 있습니다.



8. **백엔드 설치** 및 **복구 설치**를 선택하고 **다음**을 클릭합니다.

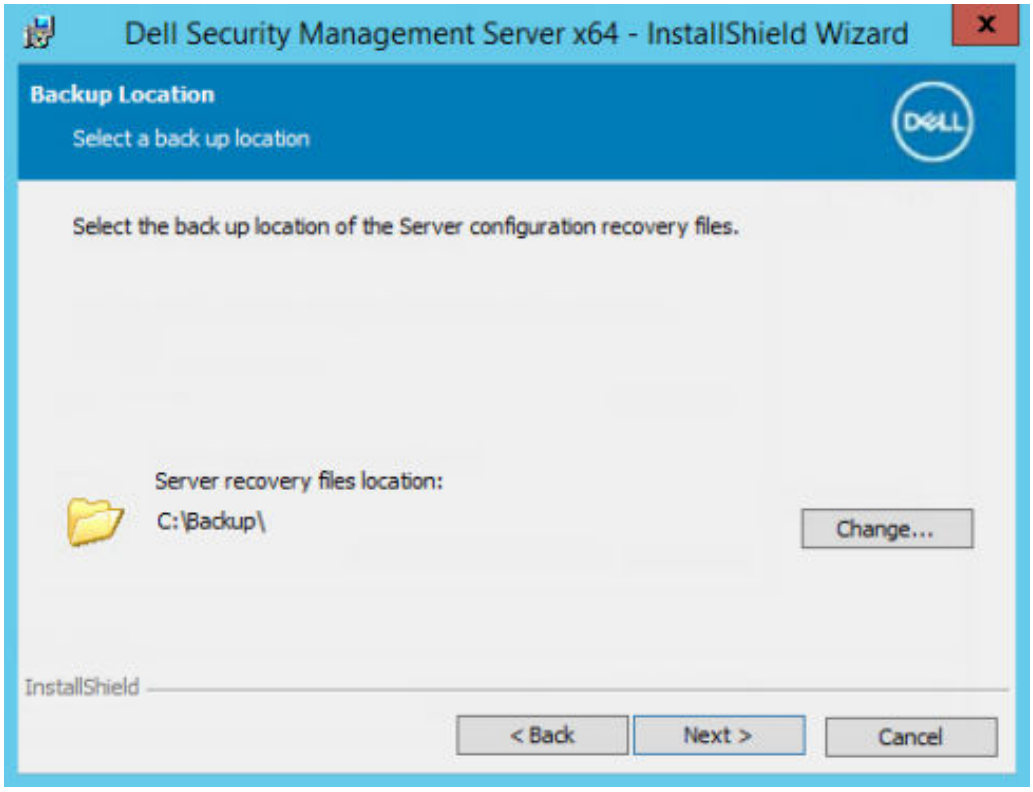


9. Security Management Server를 기본 위치인 `C:\Program Files\Dell`에 설치하려면 **다음**을 클릭합니다. 그렇지 않으면, **변경**을 클릭하여 다른 위치를 선택하고 **다음**을 클릭합니다.



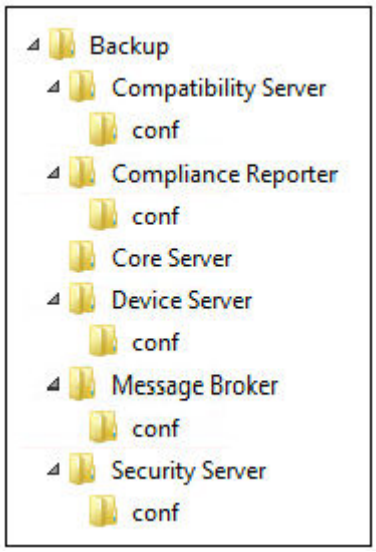
10. 백업 구성 복구 파일을 저장할 위치를 선택하려면, **변경**을 클릭하여 원하는 폴더로 이동하고 **다음**을 클릭합니다.

    원격 네트워크 위치 또는 외부 드라이브를 백업 위치로 선택하는 것이 좋습니다.



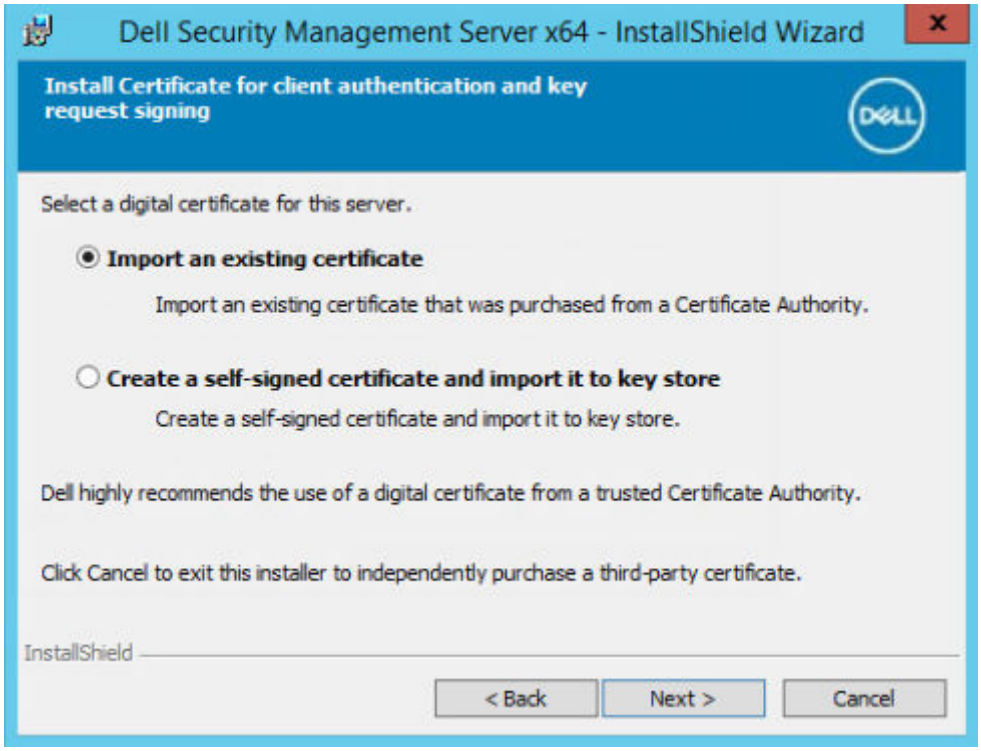
설치를 마친 후, 모든 구성 파일에 대한 변경 사항(Server 구성 도구를 통한 변경 사항 포함)은 Backup 폴더에 수동으로 저장해야 합니다. 구성 파일은 수동으로 Dell Server를 복원하는 데 필요한 전체 정보에서 중요한 역할을 합니다.

노트: 설치 시에 설치 프로그램에서 생성된 폴더 구조(아래 예제 참조)는 그대로 유지해야 합니다.



11. 사용할 디지털 인증서 유형을 선택할 수 있습니다. **신뢰할 수 있는 인증 기관의 디지털 인증서를 사용할 것을 권장합니다.** 아래에서 옵션 "a" 또는 "b"를 선택하십시오.

    a. CA 기관에서 구입한 기존 인증서를 사용하려면 **기존 인증서 가져오기**를 선택하고 **다음**을 클릭합니다.



찾아보기를 클릭하여 인증서 경로를 입력합니다.

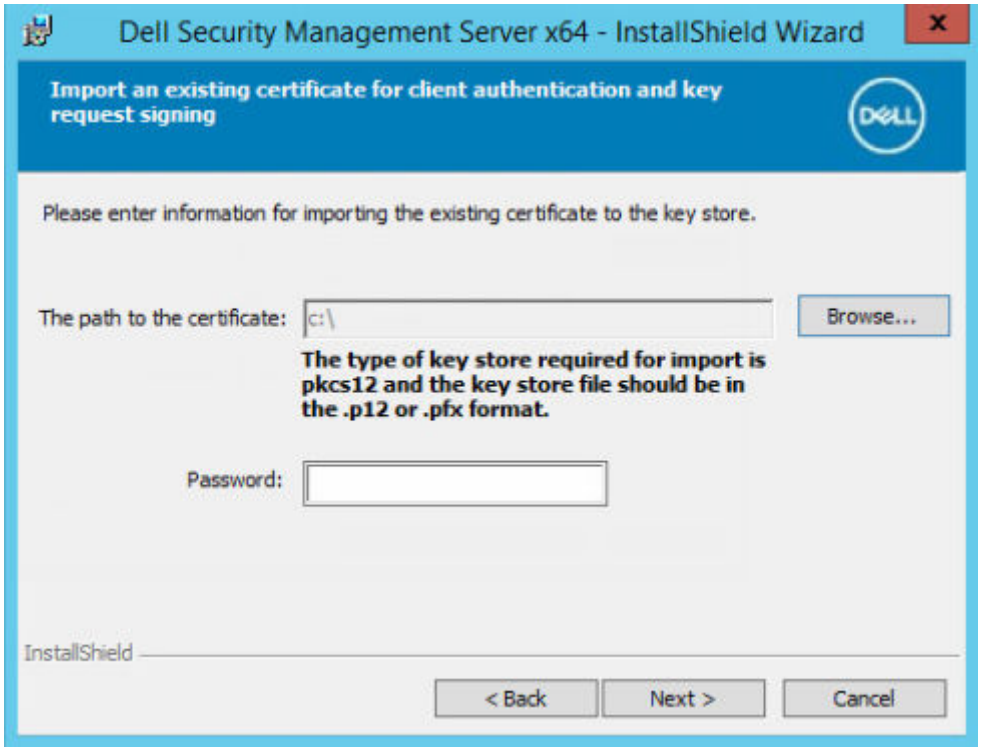
이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 Certificate Management Console을 사용하여 PFX에 인증서 내보내기를 참조하십시오.

다음을 클릭합니다.

노트:

이 설정을 사용하려면, 내보내진 CA 인증서 중 가져올 CA 인증서에 최대의 신뢰 체인이 수립되어 있어야 합니다. 확실하지 않을 경우, CA 인증서를 다시 내보내고 "인증서 내보내기 마법사"에서 다음 옵션이 선택되었는지 확인하십시오.

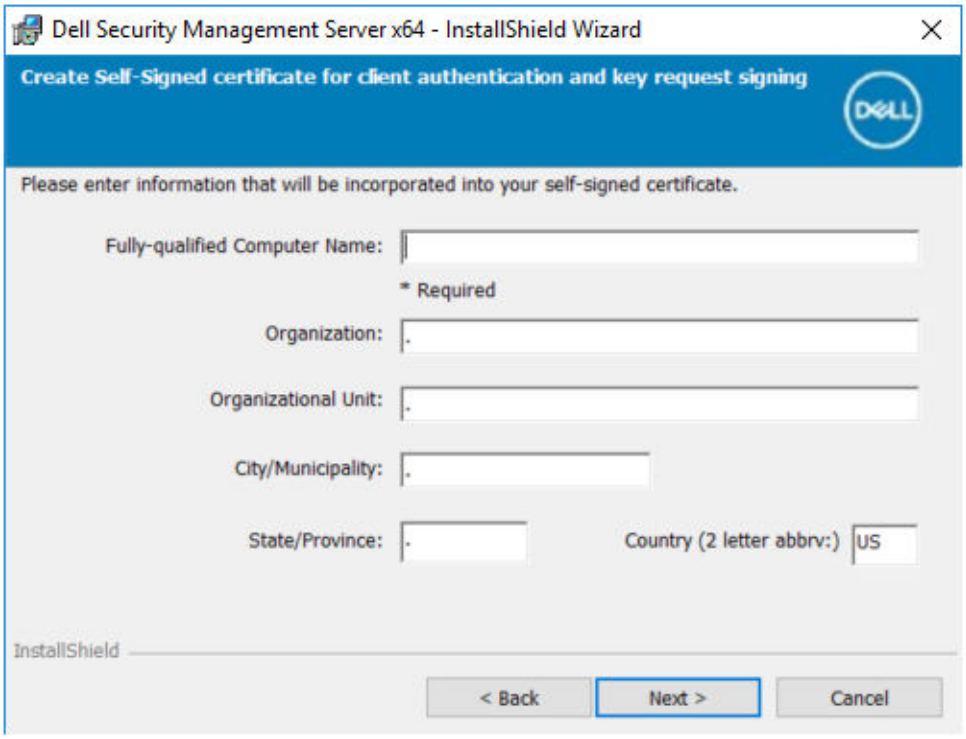
- 개인 정보 교환 - PKCS#12(.PFX)
- 가능한 한 모든 인증서를 인증서 경로에 포함
- 모든 확장 속성을 내보냄



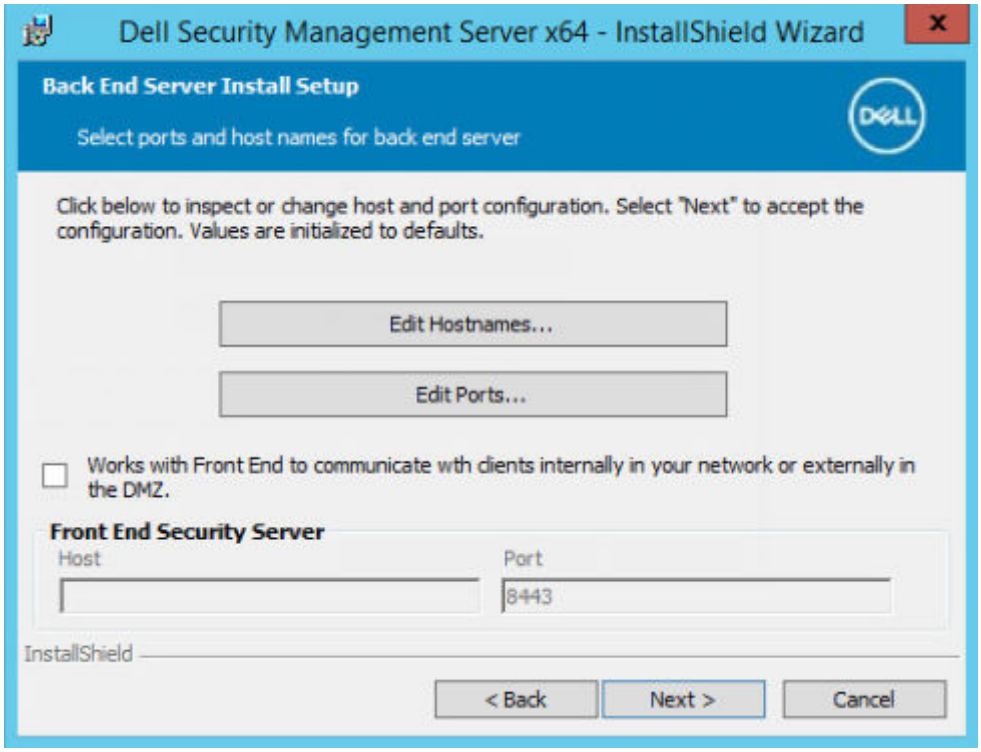
또는

b. 자체 서명된 인증서를 만들려면 **자체 서명된 인증서를 생성하여 키 스토리지에 가져오기를 선택하고 다음을 클릭합니다.**
자체 서명 인증 대화상자에 다음 정보를 입력합니다.
정규화된 컴퓨터 이름(예: computername.domain.com)
조직
조직 단위(예: 보안 팀)
시
도(전체 이름)
국가: 알파벳 두 글자로 된 국가 약어
다음을 클릭합니다.

노트: 기본적으로 인증서 유효 기간은 10년입니다.



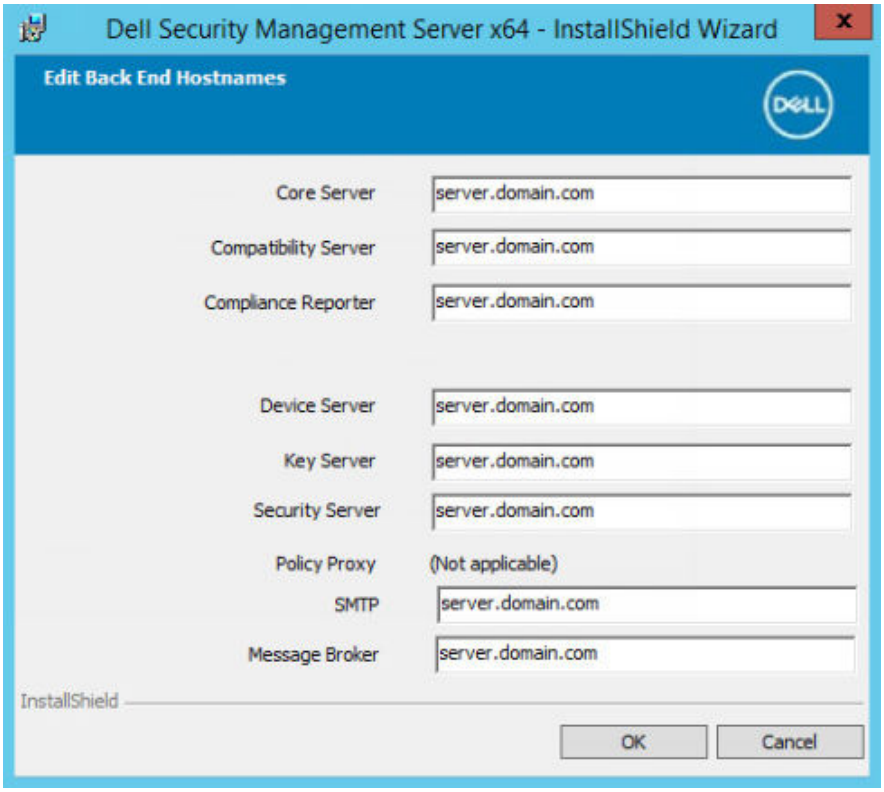
12. *백엔드 서버 설치 설정* 대화상자에서 호스트 이름 및 포트를 보거나 편집할 수 있습니다.
    - 기본 호스트 이름 및 포트를 수락하려면 *백엔드 서버 설치 설정* 대화상자에서 **다음**을 클릭합니다.
    - 프론트 엔드 서버를 사용하는 경우 **네트워크 내부 또는 DMZ 외부로 클라이언트와 통신하도록 프론트 엔드 작동**을 선택하고 프론트 엔드 보안 서버 호스트 이름(예: server.domain.com)을 입력합니다.



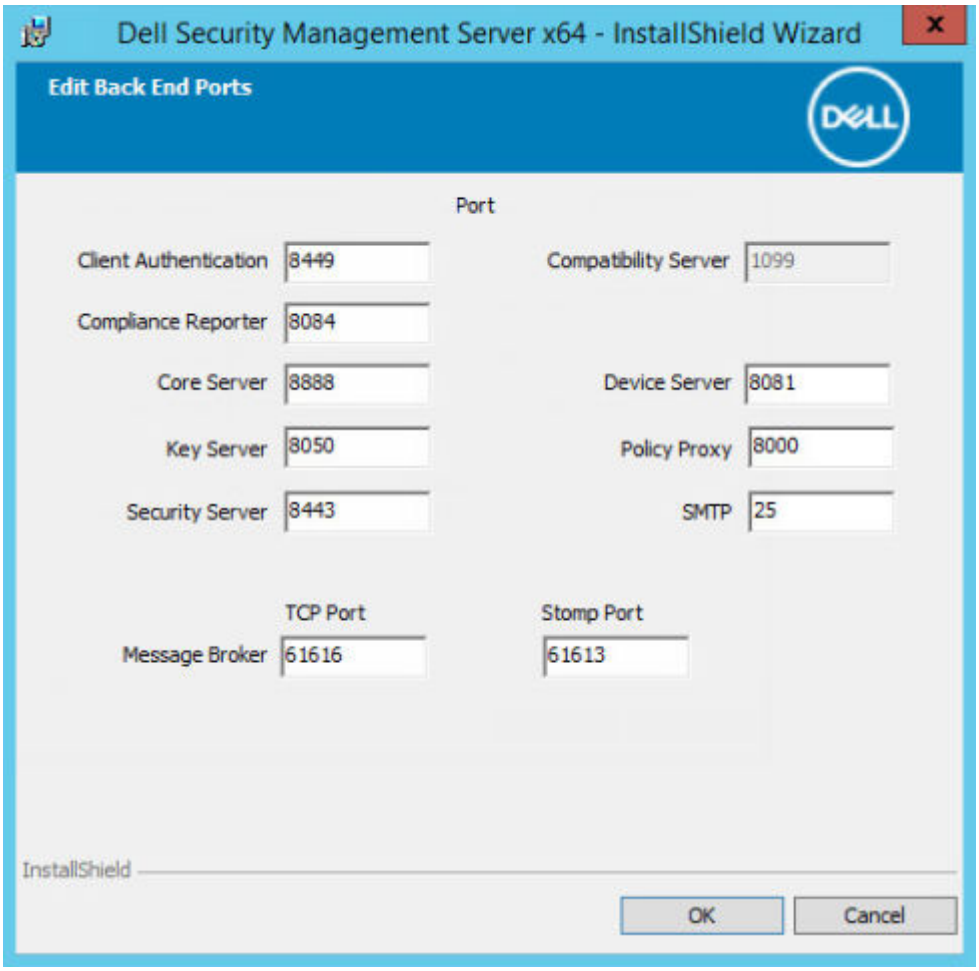
    - 호스트 이름을 보거나 편집하려면 **호스트 이름 편집**을 클릭합니다. 필요한 경우에만 호스트 이름을 편집합니다. 기본값 사용을 권장합니다.

      노트: 호스트 이름에는 밑줄("_")을 사용할 수 없습니다.

      작업을 마친 후 **확인**을 클릭합니다.



- 포트를 보거나 편집하려면 **포트 편집**을 클릭합니다. 필요한 경우에만 포트를 편집합니다. 기본값 사용을 권장합니다. 작업을 마친 후 **확인**을 클릭합니다.

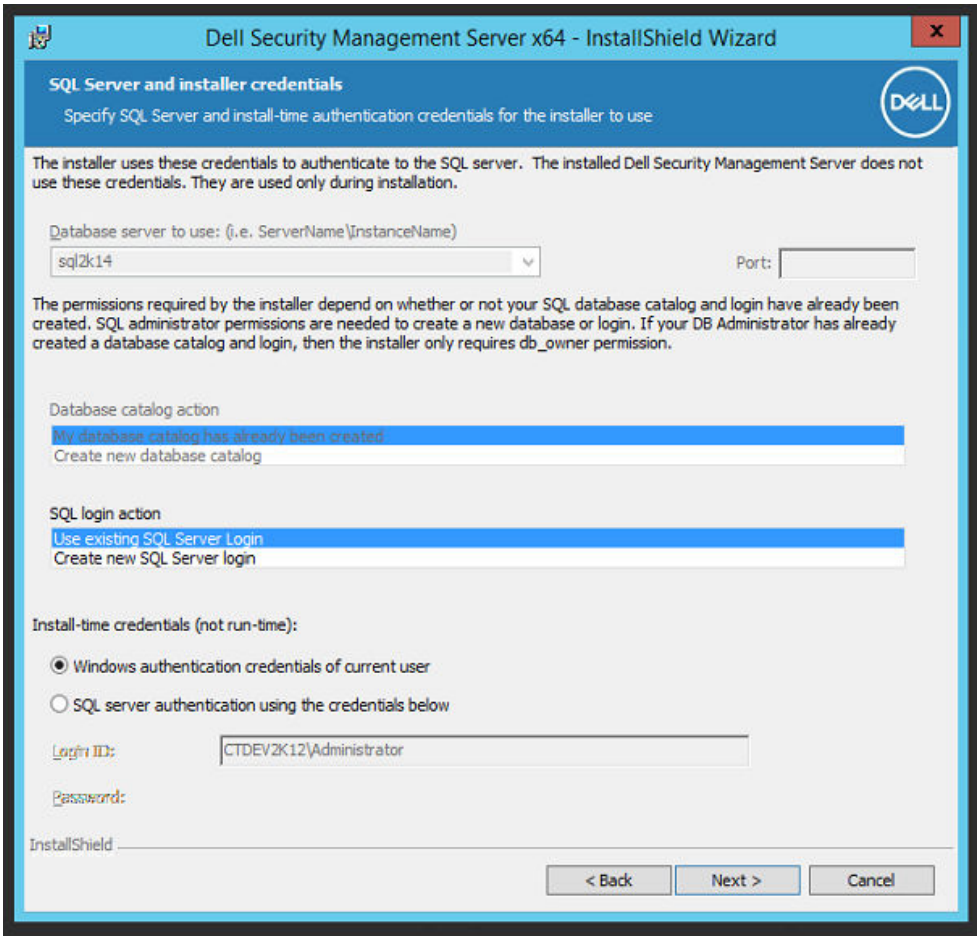


13. 사용할 설치 프로그램에 대해 인증 방법을 지정합니다.

a. **찾아보기**를 클릭하여 데이터베이스가 위치한 서버를 선택합니다.
b. 인증 유형을 선택합니다.

- **현재 사용자의 Windows 인증 자격 증명**

  Windows 인증을 선택하면 Windows에 로그인하는 데 사용한 자격 증명이 인증에 사용됩니다(*사용자 이름* 및 *암호*는 수정할 수 없음). 해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다.



또는

- **다음 자격 증명을 사용해 SQL 서버 인증**

  SQL 인증을 사용하려면 사용되는 SQL 계정에 SQL 서버에 대한 시스템 관리자 권한이 있어야 합니다.

  설치 프로그램은 이 허가를 통해 SQL 서버에 인증해야 합니다: 데이터베이스 생성, 사용자 추가, 허용 할당.

c. **찾아보기**를 클릭하여 기존 데이터베이스 카탈로그의 이름을 선택합니다.
d. **다음**을 클릭합니다.

14. 기존 데이터베이스 오류 대화 상자가 표시되는 경우 적절한 옵션을 선택합니다.

    설치 프로그램에서 데이터베이스의 문제가 발견된 경우 *기존 데이터베이스 오류* 대화 상자가 표시됩니다. 대화 상자의 옵션은 상황에 따라 다르게 표시됩니다.

- 데이터베이스 스키마가 이전 버전입니다. 단계 a를 참조하십시오.
- 데이터베이스에 현재 설치되고 있는 버전에 일치하는 데이터베이스 스키마가 이미 있습니다. 단계 b를 참조하십시오.

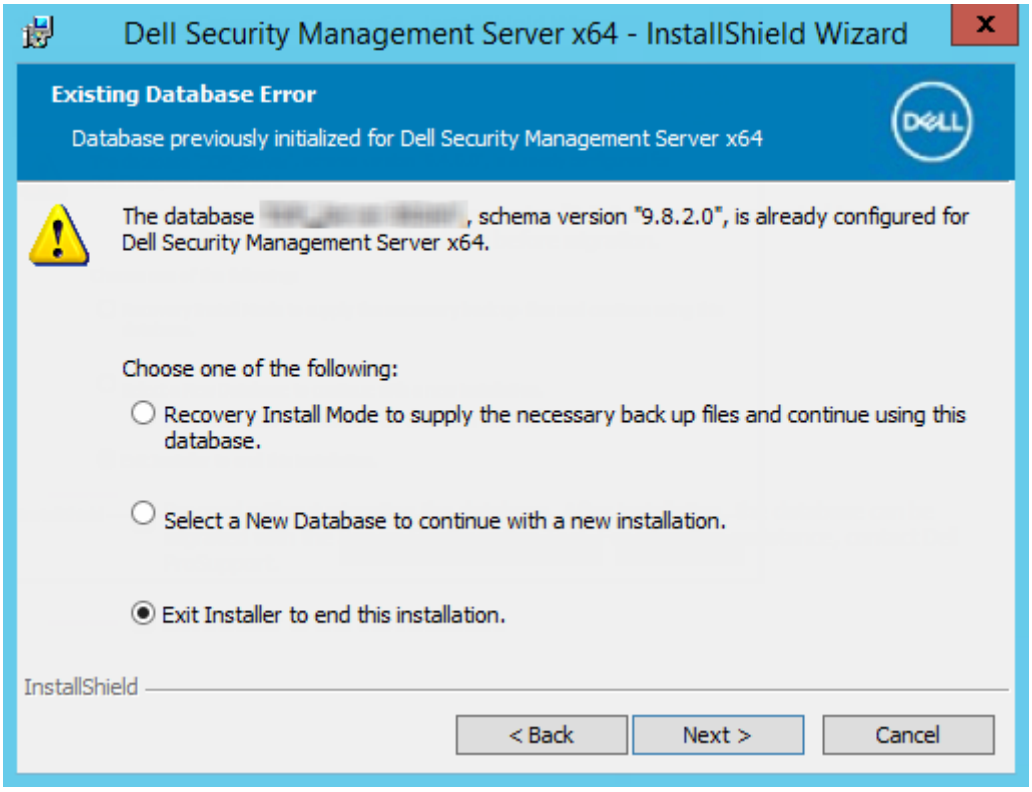
a. 데이터베이스가 이전 버전인 경우, **설치 프로그램을 종료해 이 설치 완료**를 선택합니다. 다음, 데이터베이스를 백업해야 합니다.

다음 옵션은 반드시 Dell ProSupport의 도움을 받아 사용해야 합니다.

- **현재 스키마에 이 데이터베이스 마이그레이션** 옵션은 오류가 발생한 서버 구현에서 상태가 양호한 데이터베이스를 복구하는 데 사용됩니다. 이 옵션으로 \Backup 폴더의 복구 파일을 사용하여 데이터베이스에 재연결하고 데이터베이스를 현재 스키마로 마이그레이션합니다. 이 옵션은 Security Management Server의 올바른 버전을 재설치하고 업그레이드할 최신 설치 프로그램을 실행한 *이후에만* 사용해야 합니다.
- **데이터베이스 마이그레이션 없이 진행** 옵션은 데이터베이스를 완전히 구성하지 않은 상태에서 Security Management Server를 설치합니다. 데이터베이스 구성은 Server 구성 도구를 사용하여 수동으로 나중에 완료해야 하고 추가 수동 변경이 필요합니다.

b. 데이터베이스 스키마가 현재 버전의 스키마이지만 Security Management Server backend에 연결되어 있지 않은 경우, *복구로 간주합니다.* 이 단계에서 **복구 설치**를 선택하지 않은 경우 이 대화 상자가 나타납니다.
   - 선택한 데이터베이스로 설치를 계속 진행하려면 **복구 설치 모드**를 선택합니다.
   - 다른 데이터베이스를 지정하려면 **새 데이터베이스 선택**을 선택합니다.
   - **설치 프로그램을 종료해 이 설치 종료**를 선택합니다.

c. **다음**을 클릭합니다.



15. 사용할 제품에 대해 인증 방법을 선택합니다. 제품에서 데이터베이스 및 Dell 서비스로 작업하는 데 사용할 계정입니다.

- **Windows 인증을 사용하려면**

  아래의 자격 증명을 사용해 Windows 인증을 선택하고 제품에서 사용할 수 있는 계정에 대한 자격 증명을 입력한 후 **다음**을 클릭합니다.

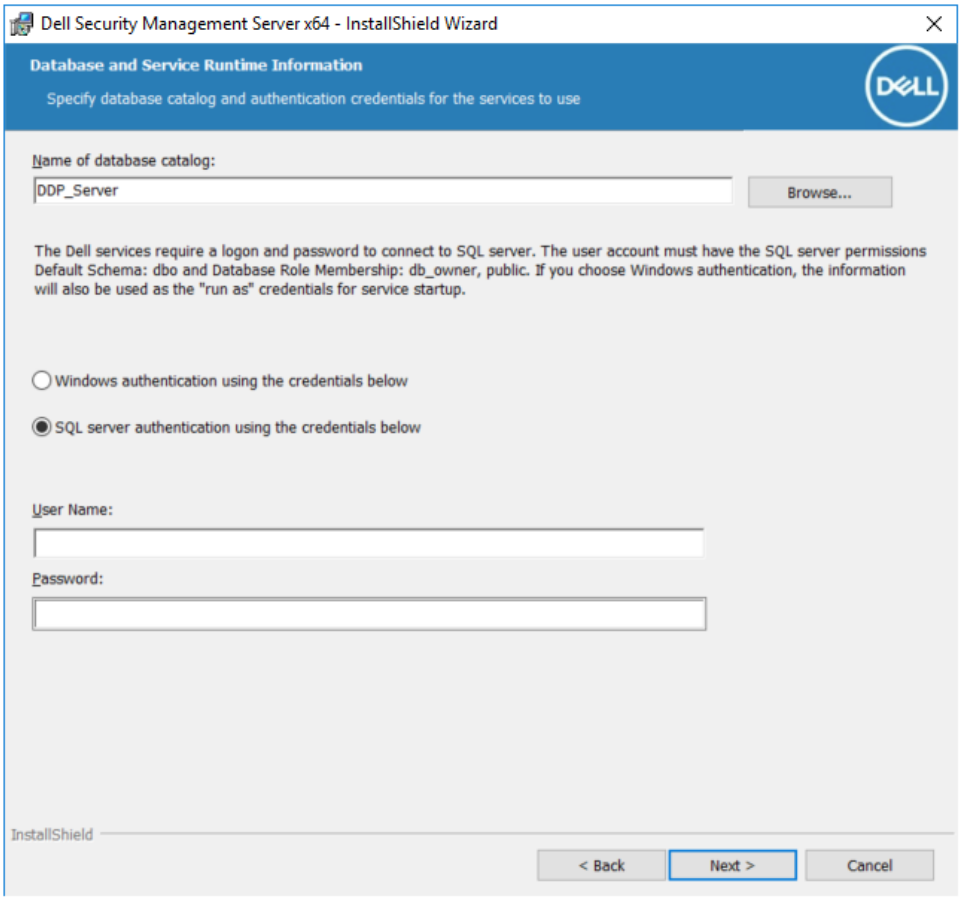
  해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.

  또는

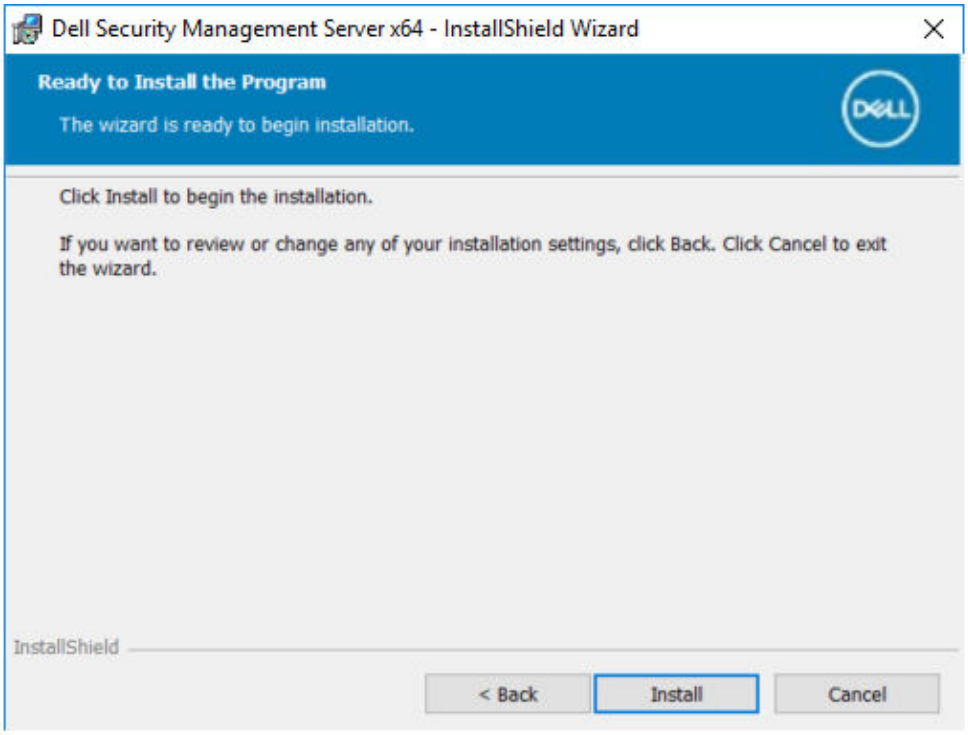
- **SQL Server 인증을 사용하려면**

  다음 자격 증명을 사용해 **SQL Server 인증**을 선택하고 SQL Server 자격 증명을 입력한 다음, **다음**을 클릭합니다.

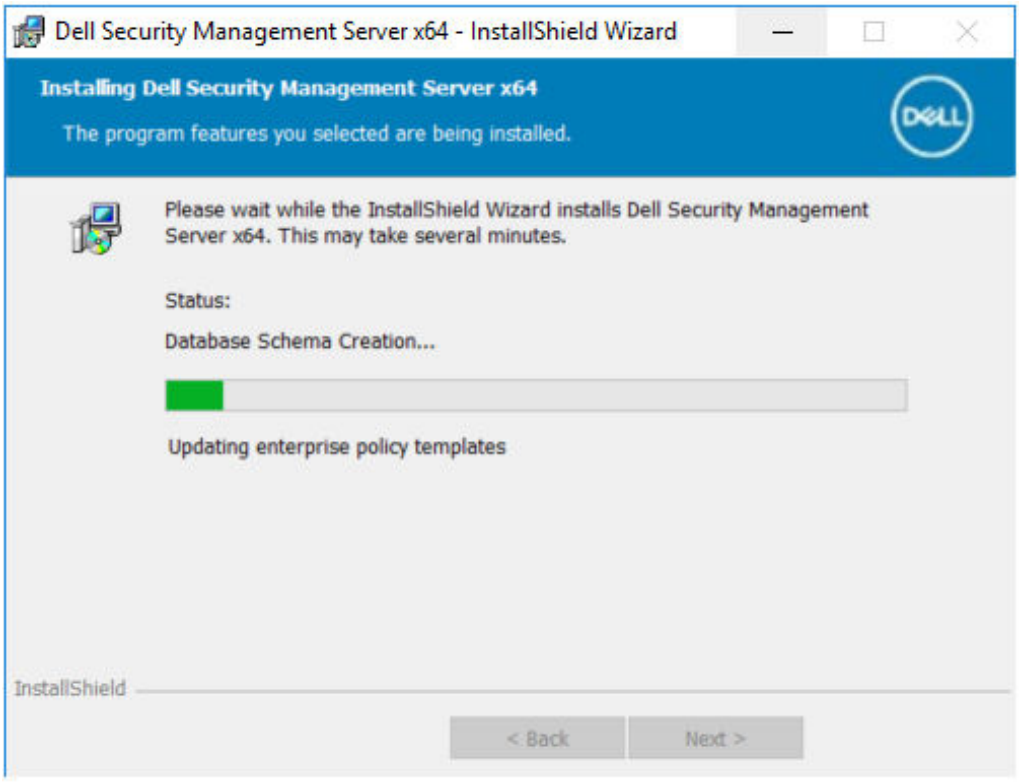
  사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.



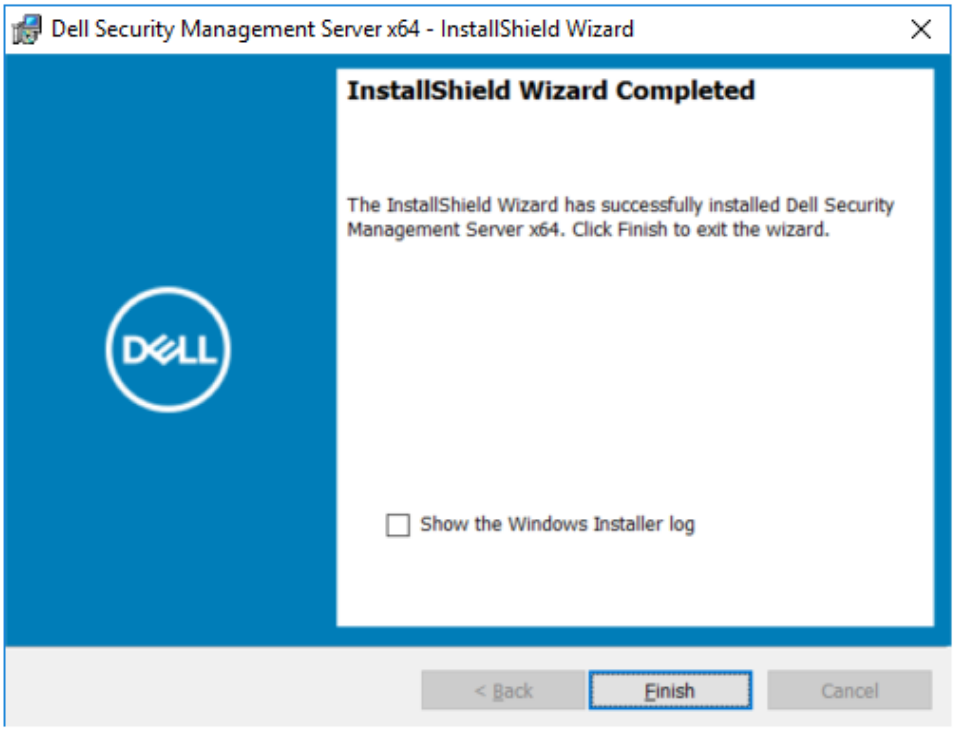
16. *프로그램 설치 준비 완료* 대화상자에서 **설치**를 클릭합니다



진행률 대화상자에 설치 과정 상태가 표시됩니다.



설치가 완료되면 **마침**을 클릭합니다.



백엔드 서버 설치 작업이 완료됩니다.

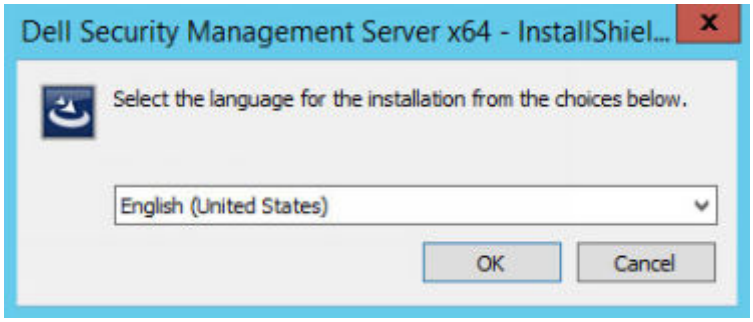
설치가 끝나면 Dell 서비스가 다시 시작됩니다. 서버를 다시 부팅할 필요는 없습니다.

프론트 엔드 서버 설치

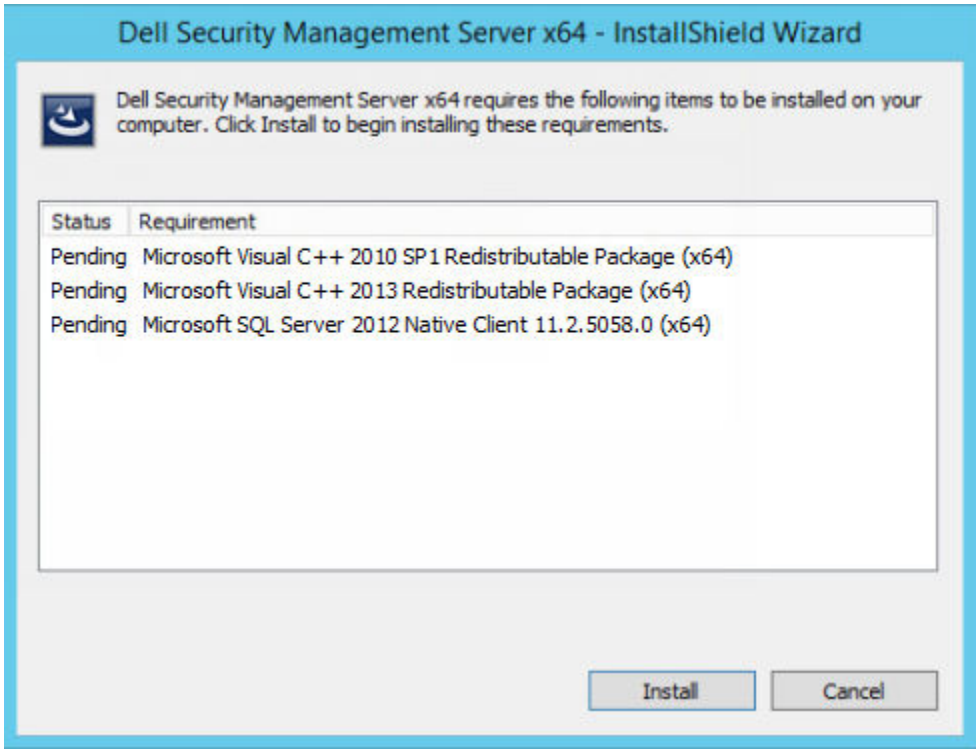
프론트 엔드 서버 설치에서는 Security Management Server와 함께 사용하기 위한 프론트 엔드(DMZ mode) 옵션을 제공합니다. DMZ에 Dell 구성요소를 배포하려면, 구성요소가 공격으로부터 적절히 보호를 받을 수 있는지 확인해야 합니다.

이 설치를 수행하려면 DMZ 서버의 정규화된 호스트 이름이 필요합니다.

1. Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server을 설치할 서버의 루트 디렉토리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. 설치할 언어를 선택하고 **확인**을 클릭합니다.

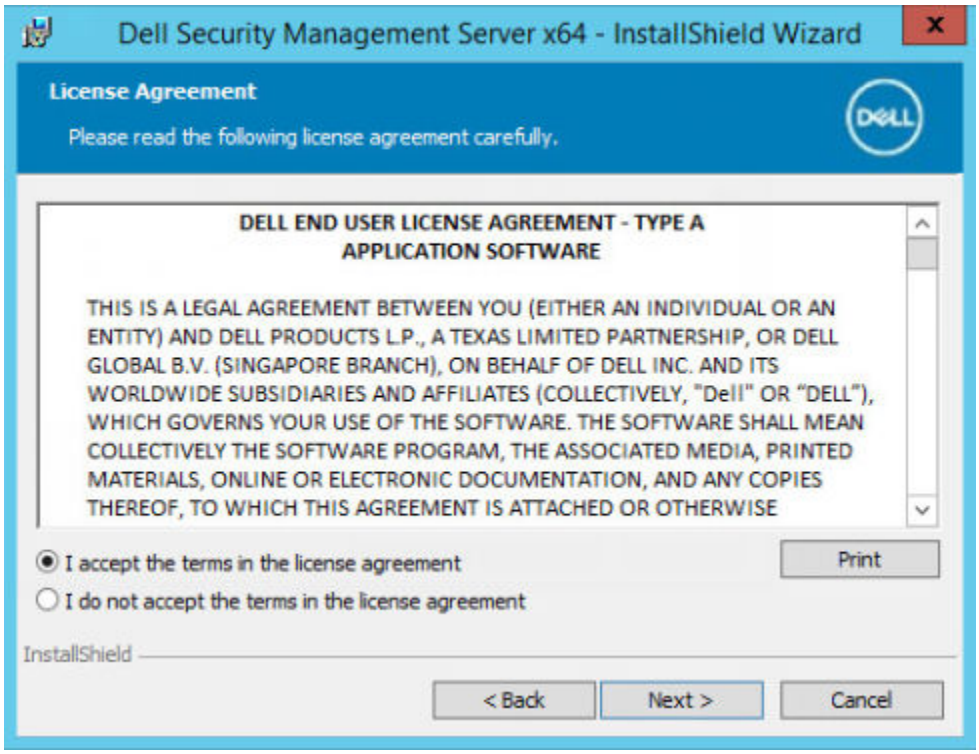


4. 사전 요구 사항이 아직 설치되어 있지 않으면, 사전 요구 사항이 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.

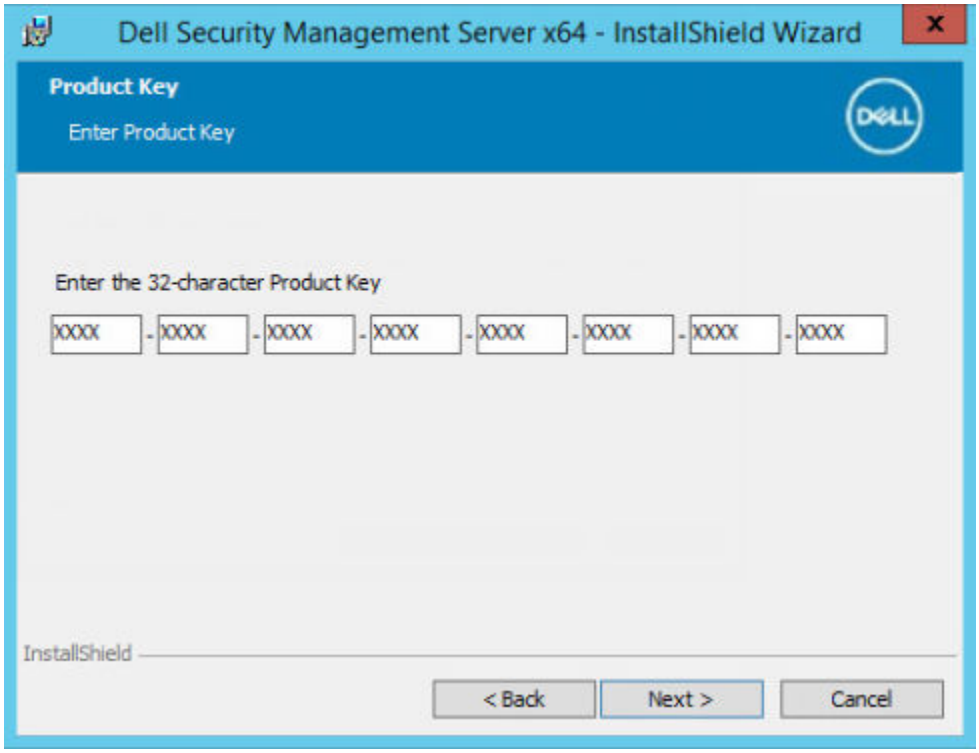


5. 시작 대화 상자에서 **다음**을 클릭하십시오.

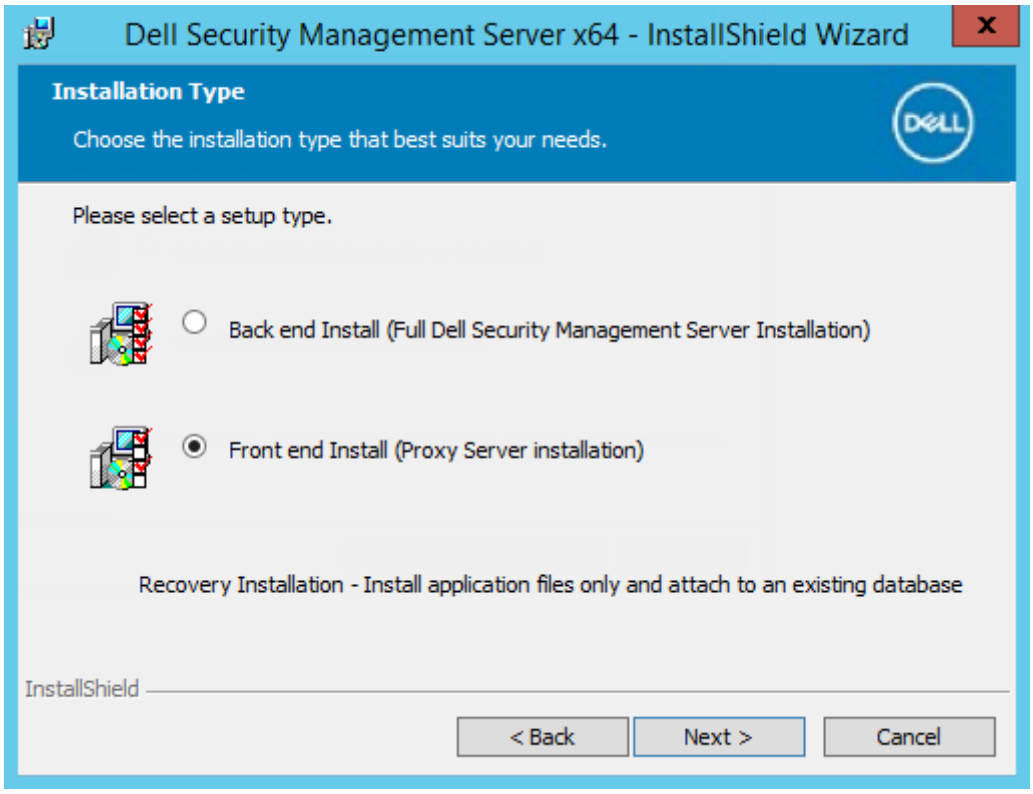
6. 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.



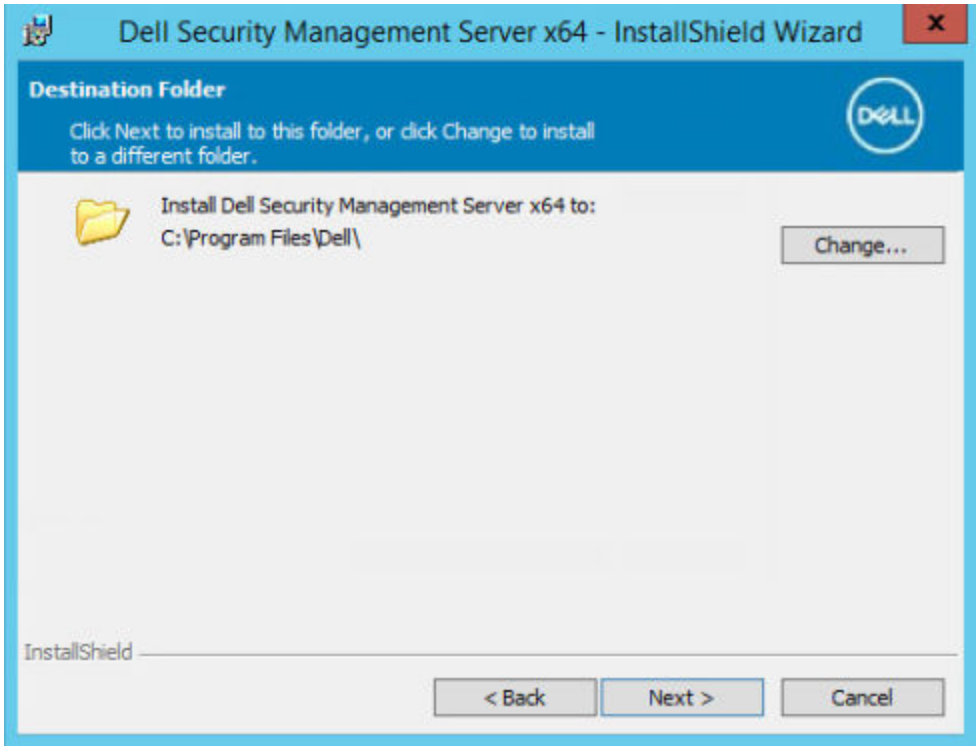
7. 선택 사항으로 사전 설치 구성의 설명에 따라 `EnterpriseServerInstallKey.ini` 파일을 `C:\Windows`에 복사한 경우 **다음**을 클릭합니다. 32자리 제품 키를 입력한 후 **다음**을 클릭합니다. 제품 키는 `EnterpriseServerInstallKey.ini` 파일에 있습니다.



8. **프론트 엔드 설치**를 선택하고 **다음**을 클릭합니다.



9. 프론트 엔드 서버를 기본 위치인 `C:\Program Files\Dell`에 설치하려면 **다음**을 클릭합니다. 그렇지 않은 경우, **변경**을 클릭하여 다른 위치를 선택한 후 **다음**을 클릭합니다.

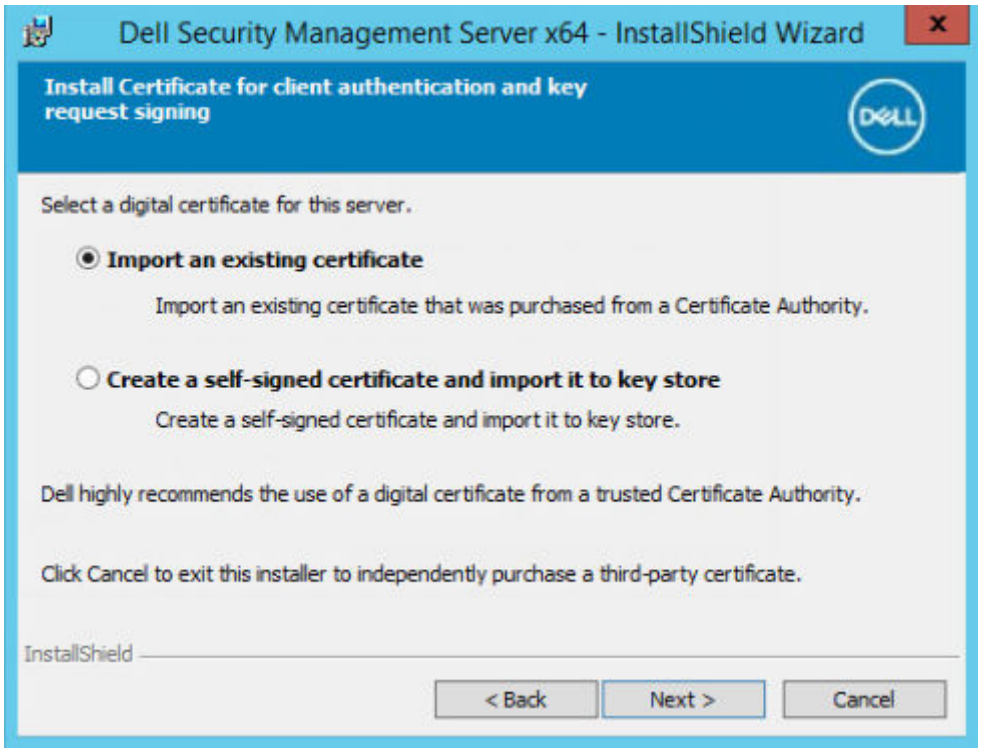


10. 사용할 디지털 인증서 유형을 선택할 수 있습니다.

    노트: 신뢰할 수 있는 인증 기관의 디지털 인증서를 사용할 것을 권장합니다.

    아래에서 옵션 "a" 또는 "b"를 선택하십시오.

    a. CA 기관에서 구입한 기존 인증서를 사용하려면 **기존 인증서 가져오기**를 선택하고 **다음**을 클릭합니다.



    찾아보기를 클릭하여 인증서 경로를 입력합니다.

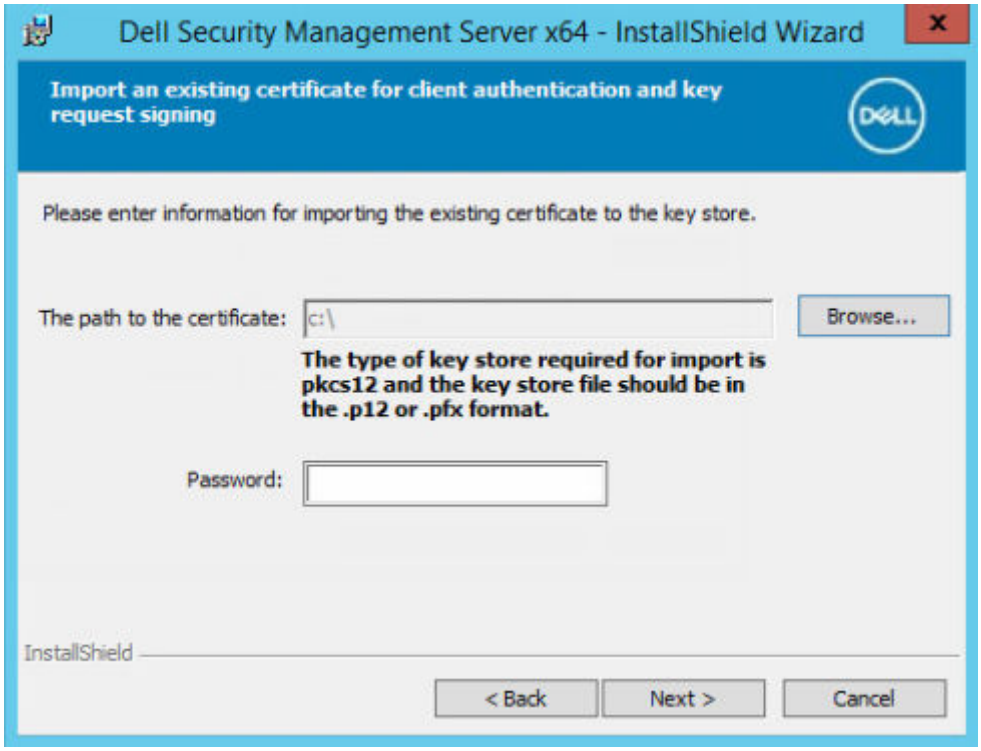
    이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 Certificate Management Console을 사용하여 PFX에 인증서 내보내기를 참조하십시오.

    다음을 클릭합니다.

노트:

이 설정을 사용하려면, 내보내진 CA 인증서 중 가져올 CA 인증서에 최대의 신뢰 체인이 수립되어 있어야 합니다. 확실하지 않을 경우, CA 인증서를 다시 내보내고 "인증서 내보내기 마법사"에서 다음 옵션이 선택되었는지 확인하십시오.

- 개인 정보 교환 - PKCS#12(.PFX)
- 가능한 한 모든 인증서를 인증서 경로에 포함
- 모든 확장 속성을 내보냄



b. 자체 서명된 인증서를 만들려면 **자체 서명된 인증서를 생성하여 키 스토리지에 가져오기를 선택하고 다음을 클릭합니다.**

자체 서명 인증 대화상자에 다음 정보를 입력합니다.

정규화된 컴퓨터 이름(예: computername.domain.com)

조직

조직 단위(예: 보안 팀)

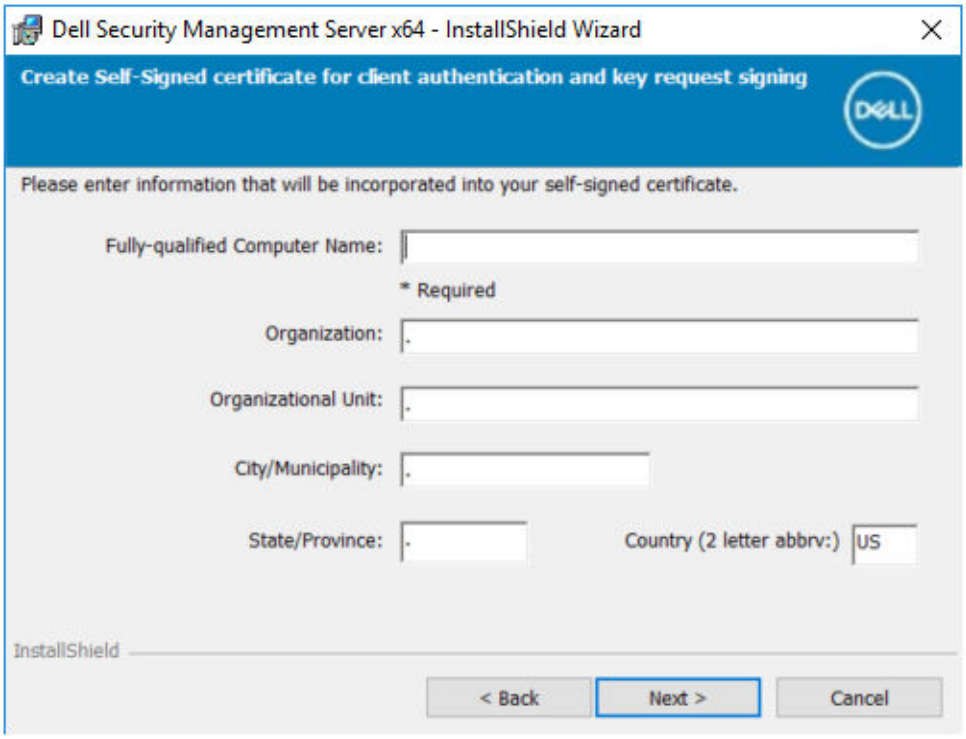
시

도(전체 이름)

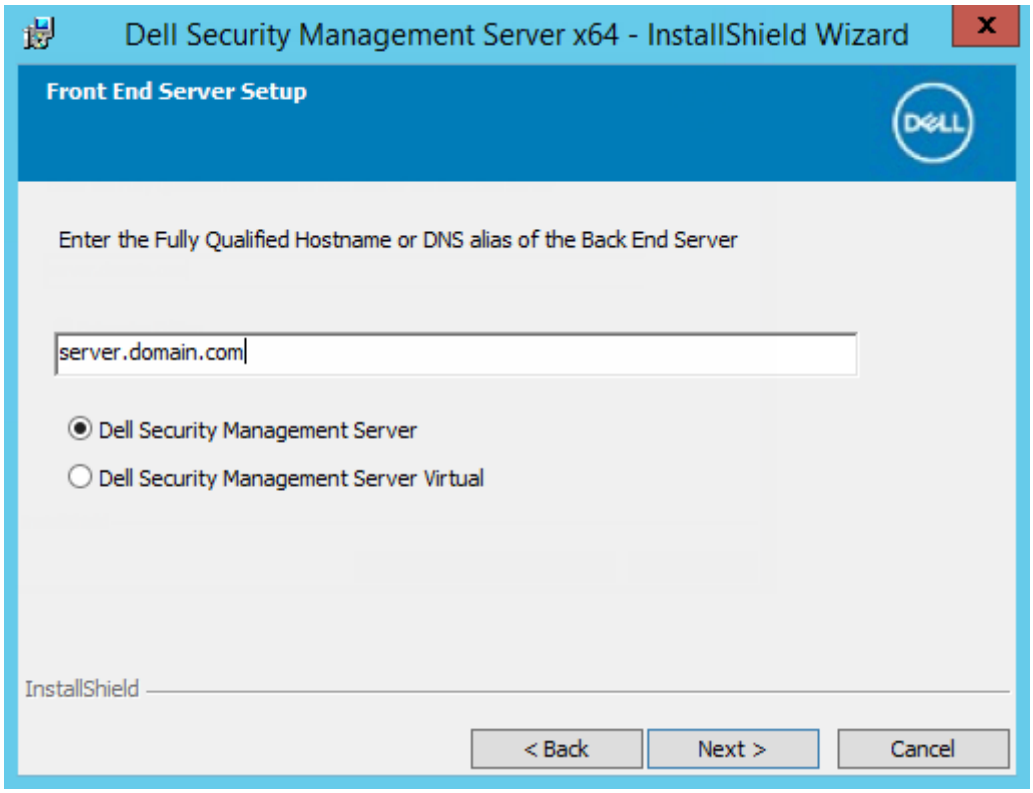
국가: 알파벳 두 글자로 된 국가 약어

다음을 클릭합니다.

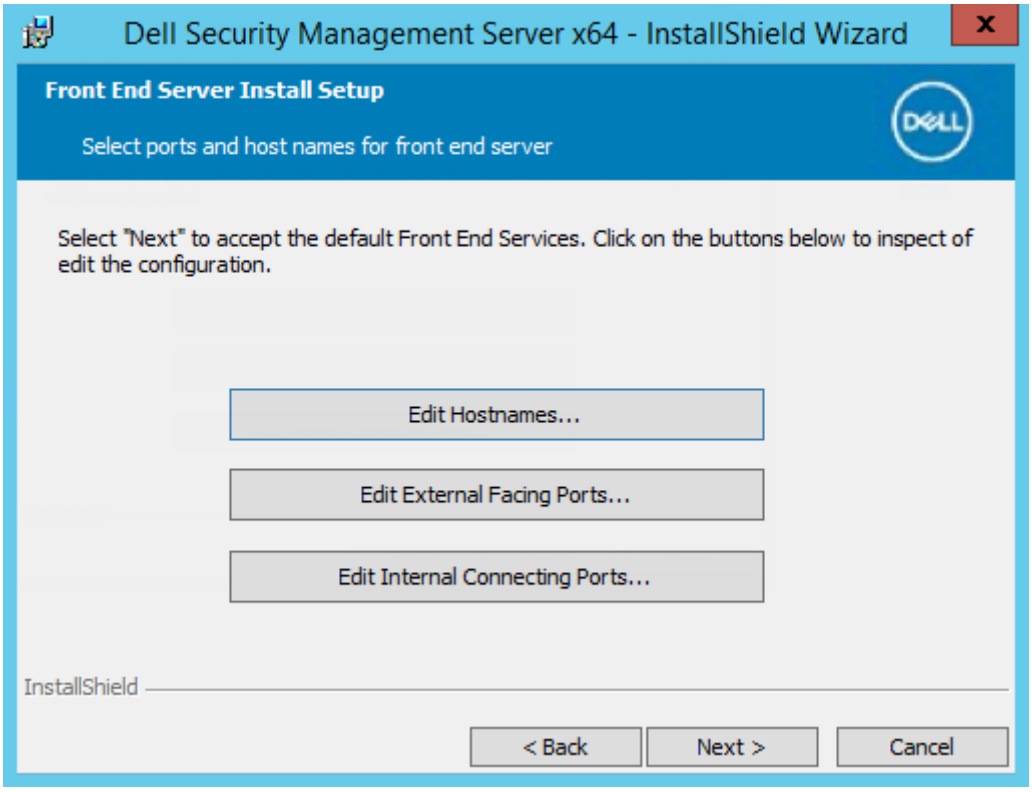
노트: 기본적으로 인증서 유효 기간은 10년입니다.



11. *프론트 엔드 서버 설정* 대화상자에서, 백엔드 서버의 정규화된 호스트 이름이나 DNS 별칭을 입력하고 **Dell Security Management Server**를 선택한 후 **다음**을 클릭합니다.



12. *프론트 엔드 서버 설치 설정* 대화상자에서 호스트 이름 및 포트를 보거나 편집할 수 있습니다.
    - 기본 호스트 이름 및 포트를 수락하려면 *프론트 엔드 서버 설치 설정* 대화상자에서 **다음**을 클릭합니다.



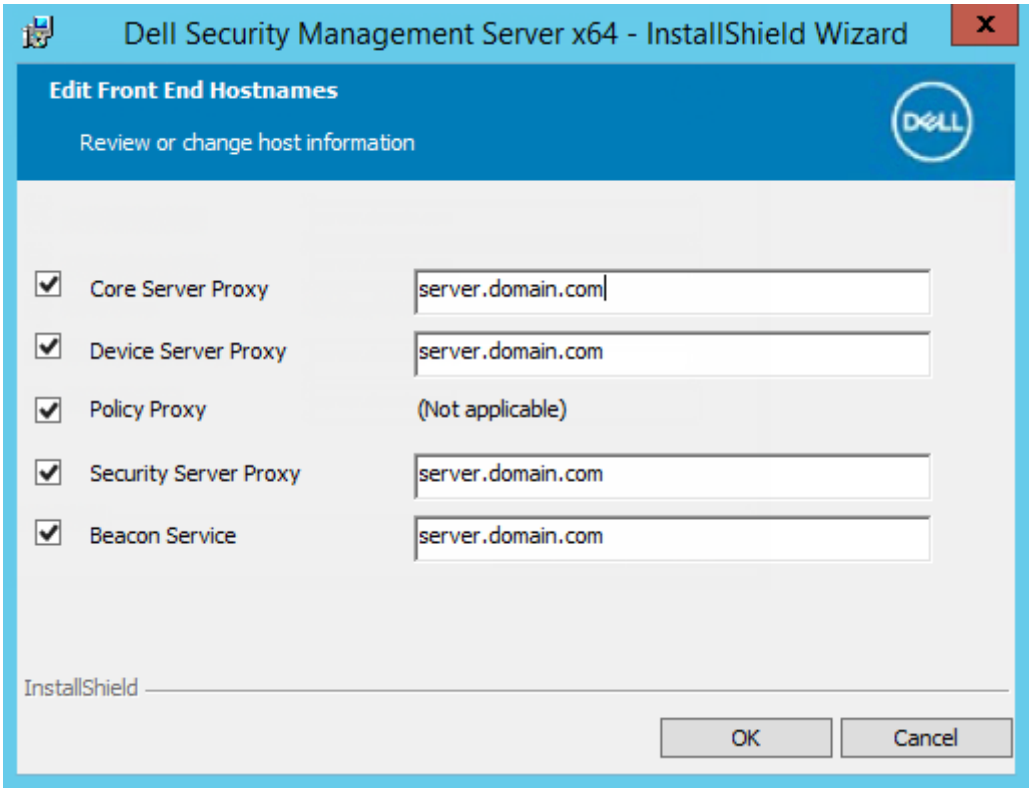
- 호스트 이름을 보거나 편집하려면 *프론트 엔드 서버 설정* 대화상자에서 **호스트 이름 편집**을 클릭합니다. 필요한 경우에만 호스트 이름을 편집합니다. 기본값 사용을 권장합니다.

  노트:

  호스트 이름에는 밑줄("_")을 사용할 수 없습니다.

  프록시 설치를 구성하지 않으려는 경우에만 프록시를 선택 취소하십시오. 이 대화상자에서 프록시를 선택 취소하면 프록시가 설치되지 않습니다.

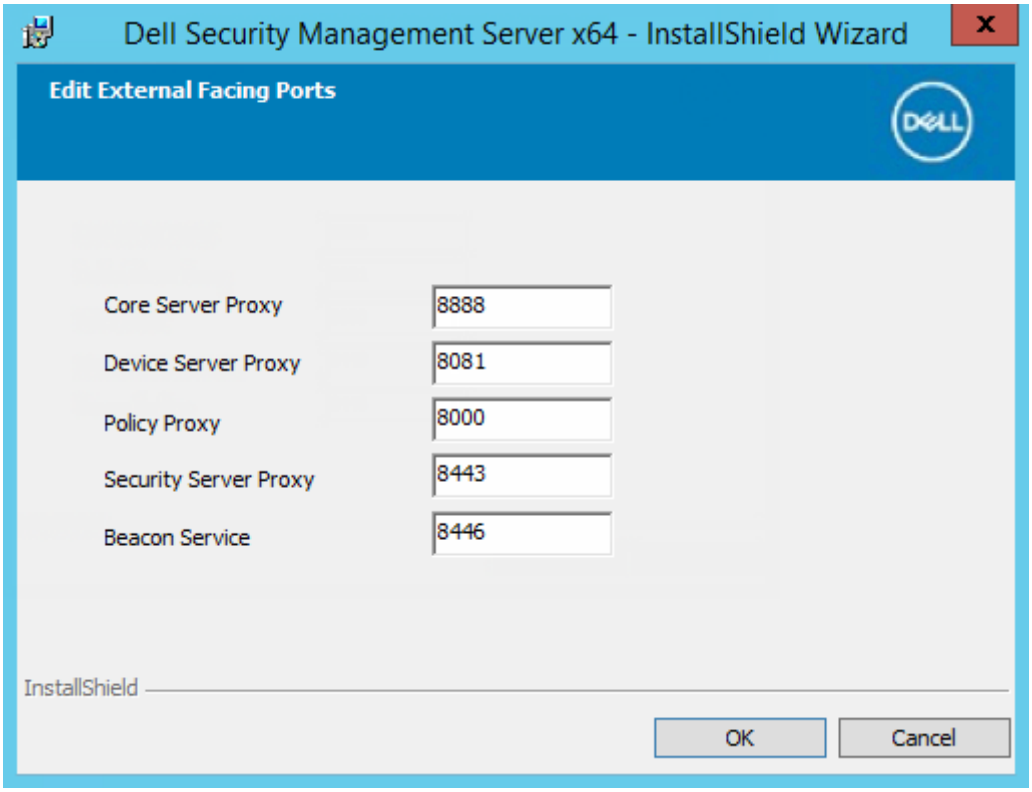
  작업을 마친 후 **확인**을 클릭합니다.

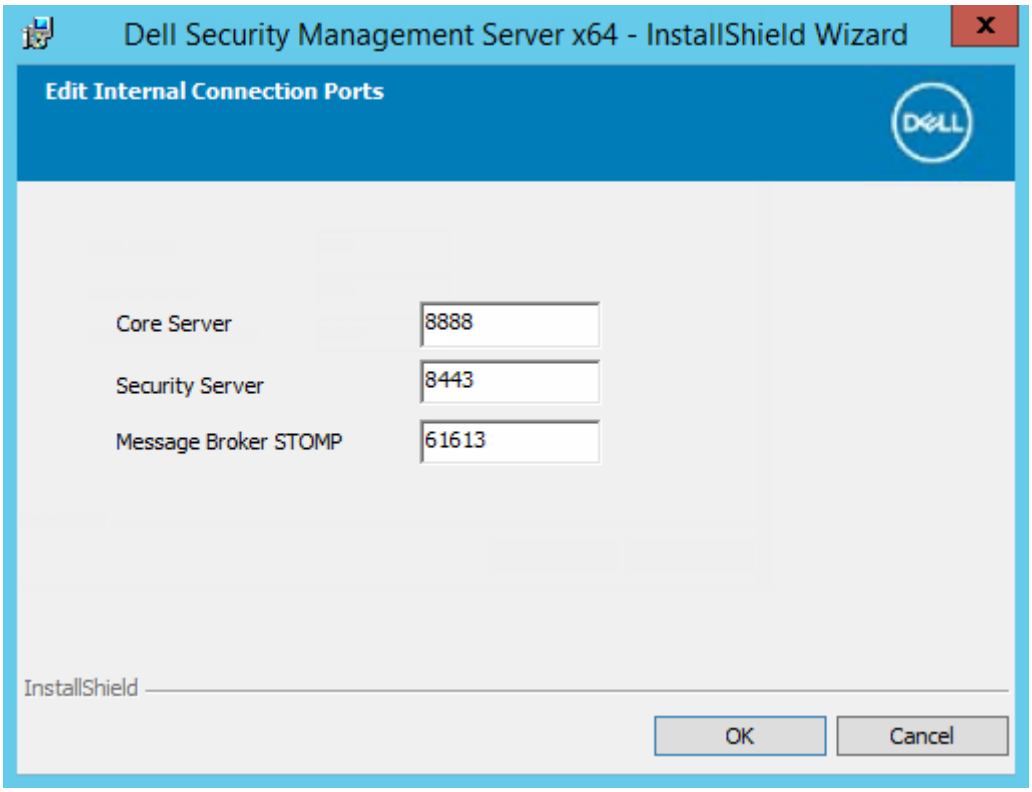


- 포트를 보거나 편집하려면 *프론트 엔드 서버 설정* 대화상자에서 **외부 연결 포트 편집** 또는 **내부 연결 포트 편집**을 클릭합니다. 필요한 경우에만 포트를 편집합니다. 기본값 사용을 권장합니다.

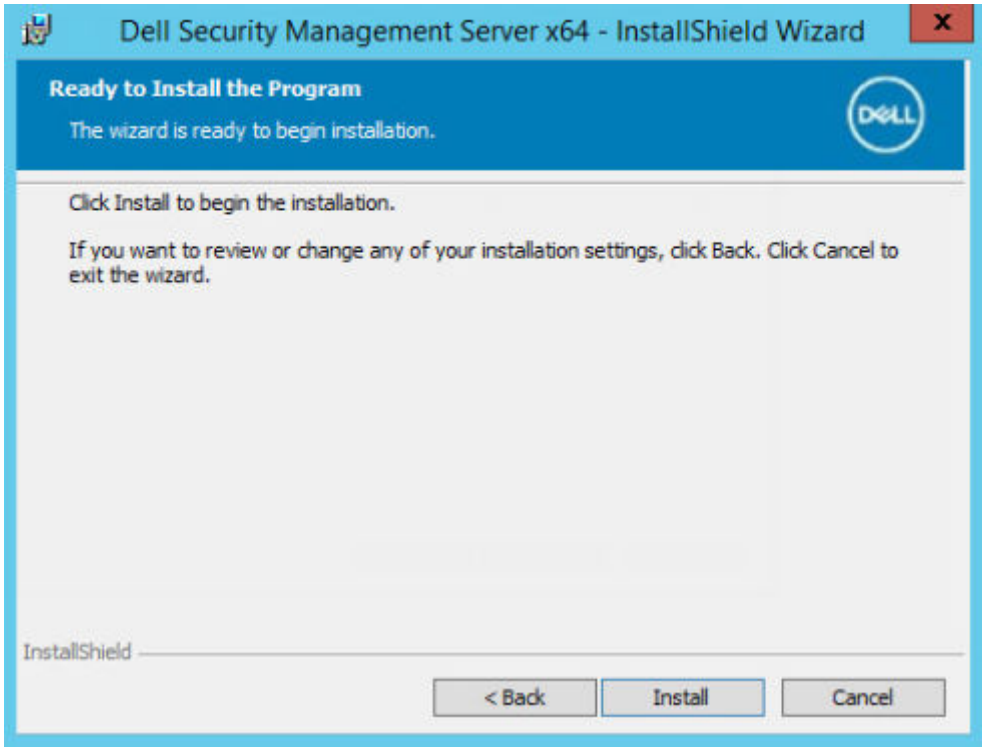
  프론트 엔드 호스트 이름 편집 대화상자에서 프록시를 선택 취소하면 외부 포트 또는 내부 포트 대화상자에 해당 포트가 표시되지 않습니다.

  작업을 마친 후 **확인**을 클릭합니다.

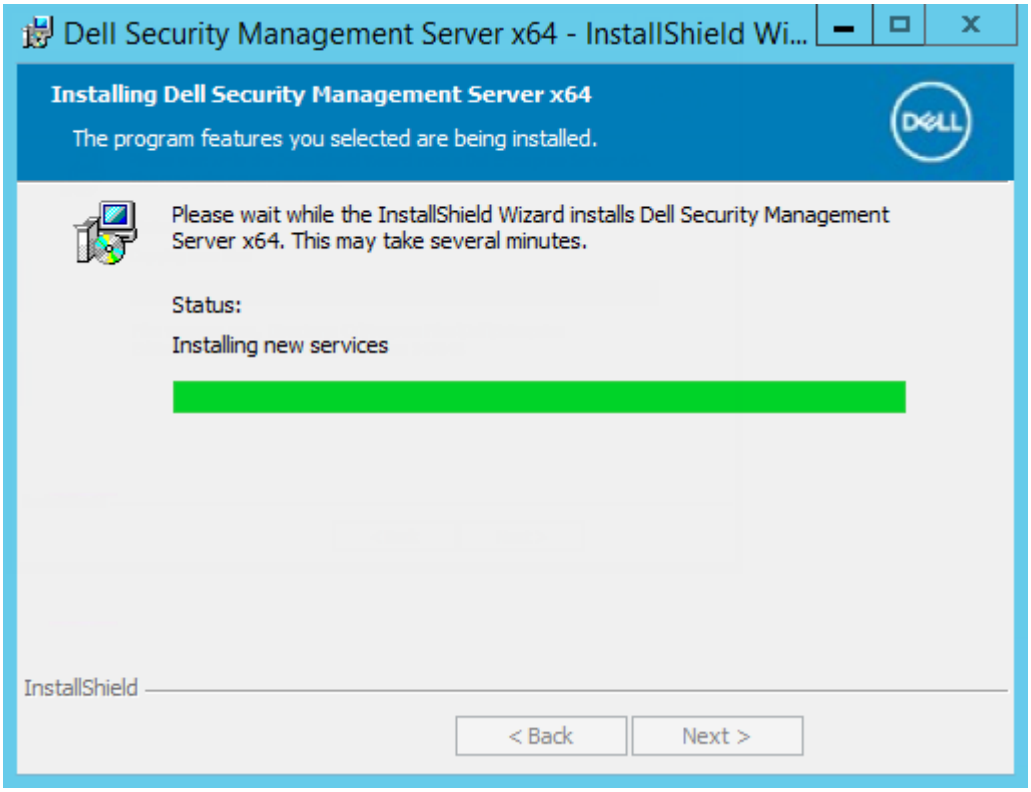




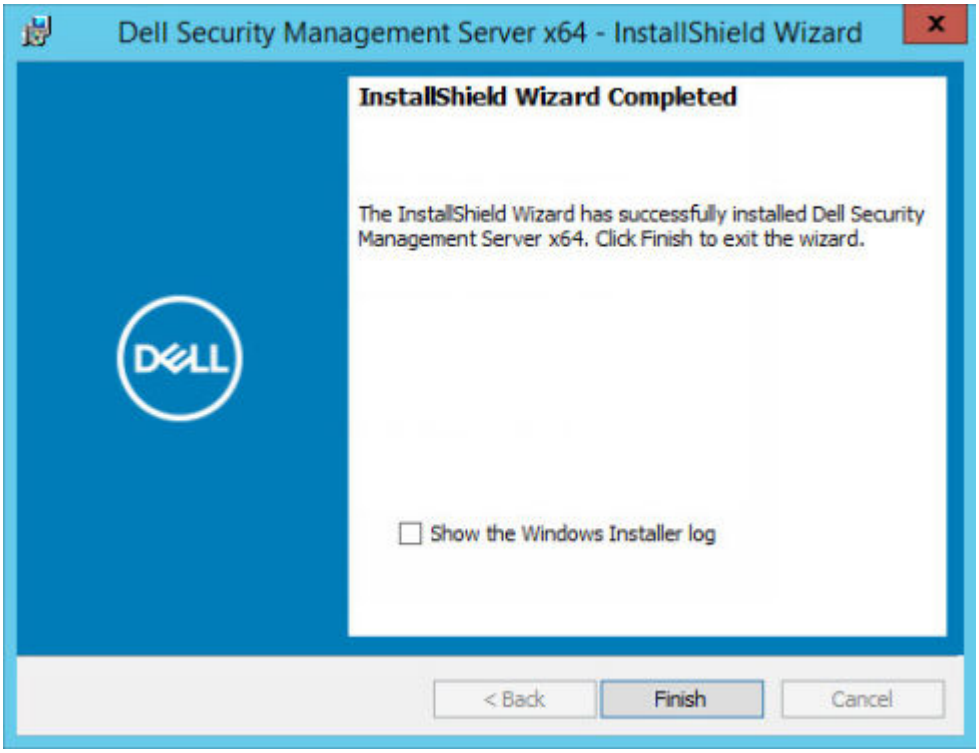
13. *프로그램 설치 준비 완료* 대화상자에서 **설치**를 클릭합니다.



진행률 대화상자에 설치 과정 상태가 표시됩니다.



14. 설치가 완료되면 **마침**을 클릭합니다.



프론트 엔드 서버 설치 작업이 완료됩니다.

업그레이드/마이그레이션

Enterprise Server v9.2 이상을 Security Management Server v10.x로 업그레이드할 수 있습니다. Dell Server 버전이 v9.2 보다 오래된 경우, 먼저 v9.2로 업그레이드한 다음 최신 버전으로 업그레이드해야 합니다.

업그레이드/마이그레이션을 시작하기 전에

시작하기 전에 모든 사전 설치 구성이 완료되었는지 확인하십시오.

Security Management Server 설치와 관련된 모든 최신 해결 방법이나 알려진 문제는 *Security Management Server 기술 권고사항*을 읽어 보십시오.

설치가 수행되는 사용자 계정에는 SQL 데이터베이스에 대해 데이터베이스 소유자 권한이 있어야 합니다. 액세스 권한이나 데이터베이스와의 연결에 대해 잘 모르는 경우에는 설치를 시작하기 전에 데이터베이스 관리자에게 문의하여 확인하시기 바랍니다.

Dell Server 데이터베이스에 데이터베이스 모범 사례를 사용하고 조직의 재해 복구 계획에 Dell 소프트웨어를 포함시킬 것을 권장합니다.

DMZ에 Dell 구성요소를 배포하려면, 구성요소가 공격으로부터 적절히 보호를 받을 수 있는지 확인해야 합니다.

프로덕션 환경의 경우, SQL Server를 전용 서버에 설치할 것을 권장합니다.

정책의 최대 성능을 활용하기 위해, Dell은 Security Management Server와 클라이언트 모두 가장 최신 버전으로 업데이트할 것을 권장합니다.

Security Management Server v10.x는 다음을 지원합니다.

- Encryption Enterprise:
  - Windows 클라이언트 v8.x/v10.x
  - Mac 클라이언트 v8.x/v10.x
  - SED Management v8.x/v10.x
  - BitLocker Manager v8.x/10.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprisev1.x/v2.x

- Security Management Server v9.2 이상에서 업그레이드/마이그레이션 (v9.2 이전 Security Management Server에서 마이그레이션 하는 경우, Dell ProSupport에 연락하여 도움을 요청합니다.)

사용자의 Security Management Server를 새 정책이 처음 도입되는 버전으로 업그레이드/마이그레이션할 경우, 새 정책에 기본값이 아닌 사용자가 선호하는 정책 설정을 적용하기 위해 업그레이드/마이그레이션 이후에 업데이트된 정책을 커밋하십시오.

일반적으로 권장되는 업그레이드 경로는 Security Management Server와 그 구성요소들을 업그레이드/마이그레이션한 후에 클라이언트 설치/업그레이드를 수행하는 것입니다.

정책 변경사항 적용

1. Dell 관리자 계정으로 Management Console에 로그인합니다.
2. 왼쪽 메뉴에서 **관리 커밋**을 클릭합니다.
3. *주석*에서 변경에 대한 설명을 입력합니다.
4. **정책 커밋**을 클릭합니다.
5. 커밋이 완료되면, Management Console에서 로그아웃합니다.

   Dell 서비스가 실행 중인지 확인

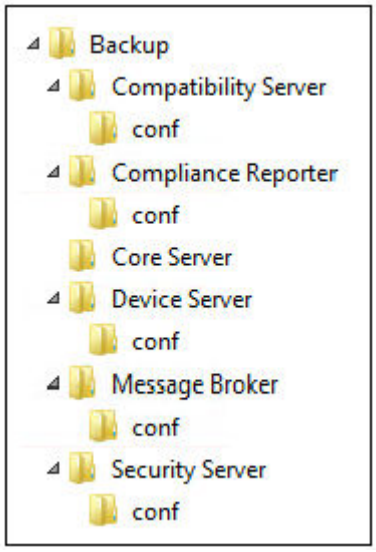
6. Windows *시작* 메뉴에서 **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *Services*가 열리면 각 Dell 서비스로 이동하여 필요한 경우 **서비스 시작**을 클릭합니다.

   기존 설치 백업

7. 기존 설치 전체를 대체 위치에 백업하십시오. 백업해야 할 항목은 SQL 데이터베이스, secretKeyStore, 구성 파일입니다. 기존 설치에 포함된 일부 파일은 업그레이드/마이그레이션 프로세스가 완료된 후에 필요합니다.

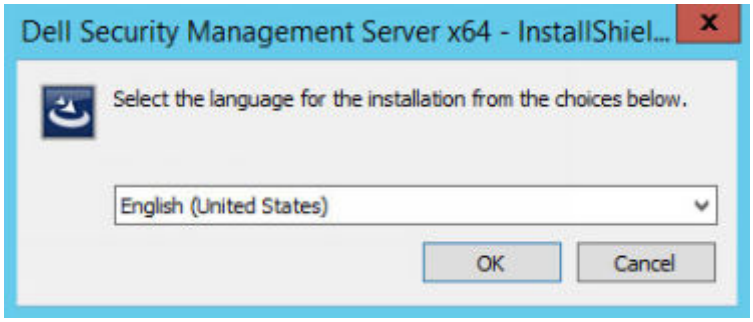
   노트:

   설치 시에 설치 프로그램에서 생성된 폴더 구조(아래 참조)는 그대로 유지해야 합니다.



백엔드 서버 업그레이드/마이그레이션

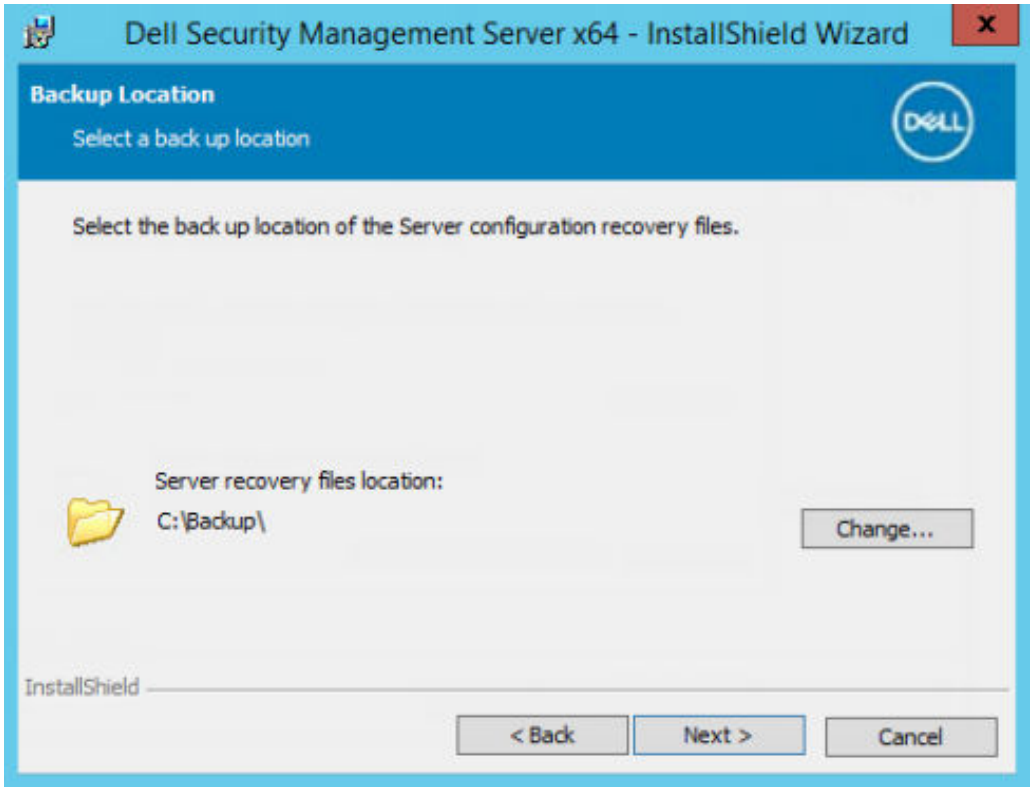
1. Dell 설치 미디어에서 Security Management Server 디렉터리로 이동합니다. Security Management Server-x64를 Security Management Server를 설치할 서버의 루트 디렉터리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭은 안 됨). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. 설치할 언어를 선택하고 **확인**을 클릭합니다.



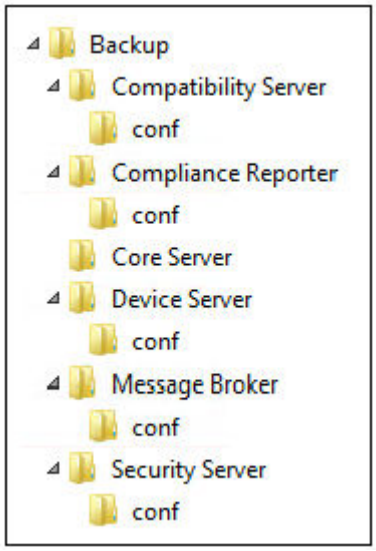
4. *시작* 대화상자에서 **다음**을 클릭합니다.

5. 라이센스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.

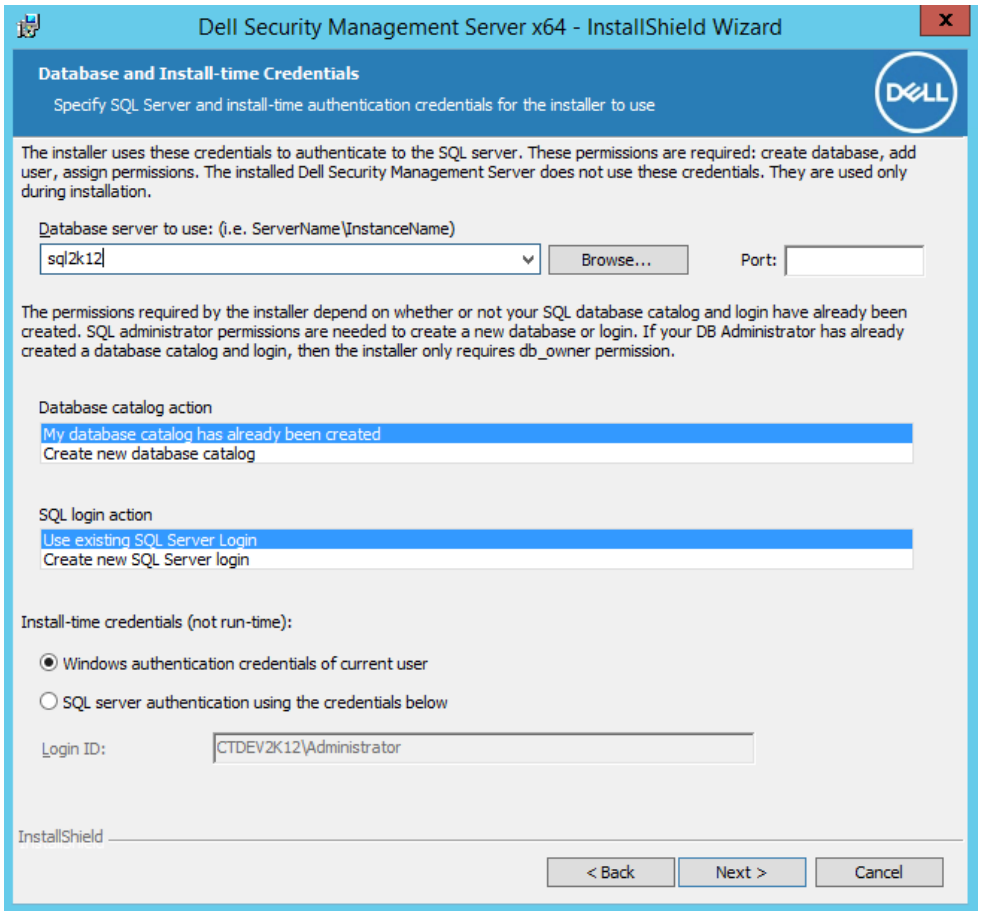
6. 백업 구성 파일을 저장할 위치를 선택하려면, **변경**을 클릭하여 원하는 폴더로 이동하고 **다음**을 클릭합니다.
   원격 네트워크 위치 또는 외부 드라이브를 백업 위치로 선택하는 것이 좋습니다.



   설치 시에 설치 프로그램에서 생성된 폴더 구조(아래 예제 참조)는 그대로 유지해야 합니다.



7. 설치 프로그램이 이전 데이터베이스를 제대로 찾으면 대화상자가 알아서 채워집니다.



기존 데이터베이스에 연결하려면 사용할 인증 방법을 지정합니다. 설치한 이후, 설치된 제품은 여기에 특정된 자격 증명을 사용하지 않습니다.

a. 데이터베이스 인증 유형을 선택합니다.

- **현재 사용자의 Windows 인증 자격 증명**

  Windows 인증을 선택하면 Windows에 로그인하는 데 사용한 자격 증명이 인증에 사용됩니다(*사용자 이름* 및 *암호*는 수정할 수 없음).

  해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.

또는

- **다음 자격 증명을 사용해 SQL 서버 인증**

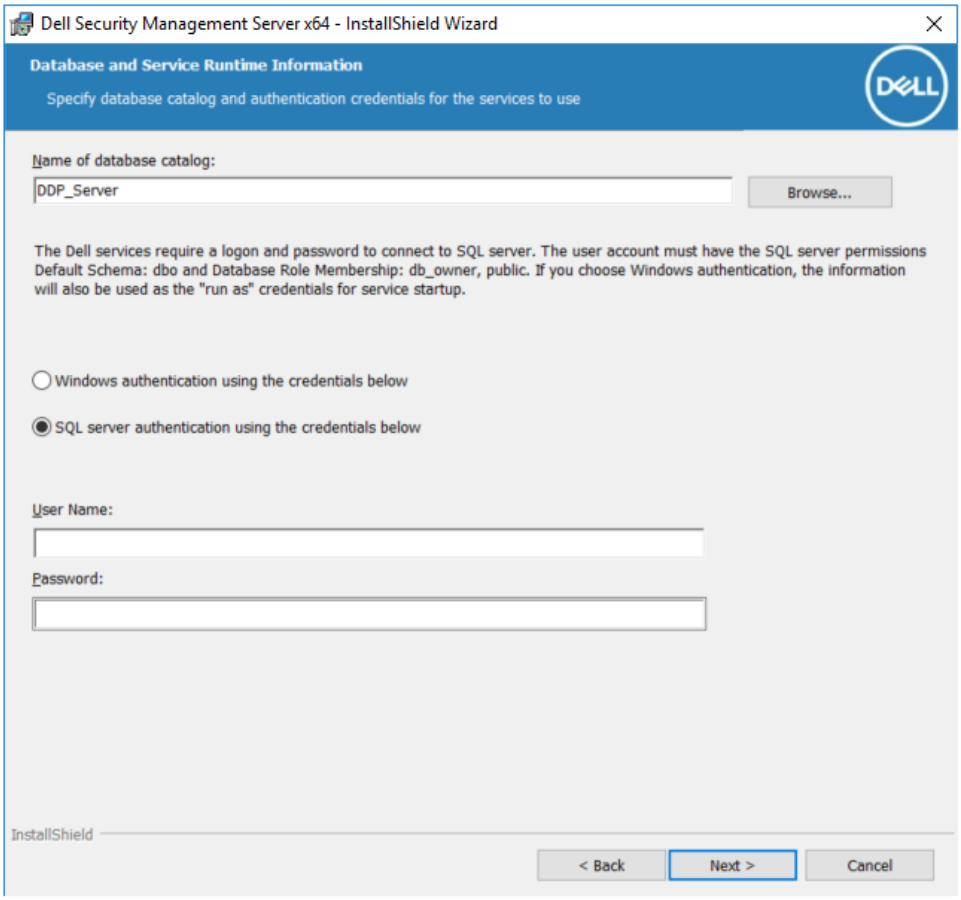
  SQL 인증을 사용하려면 사용되는 SQL 계정에 SQL 서버에 대한 시스템 관리자 권한이 있어야 합니다.

  설치 프로그램은 이 허가를 통해 SQL 서버에 인증해야 합니다: 데이터베이스 생성, 사용자 추가, 허용 할당.

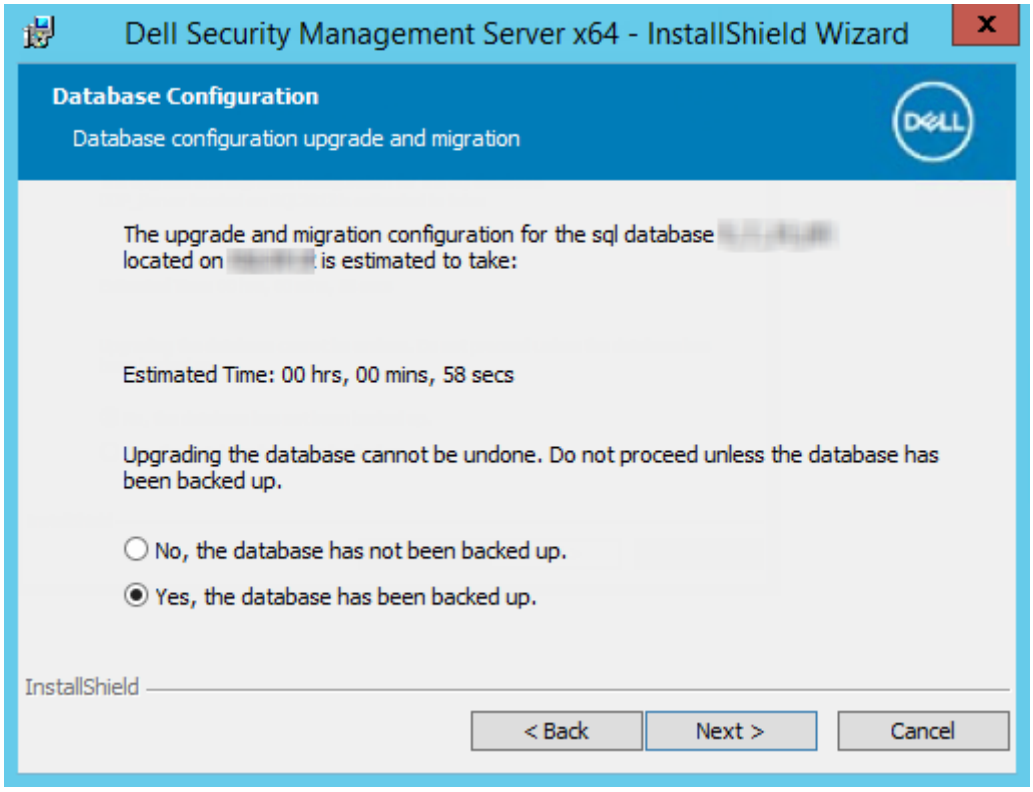
b. **다음**을 클릭합니다.

8. 서비스 런타임 계정 정보 대화 상자가 채워져 있지 않으면 설치 후에 제품에서 사용할 인증 방법을 지정합니다.
   a. 인증 유형을 선택합니다.
   b. Dell 서비스가 SQL Server에 액세스할 때 사용할 도메인 서비스 계정의 사용자 이름과 암호를 입력한 뒤 **다음**을 클릭합니다.

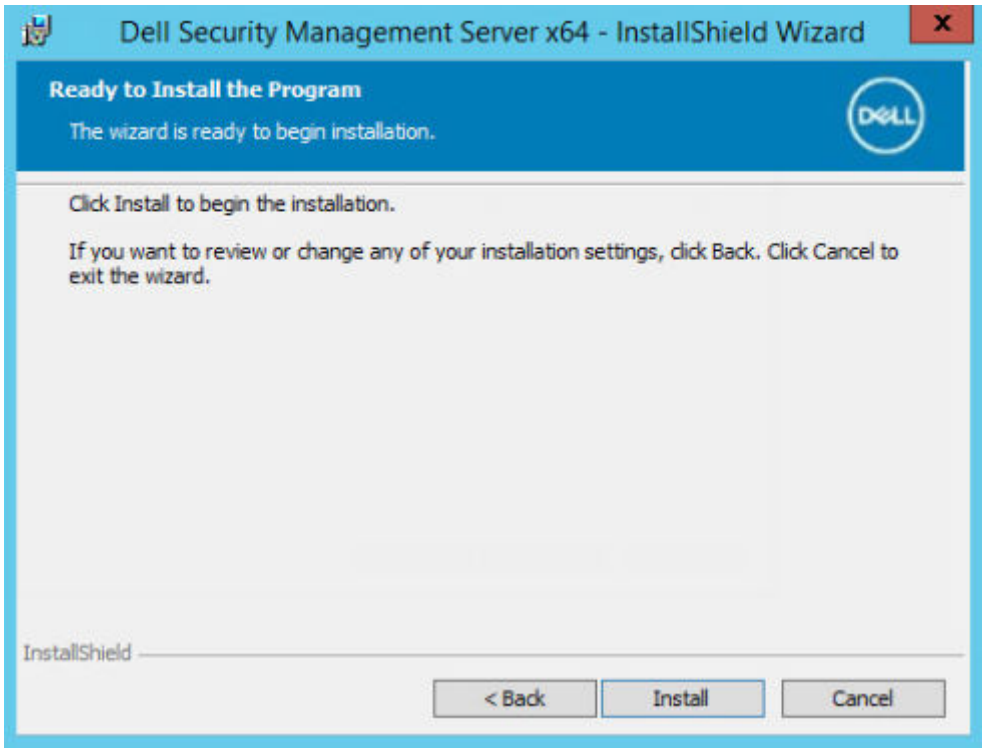
   사용자 계정은 DOMAIN\\Username 형식이어야 하며 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다.



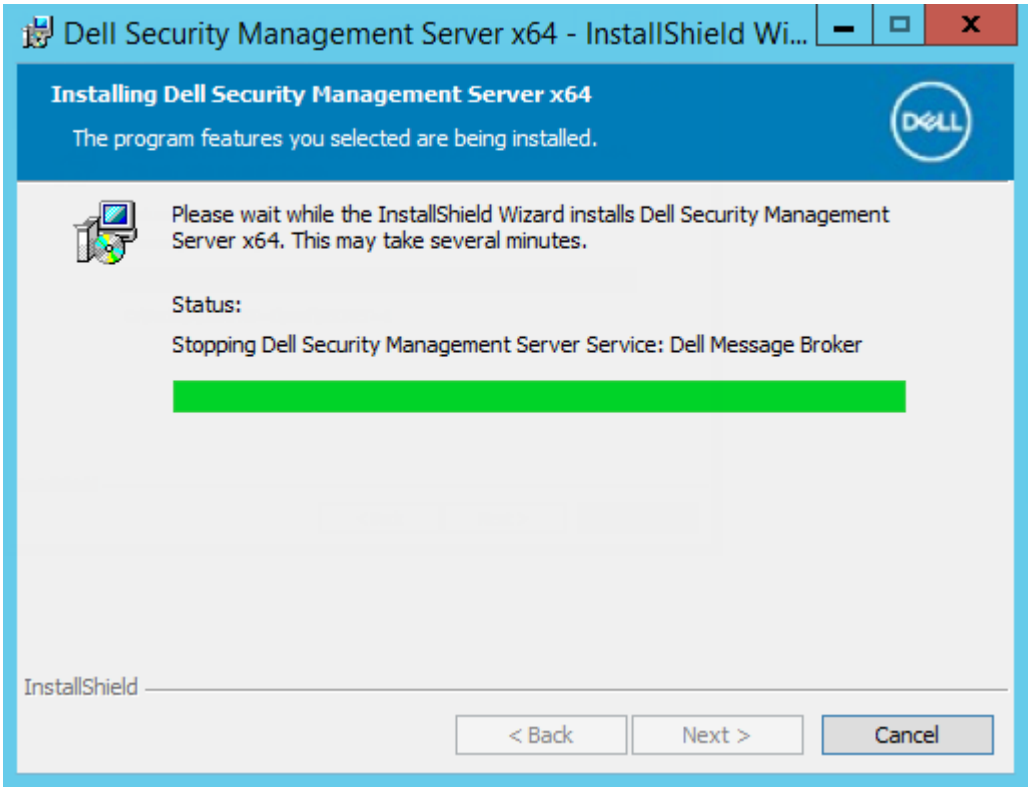
9. 설치를 계속하기 전에 데이터베이스를 ***반드시*** 백업해야 합니다. ***데이터베이스 업그레이드는 롤백할 수 없습니다.*** 데이터베이스가 백업된 뒤에만 **예, 데이터베이스가 백업되었습니다**를 선택하고 **다음**을 클릭합니다.



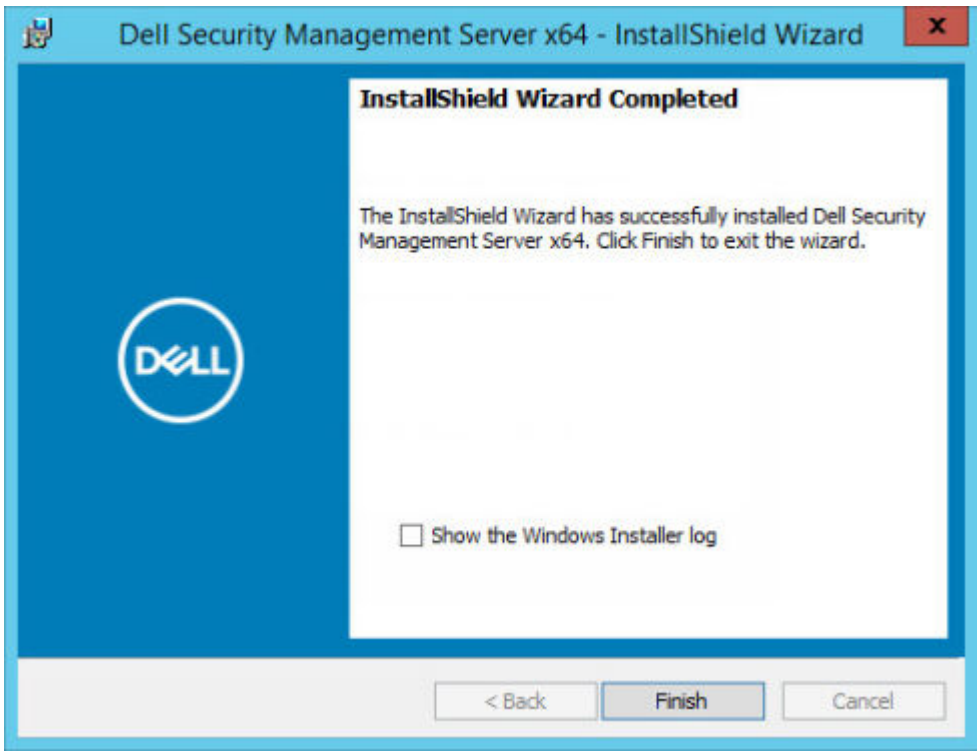
10. **설치**를 클릭하고 설치를 시작합니다.



진행률 대화상자에 업그레이드 과정 상태가 표시됩니다.



11. 설치가 완료되면 **마침**을 클릭합니다.



마이그레이션이 끝나면 Dell 서비스가 다시 시작됩니다. Dell Server를 다시 부팅할 필요는 없습니다.

설치 프로그램이 12~13단계를 알아서 수행합니다. 변경 사항이 올바르게 적용되었는지 보려면 이 값을 확인하는 것이 좋습니다.

12. 백업해 놓은 설치 정보에서, <Compatibility Server 설치 디렉터리>\conf\secretKeyStore를 새 설치 정보 <Compatibility Server 설치 디렉터리>\conf\secretKeyStore에 복사하여 붙여넣습니다.

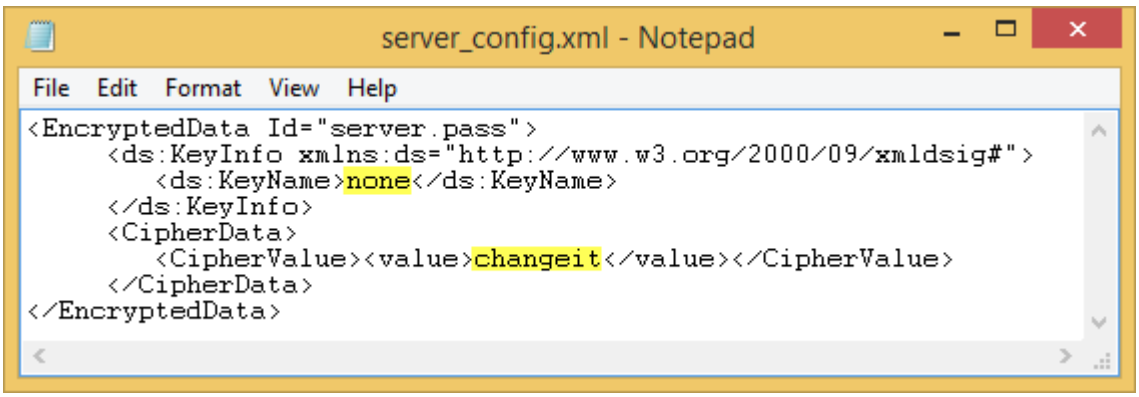
13. 새 설치에서, <Compatibility Server 설치 디렉터리>\conf\server_config.xml을 열고 **server.pass** 값을 다음과 같이 백업된 <Compatibility Server 설치 디렉터리>\conf\server_config.xml의 값으로 교체합니다.

server.pass에 대한 지침:

암호를 알고 있는 경우, 의 견본 server_config.xml 파일을 참조하여 다음과 같이 수정하십시오.

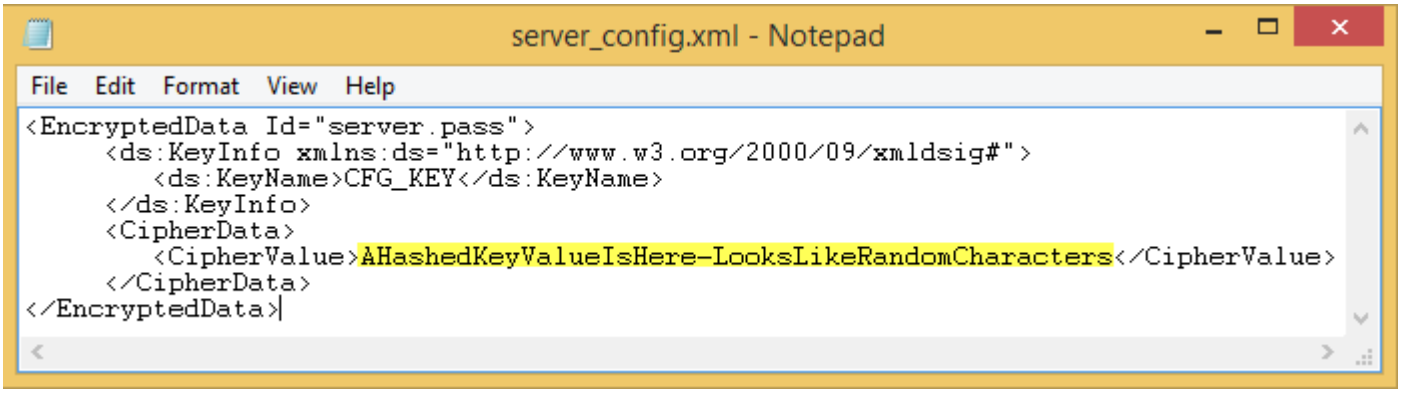
- *KeyName*을 **CFG_KEY** 값에서 **none으로 편집합니다.**
- 일반 텍스트 암호를 입력하고 이를 *<value> </value>*로 묶습니다. 이 예에서는 **<value>changeit</value>**과 같습니다.
- Security Management Server가 시작되면, 일반 텍스트 암호가 해시되고 이 해시값이 일반 텍스트를 대체합니다.

암호를 알 경우



암호를 모르는 경우, 백업된 <Compatibility Server install dir>\conf\server_config.xml 파일에서 그림 4-2에 표시된 부분과 유사한 부분을 잘라내서 새 *server_config.xml* 파일의 해당 부분에 붙여 넣습니다.

암호를 모를 경우



파일을 저장하고 닫습니다.

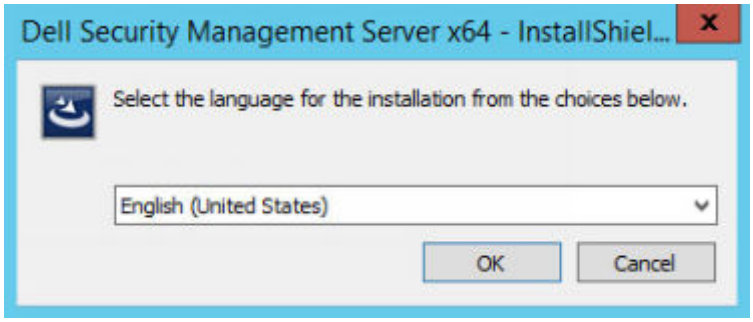
노트:

나중에라도 server_config.xml의 server.pass 값을 편집하여 Security Management Server 암호를 변경하려 하지 마십시오. 이 값을 변경하면, 데이터베이스에 대한 액세스 권한을 잃습니다.

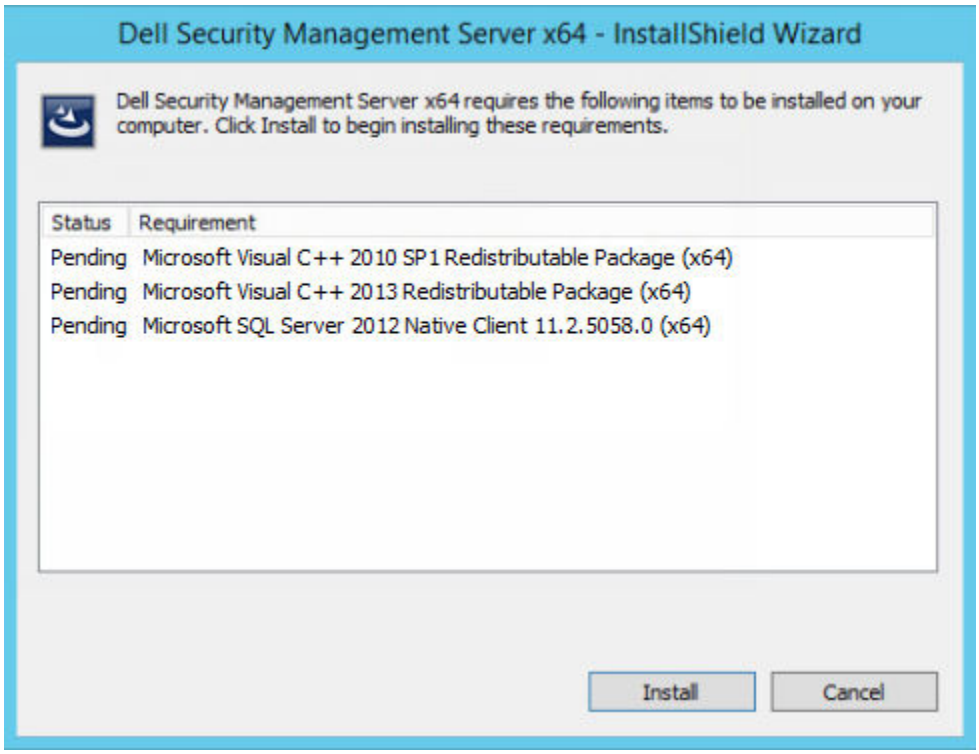
백엔드 서버 마이그레이션 작업이 완료됩니다.

프론트 엔드 서버 업그레이드/마이그레이션

1. Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server를 설치할 서버의 루트 디렉터리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭은 안 됨). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. 설치할 언어를 선택하고 **확인**을 클릭합니다.

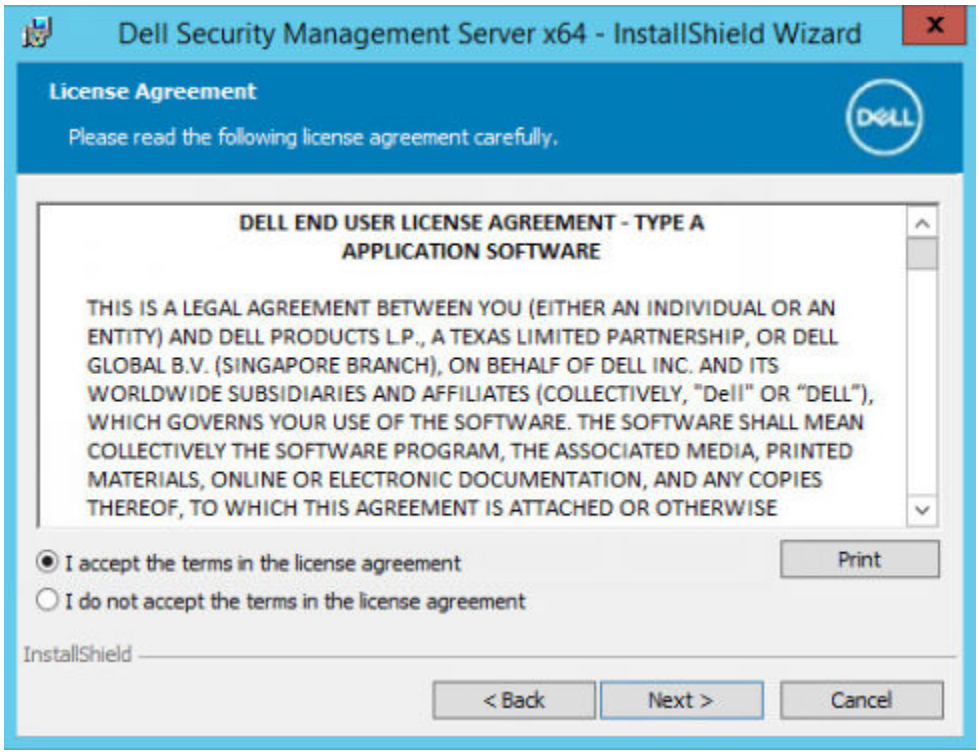


4. 사전 요구 사항이 아직 설치되어 있지 않으면, 사전 요구 사항이 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.

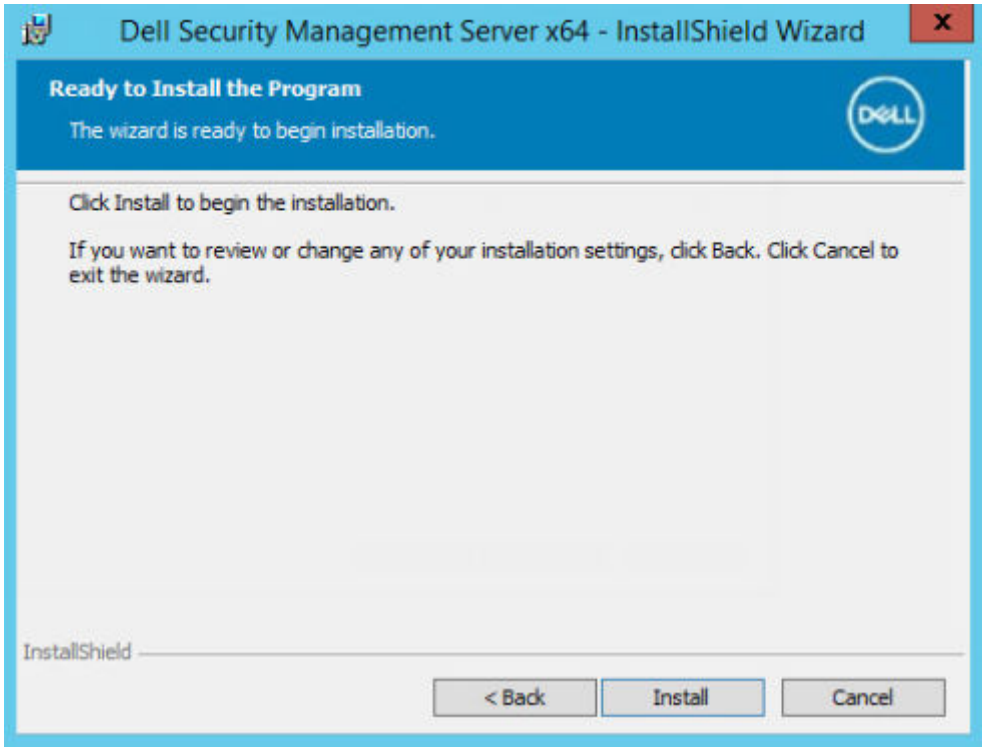


5. *시작* 대화상자에서 **다음**을 클릭합니다.

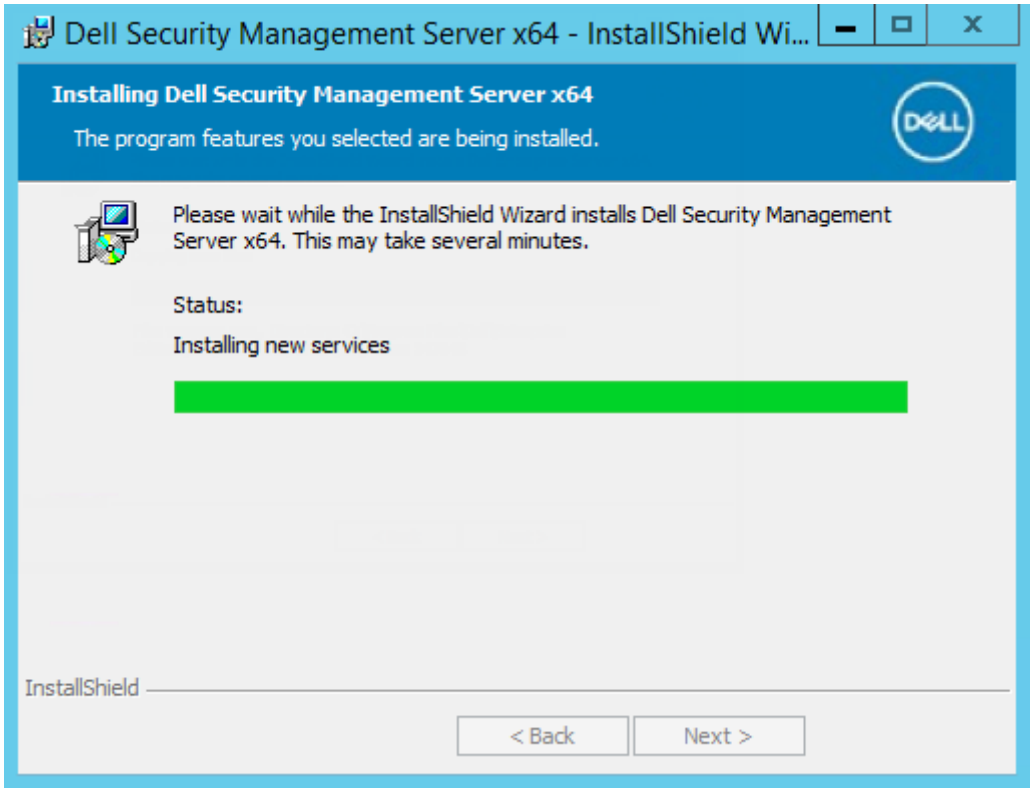
6. 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.



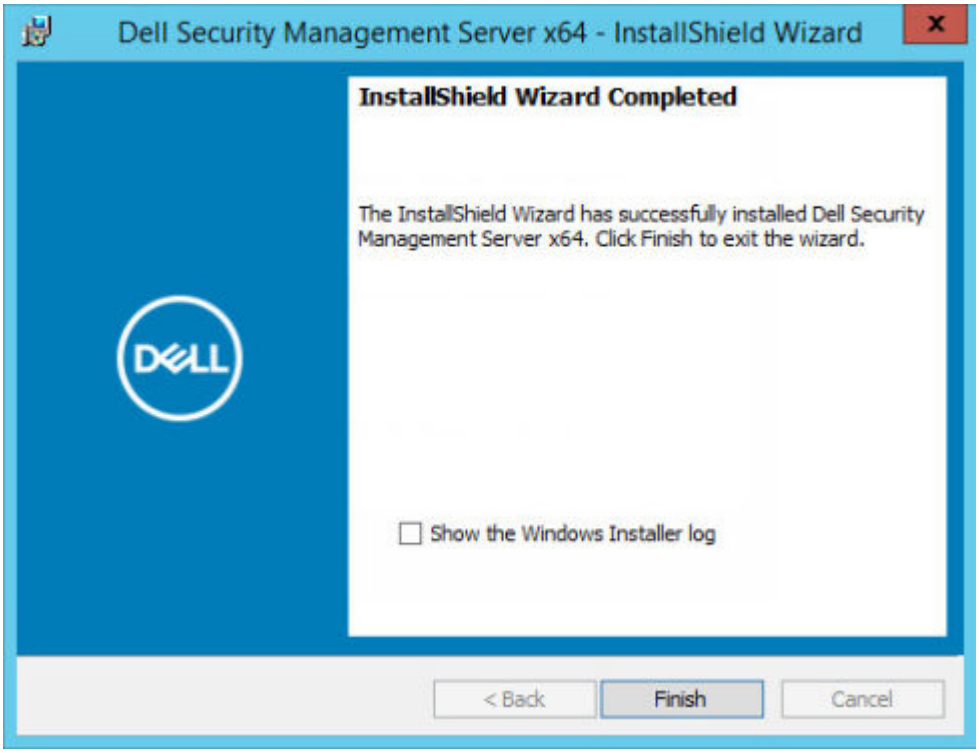
7. *프로그램 설치 준비 완료* 대화상자에서 **설치**를 클릭합니다.



진행률 대화상자에 설치 과정 상태가 표시됩니다.



8. 설치가 완료되면 **마침**을 클릭합니다.



9. 프론트엔드 서버와 통신하도록 백엔드 서버를 설정합니다.
   a. 백엔드 서버에서 <Security Server install dir>\conf\로 이동하고 application.properties 파일을 엽니다.
   b. publicdns.server.host를 찾아서 외부에서 확인 가능한 호스트 이름에 이름을 설정합니다.
   c. publicdns.server.port를 찾아서 포트를 설정합니다(기본값은 8443).

   설치가 끝나면 Dell 서비스가 다시 시작됩니다. 설치 후 구성 작업이 완료될 때까지 Dell Server를 다시 부팅할 필요가 없습니다.

연결되지 않은 모드 설치

연결되지 않은 모드는 인터넷과 보호되지 않은 LAN 또는 기타 네트워크에서 Security Management Server를 격리합니다. Security Management Server가 연결되지 않은 모드로 설치된 후에는 계속 연결되지 않은 모드를 유지하며 연결된 모드로 돌아갈 수 없습니다.

명령줄에서 연결되지 않은 모드로 Security Management Server를 설치합니다.

다음 표에는 이용할 수 있는 스위치가 나와 있습니다.

스위치	의미
/v	변수를 *.exe 내의 .msi로 전달
/s	자동 모드

다음 표에는 사용할 수 있는 디스플레이 옵션이 나와 있습니다.

옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	**취소** 단추가 있는 진행률 대화 상자
/qn	사용자 인터페이스 없음

다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다. 이러한 매개 변수는 명령줄에서 지정할 수도 있고 다음과 같이 속성을 사용하여 파일에서 호출할 수도 있습니다.

INSTALL_VALUES_FILE=\"<file_path>\" "

매개 변수
AGREE_TO_LICENSE=Yes - 이 값은 "Yes"가 되어야 합니다.
PRODUCT_SN=xxxxx - 표준 위치에 라이센스 정보가 있으면 선택 사항입니다. 그렇지 않으면 여기에 입력합니다.
INSTALLDIR=<path> - 선택 사항.
BACKUPDIR=<path> - 복구 파일이 저장되는 위치입니다. **노트:** 이 설치 단계 중에는 설치 프로그램에서 생성된 폴더 구조(아래 예제 참조)를 그대로 유지해야 합니다.
AIRGAP=1 - Security Management Server를 연결되지 않은 모드로 설치하려면 이 값이 "1"이 되어야 합니다.
SSL_TYPE=n - 여기에서 n이 1이면 CA 기관에서 구매한 기존의 인증서를 가져오는 것이고 2이면 자체 서명 인증서를 만드는 것입니다. SSL_TYPE 값으로 어떤 SSL 속성이 필요한지를 결정합니다. SSL_TYPE=1일 때 다음과 같은 사항이 필요합니다. SSL_CERT_PASSWORD=xxxxx SSL_CERT_PATH=xxxxx SSL_TYPE=2일 때 다음과 같은 사항이 필요합니다. SSL_CITYNAME SSL_DOMAINNAME SSL_ORGNAME SSL_UNITNAME SSL_COUNTRY - 선택 사항, 기본값 = "US" SSL_STATENAME
SSOS_TYPE=n - 여기에서 n이 1이면 CA 기관에서 구매한 기존의 인증서를 가져오는 것이고 2이면 자체 서명 인증서를 만드는 것입니다. SSOS_TYPE 값으로 어떤 SSOS 속성이 필요한지를 결정합니다. SSOS_TYPE=1일 때 다음과 같은 사항이 필요합니다. SSOS_CERT_PASSWORD=xxxxx SSOS_CERT_PATH=xxxxx SSOS_TYPE=2일 때 다음과 같은 사항이 필요합니다. SSOS_CITYNAME SSOS_DOMAINNAME SSOS_ORGNAME SSOS_UNITNAME SSOS_COUNTRY - 선택 사항, 기본값 = "US" SSOS_STATENAME
DISPLAY_SQLSERVER - 이 값의 구문을 분석하여 SQL Server 인스턴스 및 포트 정보를 얻습니다. 예: DISPLAY_SQLSERVER=SQL_server\Server_instance, port
IS_AUTO_CREATE_SQLSERVER=FALSE - 선택 사항. 기본값은 FALSE이며 데이터베이스가 생성되지 않는다는 것을 의미합니다. 데이터베이스가 서버에 이미 있어야 합니다. 새 데이터베이스를 생성하려면 이 값을 TRUE로 설정합니다.
IS_SQLSERVER_AUTHENTICATION=0 - 선택 사항. 기본값은 0이며 현재 로그온한 사용자의 인증 자격 증명을 사용하여 SQL Server에 대한 인증을 한다는 것을 지정합니다. SQL 인증을 사용하려면 이 값을 1로 설정합니다.

매개 변수
노트: 설치 프로그램은 이 허가를 통해 SQL 서버에 인증해야 합니다: 데이터베이스 생성, 사용자 추가, 허용 할당. 자격 증명은 설치 시간 자격 증명이며 실행 시간 자격 증명이 아닙니다. SQL 인증을 사용하는 경우에는 다음이 필요합니다. IS_SQLSERVER_USERNAME IS_SQLSERVER_PASSWORD
EE_SQLSERVER_AUTHENTICATION - 필수. 사용할 제품에 대한 인증 방법을 지정합니다. 이 단계는 제품에 계정을 연결합니다. 또한 이 자격 증명은 Security Management Server에서 작업할 때 Dell 서비스에서 사용됩니다. Windows 인증을 사용하려면 이 값을 0으로 설정합니다. SQL 인증을 사용하려면 이 값을 1로 설정합니다. **노트:** 해당 계정에 시스템 관리자 권한 및 SQL Server를 관리할 수 있는 기능이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 Database Role Membership: dbo_owner, public을 가지고 있어야 합니다. SQL_EE_USERNAME - 필수. Windows 인증에서는 DOMAIN\Username 형식을 사용합니다. SQL 인증에서는 사용자 이름을 지정합니다. SQL_EE_PASSWORD - 필수. Windows 또는 SQL 사용자 이름과 연관된 암호를 지정합니다. SQL 인증을 사용하는 경우(EE_SQLSERVER_AUTHENTICATION=1)에는 다음과 같은 사항이 유효합니다. RUNAS_KEYSERVER_USER - Key Server를 Domain\User 형식의 Windows 사용자 이름"으로 실행"으로 설정합니다. Windows 사용자 계정을 사용해야 합니다. RUNAS_KEYSERVER_PSWD - Key Server를 Windows 사용자 계정과 연관된 Windows 암호"로 실행"으로 설정합니다.
SQL_ADD_LOGIN=T - 선택 사항. 기본값은 null입니다(이 로그인이 추가되지 않습니다). 이 값이 T로 설정될 때 SQL_EE_USERNAME이 데이터베이스에 대한 로그인이나 사용자가 아닐 경우, 설치 프로그램은 사용자의 SQL 인증 자격 증명을 추가하고 제품에서 자격 증명을 사용할 수 있도록 권한을 설정하려고 할 것입니다.
다음은 호스트 이름 매개변수입니다. 필요한 경우에만 호스트 이름을 편집합니다. 기본값 사용을 권장합니다. **server.domain.com** 형식을 사용해야 합니다. **노트:** 호스트 이름에는 밑줄("_")을 사용할 수 없습니다.
CORESERVERHOST - 선택 사항. Core Server 호스트 이름.
RMIHOST - 선택 사항. Compatibility Server 호스트 이름.
REPORTERHOST - 선택 사항. Compliance Reporter 호스트 이름.
DEVICEHOST - 선택 사항. Device Server 호스트 이름.
KEYSERVERHOST - 선택 사항. Key Server 선택 사항.
TIGAHOST - 선택 사항. Security Server 호스트 이름.
SMTP_HOST - 선택 사항. SMTP 호스트 이름.
ACTIVEMQHOST - 선택 사항. Message Broker 호스트 이름.
다음은 포트 매개변수입니다. 필요한 경우에만 포트를 편집합니다. 기본값 사용을 권장합니다.
SERVERPORT_CLIENTAUTH - 선택 사항.
REPORTERPORT - 선택 사항.
DEVICEPORT - 선택 사항.
KEYSERVERPORT - 선택 사항.
GKPORT - 선택 사항.

매개 변수
TIGAPORT - 선택 사항.
SMTP_PORT - 선택 사항.
ACTIVEMQ_TCP - 선택 사항.
ACTIVEMQ_STOMP - 선택 사항.

연결되지 않은 모드로 Security Management Server 설치

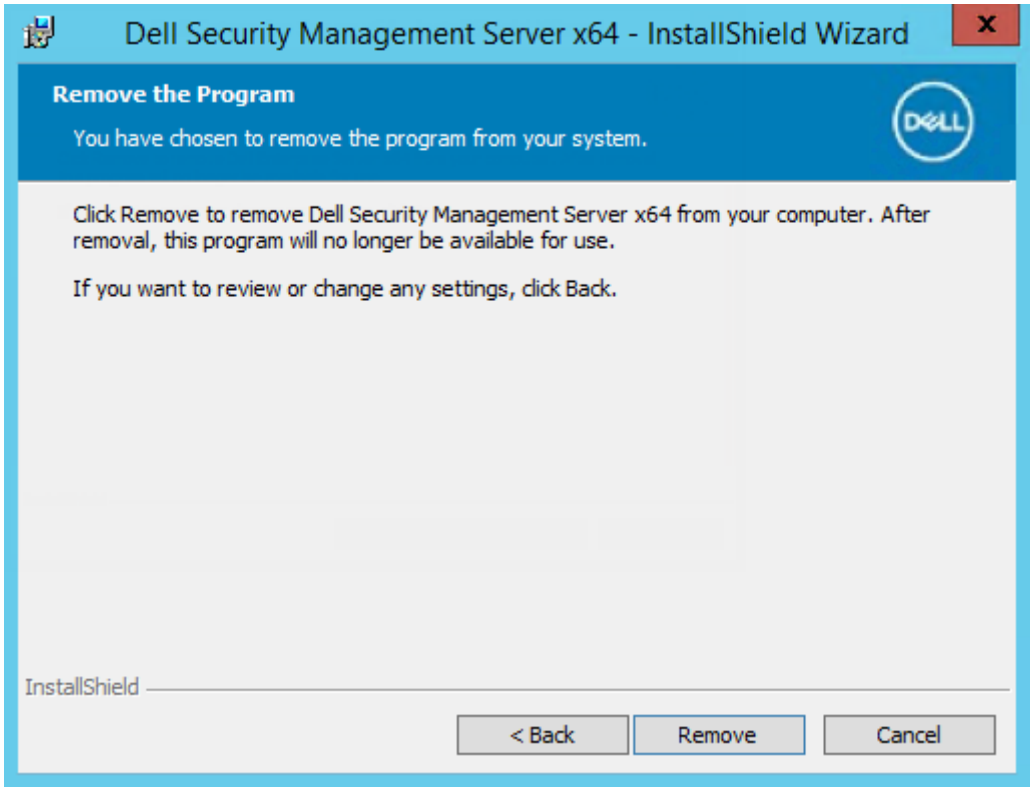
다음 예제에서는 `C:\mysetups\eeoptions.txt\" "` 파일에 나와 있는 설치 매개 변수를 사용하여 진행률 대화 상자가 표시되는 자동 모드로 Security Management Server를 설치합니다.

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

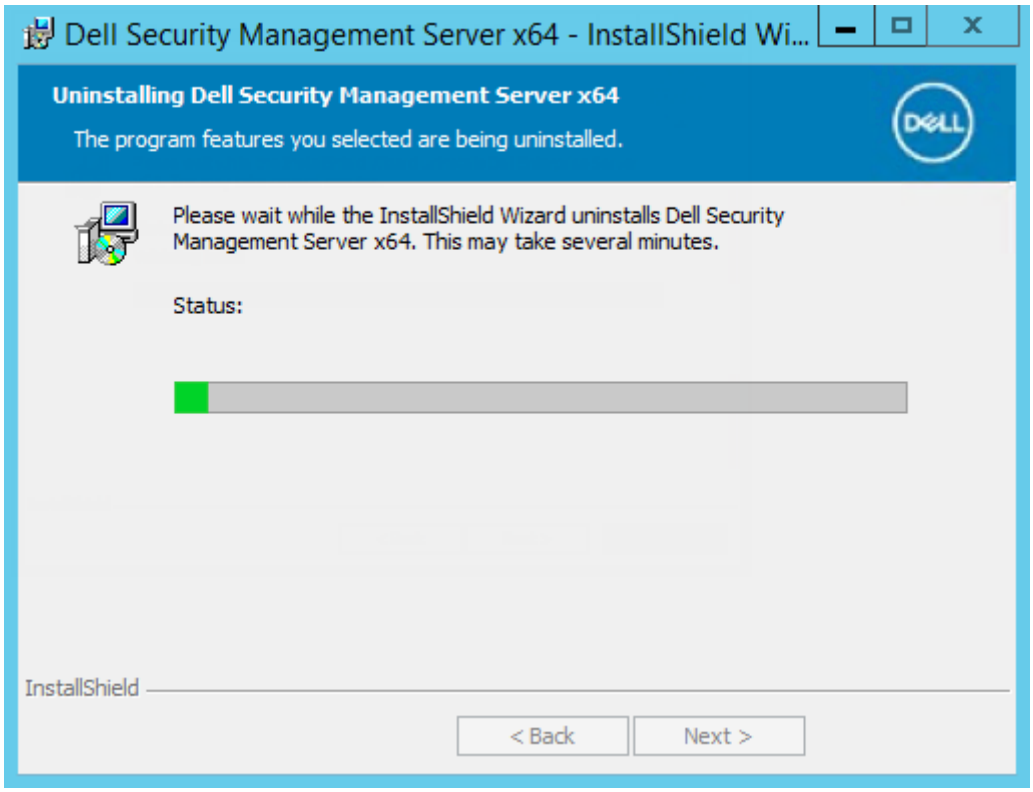
Security Management Server 설치 제거

1. Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server의 설치를 제거할 서버의 루트 디렉터리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2. **setup.exe**를 더블 클릭합니다.
3. *시작* 대화상자에서 **다음**을 클릭합니다.

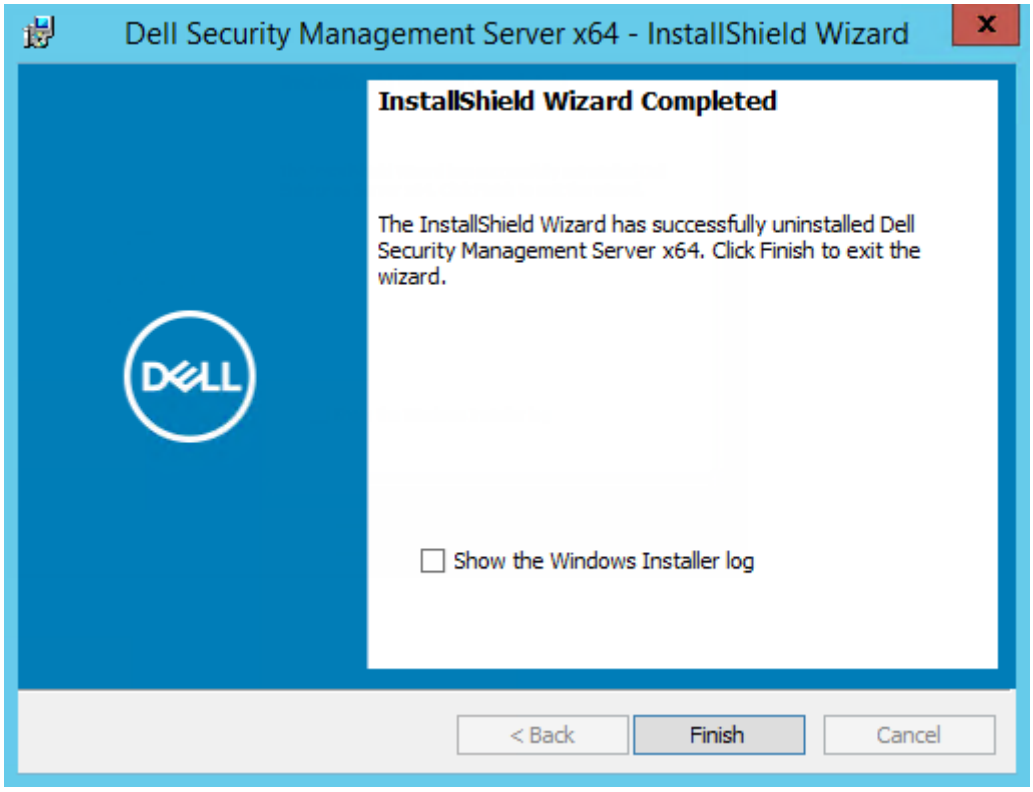
4. *프로그램 제거* 대화상자에서 **제거**를 클릭합니다.



진행률 대화상자에 제거 과정 상태가 표시됩니다.



5. 제거가 완료되면 **마침**을 클릭합니다.


Dell Security Management Server x64 - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully uninstalled Dell Security Management Server x64. Click Finish to exit the wizard.
Show the Windows Installer log
< Back
Finish
Cancel

5

설치 후 구성

Security Management Server 구성과 관련된 최신 해결 방법이나 알려진 문제는 *Security Management Server Technical Advisories*(*Security Management Server 기술 권장 사항*)을 읽어 보십시오.

Security Management Server를 처음으로 설치하든 기존 설치를 업그레이드하든, 환경의 일부 구성 요소를 구성해야 합니다.

Security Management Server를 설치한 후 다음 기본값을 수정해야 합니다.

- 다음 위치에서 백 엔드 서버 암호를 변경합니다.

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- 다음 위치에서 운영 환경의 모든 프런트 엔드 서버에 대한 암호를 변경합니다.

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

암호는 다음과 같이 표시됩니다. `proxy-server.password=ENC(<texthere>)`

암호를 변경하는 방법:

1. 다음을 선택합니다. `ENC(<texthere>)`
2. 선택한 텍스트를 다음으로 변경합니다. `CLR(<newpasswordhere>)`

   서비스가 재시작되면 수정된 행이 `CLR`에서 `ENC`로 변경되고 암호는 암호화됩니다.

참고: proxy-server.username도 수정될 수 있지만 Message Broker의 application.properties 파일 및 모든 활성 프런트 엔드 서버 내에서 일치해야 합니다.

DMZ 모드 구성

Security Server가 DMZ와 개인 네트워크에 배포되고 DMZ 서버에만 신뢰할 수 있는 인증 기관(CA)의 도메인 인증서가 있는 경우, 이 신뢰할 수 있는 인증서를 개인 네트워크 Security Server의 Java 키 저장소에 추가하기 위해 약간의 수동 절차가 필요합니다.

신뢰할 수 있는 인증서를 사용하고 있는 경우, 이 섹션을 생략하고

노트: DMZ와 개인 네트워크 서버 모두에 대해 신뢰할 수 있는 인증 기관의 도메인 인증서를 사용할 것을 강력히 권장합니다.

Microsoft 키 스토리지에서 기존 인증서와 함께 Dell 암호화를 위한 인증서 업데이트에 대한 자세한 내용은 http://www.dell.com/support/article/us/en/19/sln297240/을 참조하십시오.

Server 구성 도구

설치를 완료한 후에 환경에 대한 구성이 필요할 경우 서버 구성 도구를 사용해 변경하십시오.

서버 구성 도구를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- 새 인증서 또는 업데이트된 인증서 추가
- Dell Manager 인증서 가져오기
- ID 인증서 가져오기
- Server SSL 인증서의 설정 구성
- 이메일 서비스용 SMTP 설정 구성
- 데이터베이스 이름, 위치 또는 자격 증명 변경
- 데이터베이스 마이그레이션

  Dell Core Server와 Compatibility Server는 서버 구성 도구와 동시에 실행할 수 없습니다. *서비스*에서 Core Server 서비스와 Compatibility Server 서비스를 중단한 후에(**시작 > 실행**. ***services.msc*** 입력) Server 구성 도구를 시작하십시오.

  서버 구성 도구를 시작하려면 **시작** > **Dell** > **서버 구성 도구 실행**으로 이동합니다.

서버 구성 도구가 `C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs`에 로그를 기록합니다.

새 인증서 또는 업데이트된 인증서 추가

자체 서명된 인증서와 서명된 인증서 중에서 사용할 인증서 유형을 선택할 수 있습니다.

- **자체 서명된** 인증서는 작성자가 서명한 인증서입니다. 자체 서명된 인증서는 파일럿, POC 등에 적합합니다. 프로덕션 환경의 경우, Dell은 공용 CA 서명 또는 도메인 서명 인증서를 권장합니다.
- **서명된**(공용 CA-서명 또는 도메인-서명) 인증서는 공용 CA 또는 도메인이 서명한 인증서입니다. 공용 CA(인증 기관)에서 서명한 인증서의 경우, 일반적으로 서명 CA의 인증서가 Microsoft 인증서 저장소에 이미 있기 때문에 "신뢰 체인"이 자동적으로 수립됩니다. 도메인 CA에서 서명한 인증서의 경우, 워크스테이션이 도메인에 연결되어 있으면 도메인의 서명 CA 인증서가 워크스테이션의 Microsoft 인증서 저장소에 추가되므로 역시 "신뢰 체인"이 생성됩니다.

인증서 구성으로 영향을 받는 구성 요소:

- Java 서비스(예: Device Server 등)
- .NET 애플리케이션(Core Server)
- 부팅 전 인증을 위해 사용하는 스마트 카드의 유효성 검사(Security Server)
- Dell Manager로 보내는 정책 번들에 서명할 때 사용할 개인 암호화 키 가져오기 Dell Manager는 자체 암호화 드라이브 또는 BitLocker Manager가 탑재된 관리되는 암호화 클라이언트에 대해 SSL 유효성을 검사합니다.
- 클라이언트 워크스테이션:
  - BitLocker Manager를 실행하는 워크스테이션
  - Encryption Enterprise를 실행하는 워크스테이션(Windows)
  - Endpoint Security Suite Enterprise를 실행하는 워크스테이션

사용할 인증서 유형과 관련된 정보:

스마트 카드를 사용해 부팅 전 인증을 실행하려면 Security Server로 SSL 유효성을 검사해야 합니다. Dell Manager가 Dell Core Server에 연결할 때 SSL 유효성 검사를 수행합니다. 이러한 연결 유형에서는 서명 CA가 키 저장소(Dell Server 구성 요소에 따라 Java 키 저장소 또는 Microsoft 키 저장소)에 있어야 합니다. 자체 서명 인증서가 채택된 경우, 다음 옵션이 사용 가능합니다:

- 부팅 전 인증에 사용되는 스마트 카드의 유효성 검사 방법:
  - "Root Agency" 서명 인증서와 전체 신뢰 체인을 Security Server Java 키 저장소로 가져옵니다. 전체 신뢰 체인을 가져와야 합니다.

Dell Manager:

- Microsoft 키 저장소 워크스테이션의 "안전한 루트 인증서 인증 기관"에 "Root Agency" 서명 인증서를 삽입합니다(생성된 자체 서명 인증서에서).

  Security Management Server은 Active Directory를 사용 중일 때 LDAP 채널 바인딩 및 LDAP 서명을 위한 Microsoft 요구 사항과 호환됩니다.

  Security Management Server에서 이 기능을 사용하려면 Microsoft 인증서 키 저장소 내의 "안전한 루트" 저장소로 가져온 도메인 컨트롤러 인증서에 대한 루트 발급 인증서가 있어야 합니다.
- 서버측 SSL 유효성 검사의 동작을 수정합니다. 서버측 SSL 신뢰 유효성 검사를 끄려면 설정 탭에서 **신뢰 체인 검사 비활성화**를 선택합니다.

인증서를 만드는 방법은 *빠른 생성*과 *고급*의 두 가지가 있습니다.

한 가지 방법을 선택합니다.

- 빠른 생성 - 모든 구성요소에 대해 자체 서명 인증서를 생성하려면 이 방법을 선택합니다. 가장 쉬운 방법이기는 하지만 자체 서명된 인증서는 파일럿, POC 등에 적합합니다. 프로덕션 환경이라면 Dell은 공용 CA-서명 또는 도메인-서명 인증서를 권장합니다.
- 고급 - 각 구성 요소를 개별적으로 구성하려면 이 방법을 선택합니다.

빠른 생성

1. 상단 메뉴에서 **작업** >**인증서 구성**을 선택합니다.
2. 구성 마법사가 시작되면 **빠른 생성**을 선택하고 **다음**을 클릭합니다. 해당되는 경우, Security Management Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.
3. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

인증서 설치가 완료되었습니다. 이 섹션의 다음 부분은 인증서 생성을 위한 고급 방법에 대해 설명합니다.

고급

인증서를 생성하는 데 2가지 경로, 즉 *자체 서명 인증서 생성* 및 *현재 설정 사용*이 있습니다. **한 가지** 경로를 선택합니다.

- 경로 1 – 자체 서명 인증서 생성
- 경로 2 – 현재 설정 사용

경로 1 – 자체 서명 인증서 생성

1. 상단 메뉴에서 **작업** >**인증서 구성**을 선택합니다.
2. 구성 마법사가 시작되면 **고급**을 선택하고 **다음**을 클릭합니다.
3. **자체 서명 인증서 생성**을 선택하고 **다음**을 클릭합니다. 해당되는 경우, Security Management Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.
4. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

인증서 설치가 완료되었습니다. 이 섹션의 다음 부분은 인증서 생성을 위한 다른 방법에 대해 설명합니다.

경로 2 – 현재 설정 사용

1. 상단 메뉴에서 **작업** >**인증서 구성**을 선택합니다.
2. 구성 마법사가 시작되면 **고급**을 선택하고 **다음**을 클릭합니다.
3. **현재 설정 사용**을 선택하고 **다음**을 클릭합니다.
4. *Compatibility Server SSL 인증서* 창에서 **자체 서명 인증서 생성**을 선택하고 **다음**을 클릭합니다. 해당되는 경우, Security Management Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.

   다음을 클릭합니다.
5. *Core Server SSL 인증서* 창에서 다음 중 하나를 선택합니다.
   - *인증서 선택* - 기존 인증서를 사용하려면 이 옵션을 선택합니다. **다음**을 클릭합니다.

     기존 인증서 위치를 탐색하여 기존 인증서와 연결된 암호를 입력하고 **다음**을 클릭합니다.

     완료되면 **마침**을 클릭합니다.
   - *자체 서명 인증서 생성* – 해당되는 경우, Security Management Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다. 이 옵션을 선택하면 Message Security 인증서 창이 표시되지 않고(이 창은 *현재 설정 사용* 옵션을 선택할 경우에 표시됨) Dell Compatibility Server에 대해 생성된 인증서가 사용됩니다.

     정규화된 컴퓨터 이름이 정확한지 확인합니다. **다음**을 클릭합니다.

     이름이 동일한 인증서가 이미 존재한다는 경고 메시지가 표시됩니다. 사용할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.

     완료되면 **마침**을 클릭합니다.
   - *현재 설정 사용* – Security Management Server의 최초 구성 후 언제든지 인증서의 설정을 변경하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 이미 구성된 인증서가 그대로 유지됩니다. 이 옵션을 선택하면 Message Security 인증서 창으로 이동합니다.

     Message Security 인증서에서 다음 중 **하나**를 선택합니다.
     - *인증서 선택* - 기존 인증서를 사용하려면 이 옵션을 선택합니다. **다음**을 클릭합니다.

       기존 인증서 위치를 탐색하여 기존 인증서와 연결된 암호를 입력하고 **다음**을 클릭합니다.

       완료되면 **마침**을 클릭합니다.
     - *자체 서명 인증서 생성* – 해당되는 경우, Security Management Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.

       다음을 클릭합니다.

       완료되면 **마침**을 클릭합니다.

인증서 설치가 완료되었습니다.

변경이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

2. Dell Server 구성 툴을 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

Dell Manager 인증서 가져오기

배포 계획 중 Encryption Management Agent가 탑재된 Security Management Server 원격 관리 클라이언트가 포함된 경우에는 새로 생성한(또는 기존) 인증서를 가져와야 합니다. Dell Manager 인증서는 Security Management Server 원격 관리 클라이언트 및 Encryption Management Agent로 보내는 정책 번들 서명에 사용하는 개인 키를 보호하는 수단으로 사용됩니다. 이 인증서는 다른 인증서와 별도로 존재할 수 있습니다. 추가적으로, 이 키가 노출되었을 경우, 새로운 키로 대체할 수 있으며, 이 키가 정책 번들을 암호화하지 못하는 경우, Dell Manager가 새로운 공용 키를 요청합니다.

1. Microsoft 관리 콘솔을 엽니다.
2. **파일** > **스냅인 추가/제거**를 클릭합니다.
3. **추가**를 클릭합니다.
4. *독립 실행형 스냅인 추가* 창에서 **인증서**를 선택하고 **추가**를 클릭합니다.
5. **컴퓨터 계정**을 선택하고 **다음**을 클릭합니다.
6. *컴퓨터 선택* 창에서 **로컬 컴퓨터(이 콘솔이 실행되고 있는 컴퓨터)**를 선택하고 **완료**를 클릭합니다.
7. **닫기**를 클릭합니다.
8. **확인**을 클릭합니다.
9. *콘솔 루트* 폴더에서 *인증서(로컬 컴퓨터)*를 확장합니다.
10. *개인* 폴더로 이동하고 원하는 인증서를 찾습니다.
11. 원하는 인증서를 강조 표시하고 **모든 작업 > 내보내기**를 오른쪽 단추로 클릭합니다.
12. 인증서 내보내기 마법사가 열리면 **다음**을 클릭합니다.
13. **예, 개인 키를 내보냅니다**를 선택하고 **다음**을 클릭합니다.
14. **개인 정보 교환 - PKCS #12(.PFX)**를 선택한 후 **가능한 경우 인증서 경로에 모든 인증서를 포함** 및 **모든 확장된 속성 내보내기** 하위 옵션을 선택합니다. **다음**을 클릭합니다.
15. 암호를 입력하고 확인합니다. 원하는 암호를 사용할 수 있습니다. 다른 사람은 쉽게 기억할 수 없지만 나는 수월하게 기억할 수 있는 암호를 선택합니다. **다음**을 클릭합니다.
16. **찾아보기**를 클릭하여 파일을 저장할 위치를 찾습니다.
17. *파일 이름*에는 파일을 저장할 이름을 입력합니다. **저장**을 클릭합니다.
18. **다음**을 클릭합니다.
19. **마침**을 클릭합니다.
20. 내보내기가 성공적으로 수행되었다는 메시지가 표시됩니다. MMC를 닫습니다.
21. Dell Server 구성 도구로 돌아갑니다.
22. 상단 메뉴에서 **작업** > **DM 인증서 가져오기**를 선택합니다.
23. 내보낸 파일이 저장된 위치를 탐색합니다. 파일을 선택하고 **열기**를 클릭합니다.
24. 이 파일에 연결된 암호를 입력하고 **확인**을 클릭합니다.

Dell Manager 인증서 가져오기가 완료되었습니다.

변경이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
2. Dell Server 구성 도구를 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

SSL/TLS 인증서 베타 가져오기

배포 시 Server Encryption이 포함된 경우, 새로 생성한(또는 기존) 인증서를 가져와야 합니다. SSL/TLS 인증서 베타는 클라이언트 서버로 보내는 정책 번들 서명에 사용하는 개인 키를 보호합니다.

1. 상단 메뉴에서 **작업** > **SSL/TLS 인증서 베타 가져오기**를 선택합니다.
2. 인증서를 찾아 선택하고 **다음**을 클릭합니다.
3. *인증서 암호* 메시지가 나타나면 기존 인증서와 연결된 암호를 입력합니다.
4. Windows 계정 대화상자에서 하나의 옵션을 선택합니다.
   a. ID 인증서와 연결된 자격 증명을 변경하려면 **ID 인증서가 있는 다른 Windows 계정 자격 증명 사용**을 선택합니다.
   b. 로그온되어 있는 계정의 자격 증명을 계속 사용하려면 **다음**을 클릭합니다.
5. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

Server SSL 인증서의 설정 구성

Server 구성 도구에서 **설정** 탭을 클릭합니다.

Dell Manager:

서버측 Dell Manager SSL 신뢰 유효성 검사를 끄려면 **신뢰 체인 검사 비활성화**에 선택합니다.

SCEP:

Mobile Edition을 사용하는 경우, SCEP를 호스팅하는 서버의 URL을 입력합니다.

노트: v9.8부터 Mobile Edition은 더 이상 지원되지 않습니다.

변경이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
2. Dell Server 구성 도구를 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

SMTP 설정 구성

Server 구성 툴에서 **SMTP** 탭을 클릭합니다.

이 탭은 Product Bulletin, 알림 및 Advanced Threat Prevention Threat Relay 메시지에 대한 SMTP 설정을 구성합니다.

구성 변경 사항이 완료되면 Security Server 서비스를 다시 시작합니다. 설정을 업데이트하려면 Security Server 서비스를 다시 시작해야 합니다.

다음 정보를 입력합니다.

1. *호스트 이름*에는 사용자의 SMTP 서버의 FQDN을 입력합니다(예: smtpservername.domain.com).
2. *사용자 이름*에는 메일 서버에 로그인할 사용자 이름을 입력합니다. 형식은 DOMAIN\jdoe, jdoe 또는 조직에서 요구하는 대로 사용할 수 있습니다.
3. *암호*에는 사용자 이름과 연결된 암호를 입력합니다.
4. *출처 주소*에는 필드에 해당 이메일이 시작될 이메일 주소를 입력합니다. 이것은 사용자 이름의 계정과 동일할 수 있지만 (jdoe@domain.com), 지정된 사용자 이름으로 이메일을 전송할 수 있는 다른 계정도 가능합니다(CloudRegistration@domain.com).
5. *포트*에는 포트 번호를 입력합니다(일반적으로 25).
6. *인증* 메뉴에서 *참* 또는 *거짓*을 선택합니다.

노트: 인증이 거짓으로 설정된 경우 사용자 이름과 암호를 비워두어야 합니다.

변경이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
2. Dell Server 구성 툴을 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

데이터베이스 이름, 위치 또는 자격 증명 변경

Server 구성 도구에서 **데이터베이스** 탭을 클릭합니다.

1. *서버 이름*에 데이터베이스를 호스팅하고 있는 서버의 정규화된 도메인 이름(인스턴스 이름이 있는 경우 포함)을 입력합니다. 예: SQLTest.domain.com\DellDB

   Dell은 IP 주소를 사용하는 경우에도 정규화된 도메인 이름을 사용할 것을 권장합니다.
2. *서버 포트*에 포트 번호를 입력합니다.

   비기본 SQL 서버 인스턴스를 사용할 때*포트:*에서 동적 포트의 인스턴스를 지정해야 합니다. 또는, SQL 서버 브라우저 서비스를 활성화하고 UDP 포트 1434가 열려있는지 확인합니다. 자세한 정보는 https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx를 참조하십시오.
3. *데이터베이스*에 데이터베이스 이름을 입력합니다.
4. *인증:*에서 **Windows 인증** 또는 **SQL Server 인증**을 선택합니다. Windows 인증을 선택하면 Windows에 로그인하는 데 사용한 자격 증명이 인증에 사용됩니다(*사용자 이름* 및 *암호*는 수정할 수 없음).
5. *사용자 이름:*에 이 데이터베이스와 관련된 적절한 사용자 이름을 입력하십시오.
6. *암호:*에서 *사용자 이름*에 나열된 사용자 이름에 대한 암호를 입력하십시오.
7. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
8. 데이터베이스 구성을 테스트하려면 상단 메뉴에서 **작업** > **데이터베이스 구성 테스트**를 선택합니다. 구성 마법사가 시작됩니다.
9. *구성 테스트* 창에서 테스트 정보를 읽고 **다음**을 클릭합니다.
10. *데이터베이스* 탭에서 Windows 인증을 선택하는 경우 대체 자격 증명을 선택적으로 입력하여 해당 자격 증명을 Security Management Server 실행에 사용할 수 있습니다. **다음**을 클릭합니다.
11. *구성 테스트* 창에 연결 설정 테스트, 호환성 테스트, 데이터베이스 마이그레이션 테스트 결과가 표시됩니다.
12. **마침**을 클릭합니다.

노트:

SQL 데이터베이스 또는 SQL 인스턴스가 비기본 데이터 정렬로 구성되어 있는 경우 비기본 데이터 정렬은 대/소문자를 구분해야 합니다. 데이터 정렬 및 대/소문자 구분 목록을 보려면 https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx를 참조하십시오.

변경이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
2. Dell Server 구성 도구를 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

데이터베이스 마이그레이션

서버를 최신으로 업그레이드하여 v9.2 이상의 데이터베이스를 최신 스키마로 마이그레이션할 수 있습니다.

Server 구성 도구에서 **데이터베이스** 탭을 클릭합니다.

1. 기존 Dell Server 데이터베이스를 아직 백업하지 않았다면, **지금 백업하십시오**.
2. 상단 메뉴에서 **작업** > **데이터베이스 마이그레이션**을 선택합니다. 구성 마법사가 시작됩니다.

3. *Enterprise Database 마이그레이션* 창에 경고 메시지가 표시됩니다. 전체 데이터베이스를 백업했는지 또는 백업이 기존 데이터베이스를 이용할 필요가 없는지 확인합니다. **다음**을 클릭합니다.

   데이터베이스 마이그레이션 창의 정보 메시지에 마이그레이션 상태가 표시됩니다.

   완료되면 오류 여부를 확인합니다.

   노트: 오류 메시지는  로 식별되며, 데이터베이스 작업이 실패했고 데이터베이스가 올바르게 마이그레이션되려면 먼저 정정 작업을 수행해야 함을 나타냅니다. 마침을 클릭하고 데이터베이스 오류를 정정한 다음 이 섹션의 지침을 다시 시작합니다.
4. **마침**을 클릭합니다.

마이그레이션이 완료되면 다음을 수행합니다.

1. 상단 메뉴에서 **구성** > **저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.
2. Dell Server 구성 도구를 닫습니다.
3. **시작** > **실행**을 클릭합니다. *services.msc*를 입력하고 **확인**을 클릭합니다. *서비스*가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

6

관리 작업

Dell 관리자 역할 지정

1. Security Management Server Virtual 관리자 계정으로 Management Console에 로그인합니다(https://server.domain.com:8443/webui). 기본 자격 증명은 **superadmin/changeit**입니다.
2. 왼쪽 창에서 **채우기** > **도메인**을 클릭합니다.
3. 사용자를 추가할 도메인을 클릭합니다.
4. 도메인 세부 정보 페이지에서 **구성원** 탭을 클릭합니다.
5. **사용자 추가**를 클릭합니다.
6. 일반 이름, UPN(Universal Principal Name) 또는 sAMAccountName 중에서 사용자 이름을 검색할 필터를 입력합니다. 와일드카드 문자는 *입니다.

   엔터프라이즈 디렉토리 서버에서 모든 사용자마다 일반 이름, UPN(Universal Principal Name) 및 sAMAccountName이 정의되어 있어야 합니다. 사용자가 도메인 또는 그룹의 멤버이지만 Management의 도메인 또는 그룹 멤버 목록에 표시되지 않으면, 엔터프라이즈 디렉토리 서버에 해당 사용자에 대해 3개 이름 모두가 올바르게 정의되어 있는지 확인하십시오.

   쿼리는 일치하는 항목을 찾을 때까지 자동으로 일반 이름, UPN, sAMAccount 이름순으로 검색합니다.
7. *디렉토리 사용자 목록*에서 도메인에 추가할 사용자를 선택합니다. 여러 사용자를 선택하려면 <Shift><클릭> 또는 <Ctrl><클릭>을 사용합니다.
8. **추가**를 클릭합니다.
9. 메뉴 표시줄에서, 지정된 사용자의 **세부 정보 및 작업** 탭을 클릭합니다.
10. 메뉴 표시줄을 스크롤하여 **관리자** 탭을 선택합니다.
11. 이 사용자에 추가할 관리자 역할을 선택합니다.
12. **저장**을 클릭합니다.

Dell 관리자 역할로 로그인

1. Management Console에서 로그아웃합니다.
2. Management Console에 로그인하고 도메인 사용자 자격 증명으로 로그인합니다.

클라이언트 액세스 라이선스 업로드

사용자는 최초 구매 시 또는 그 이후 클라이언트 액세스 라이선스를 추가하였을 경우 설치 파일로부터 별도로 클라이언트 액세스 라이선스를 받았습니다.

1. 왼쪽 창에서 **관리**를 클릭합니다.
2. **라이선스 관리를 클** 릭합니다.
3. **파일 선택** 을 클릭하여 클라이언트 라이선스 파일을 찾아 선택합니다.

정책 커밋

설치가 완료되면 정책을 커밋합니다.

설치 이후 또는 나중에 정책 수정이 저장된 이후에 정책을 커밋하려면 다음 단계를 수행합니다.

1. 왼쪽 창에서 **관리** > **커밋**을 클릭합니다.
2. *주석*에 변경에 대한 설명을 입력합니다.

3. **정책 커밋**을 클릭합니다.

Dell Compliance Reporter 구성

1. 왼쪽 창에서 **Compliance Reporter**를 클릭합니다.
2. Dell Compliance Reporter가 시작되면, 기본 자격 증명인 *superadmin/changeit*을 사용하여 로그인합니다.

백업 실행

재난 복구를 목적으로 매주 야간에 다음 위치에 대한 백업을 실행해야 합니다. 재해 복구를 위한 계획에 대한 자세한 내용은 http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en를 참조하십시오. Compliance Reporter 데이터 백업에 대한 자세한 내용은 http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en를 참조하십시오.

Security Management Server 백업

설치(27페이지의 10단계) 또는 업그레이드/마이그레이션(68페이지의 6단계) 중에 구성 파일 백업에 사용하기 위해 선택한 위치에 저장되는 파일을 정기적으로 백업하십시오. 이 데이터는 변경이 드물 뿐만 아니라 필요에 따라 수동으로 재구성이 가능하기 때문에 매주마다 백업해도 좋습니다. 다음과 같이 가장 중요한 파일들은 데이터베이스에 연결하는 데 필요한 정보를 저장하고 있습니다.

<설치 폴더>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<설치 폴더>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<설치 폴더>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

SQL Server 백업

트랜잭션 로깅을 활성화하여 야간에 전체 백업을 실행하고 3-4시간마다 차등 데이터베이스 백업을 실행하십시오. 백업 데이터베이스를 사용할 수 있는 경우에는 15분 또는 15분 미만(가능한 경우)의 간격으로 트랜잭션 로그 전달 작업을 수행하는 것이 좋습니다. 언제나 Dell은 Dell Server 데이터베이스에 데이터베이스 모범 사례를 사용하고 조직의 재해 복구 계획에 Dell 소프트웨어를 포함시킬 것을 권장합니다.

SQL Server 모범 사례에 대한 추가 정보는 Dell Security 설치 시 구현하지 않았다면 반드시 구현해야 하는 다음 목록을 참조하십시오.

PostgreSQL Server 백업

감사 이벤트가 C:\ProgramData\Dell\PostgreSQL\10.7\data의 PostgreSQL Server에 저장되며, 정기적으로 백업해야 합니다. 백업 지침은 /C:/ProgramData/Dell/PostgreSQL/10.7/data을 참조하십시오.

PostgreSQL 데이터베이스에 데이터베이스 모범 사례를 사용하고 조직의 재해 복구 계획에 Dell 소프트웨어를 포함시킬 것을 권장합니다.

7

포트

다음 표는 각 구성요소와 그 기능에 대한 설명입니다.

이름	기본 포트	설명
ACL 서비스	TCP/ 8006	여러 Dell 보안 제품에 대한 다양한 권한과 그룹 액세스를 관리합니다. **노트:** 포트 8006은 현재 보안되지 않습니다. 이 포트가 방화벽을 통해 올바르게 필터링되었는지 확인합니다. 이 포트는 내부 전용입니다.
Compliance Reporter	HTTP(S)/ 8084	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다. **노트:** 포트 8084는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다.
Management Console	HTTP(S)/ 8443	전체 엔터프라이즈 배포를 위한 관리 콘솔 및 제어 센터입니다.
Core Server	HTTPS/ 8888	정책 흐름, 라이선스 및 사전 부팅 인증을 위한 등록, SED Management, BitLocker 관리자, 위협 차단 및 Advanced Threat Prevention을 관리합니다. Compliance Reporter 및 Management Console을 통해 사용할 인벤토리 데이터를 처리합니다. 인증 데이터를 수집하고 보관합니다. 역할 기반 액세스를 관리합니다.
Device Server	HTTPS/ 8081	활성화 및 암호 복구를 지원합니다. Security Management Server의 구성요소입니다. Encryption Enterprise(Windows 및 Mac)에 필요함
Security Server	HTTPS/ 8443	포렌식 키 검색, 클라이언트 활성화, SED-PBA 및 전체 디스크 암호화-PBA 통신을 관리하고, Management Console에 인증을 위한 ID 확인을 포함한 인증 또는 조정을 위한 Active Directory도 관리하는 Policy Proxy와 통신합니다. SQL 데이터베이스 액세스가 필요합니다.
Compatibility Server	TCP/ 1099	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이터를, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 사용자 그룹에 기반하여 데이터를 처리합니다. **노트:** 포트 1099는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를

이름	기본 포트	설명
		내부용으로만 사용할 것을 권장합니다.
Message Broker 서비스	TCP/ 61616 및 STOMP/ 61613	Dell Server의 서비스 간 통신을 처리합니다. Policy Proxy 큐에 대한 Compatibility Server가 생성한 정책 정보 단계입니다. SQL 데이터베이스 액세스가 필요합니다. **노트:** 포트 61616는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다. **노트:** 포트 61613은 프런트엔드 모드로 구성된 Security Management Server에서만 열어야 합니다.
Key Server	TCP/ 8050	Kerberos API를 사용하여 클라이언트 연결을 협상, 인증 및 암호화합니다. 주요 데이터를 가져오기 위해 SQL 데이터베이스 액세스가 필요합니다.
Policy Proxy	TCP/ 8000	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다.
PostGres	TCP/ 5432	이벤트 데이터에 사용되는 로컬 데이터베이스입니다. **노트:** 포트 5432는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다.
LDAP	TCP/ 389/636(로컬 도메인 컨트롤러), 3268/3269(글로벌 카탈로그) TCP/ 135/ 49125+ (RPC)	포트 389 - 이 포트는 로컬 도메인 컨트롤러에서 정보를 요청하는 데 사용됩니다. 포트 389에 전송된 LDAP 요청을 사용하여 글로벌 카탈로그의 홈 도메인 내에 속하는 개체만 검색할 수 있습니다. 그러나 요청하는 애플리케이션에서 이러한 개체에 대한 속성을 모두 가져올 수 있습니다. 예를 들어, 포트 389에 대한 요청을 사용하여 사용자의 부서를 가져올 수 있습니다. 포트 3268 - 이 포트는 특별히 글로벌 카탈로그에 대한 대상으로 지정된 쿼리에 사용됩니다. 포트 3268에 전송된 LDAP 요청을 사용하여 전체 포리스트에서 개체를 검색할 수 있습니다. 그러나 글로벌 카탈로그에 복제하도록 표시된 속성만 반환될 수 있습니다. 예를 들어, 이 속성이 글로벌 카탈로그에 복제되지 않으므로 포트 3268을 사용하여 사용자의 부서를 반환할 수 없습니다.
Microsoft SQL 데이터베이스	TCP/ 1433	기본 SQL Server 포트는 1433이며, 클라이언트 포트에는 1024 ~ 5000 범위 내의 임의 값이 할당됩니다.

이름	기본 포트	설명
클라이언트 인증	HTTPS/ 8449	클라이언트 서버가 Dell Server를 통해 인증하도록 허용합니다. Server Encryption에 필요합니다.

8

SQL Server 모범 사례

다음 목록은 SQL Server 모범 사례로서 Dell Security 설치 시 구현하지 않았다면 반드시 구현해야 합니다.

1. 데이터 파일 및 로그 파일이 저장되는 NTFS 블록 크기가 64KB인지 확인하십시오. SQL Server 익스텐트(SQL Storage 기본 단위)는 64KB입니다.

   자세한 내용은 Microsoft의 TechNet 게시글에서 "페이지 및 익스텐트에 대한 이해"를 검색하여 확인하시기 바랍니다.

2. 일반 지침으로서 SQL Server 메모리의 최대 용량을 설치된 메모리의 80%로 설정하십시오.

   자세한 내용은 Microsoft의 TechNet 게시글에서 *서버 메모리 서버 구성 옵션*을 검색하여 확인하시기 바랍니다.

   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3. 교착 상태 발생 시 관련 정보를 수집할 수 있도록 인스턴스 시작 속성에서 -t1222를 설정합니다.

   자세한 내용은 Microsoft의 TechNet 게시글에서 "트레이스 플래그(Transact-SQL)"를 검색하여 확인하시기 바랍니다.

   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4. 매주 유지 보수 작업을 통해 인덱스를 재작성하면서 모든 인덱스가 적용되어 있는지 확인하십시오.

5. Security Management Server가 활용하는 데이터베이스에 대한 사용 권한 및 기능이 적합한지 확인하십시오. 자세한 내용은 KB 문서 SLN307771을 참조하십시오.

9

인증서

이 장에서는 Security Management Server와 함께 사용하기 위해 인증서를 얻는 방법을 설명합니다.

스마트 카드 인증을 구성하도록 구성하는 방법에 대한 내용은 http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en을 참조하십시오.

Dell Data Security 서버에서 사용하는 SSL/TLS 인증서를 요청하는 최소 요구 사항에 대한 정보는 http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en을 참조하십시오.

Microsoft 키 스토리지에서 기존 인증서와 함께 Dell 암호화를 위한 인증서 업데이트에 대한 자세한 내용은 http://www.dell.com/support/article/us/en/19/sln297240/을 참조하십시오.

자체 서명 인증서 생성 및 CSR(Certificate Signing Request) 생성

이 섹션에서는 Java 기반 구성 요소의 자체 서명 인증서를 만드는 단계에 대해 설명합니다. 이 프로세스는 .NET 기반 구성요소의 자체 서명 인증서를 만드는 데 **사용할 수 없습니다**.

자체 서명 인증서는 프로덕션이 아닌 환경에서*만* 사용하는 것이 좋습니다.

조직에서 SSL 서버 인증서를 요구하거나 다른 이유로 인증서를 만들어야 할 경우 이 섹션에서 Keytool을 이용한 Java 키 저장소를 만드는 방법을 참조할 수 있습니다.

조직에서 인증을 위해 스마트 카드를 사용할 계획인 경우, Keytool을 사용하여 스마트 카드 사용자 인증서에서 사용되는 전체 인증서 신뢰 체인을 가져와야 합니다.

Keytool은 VeriSign® 또는 Entrust®와 같은 CSR(Certificate Signing Request)의 형식으로 인증 기관(CA)에 전달해야 하는 개인 키를 만듭니다. 그런 다음 CA가 이 CSR을 기준으로 서명하는 서버 인증서를 만들고 서버 인증서가 서명 기관 인증서와 함께 파일로 다운로드됩니다. 그런 다음 인증서를 cacerts 파일로 가져옵니다.

새 키 쌍 및 자체 서명 인증서 생성

1. Compliance Reporter, Security Server 또는 Device Server의 **conf** 디렉터리로 이동합니다.
2. 다음과 같이 기본 인증서 데이터베이스를 백업합니다.

   시작 > **실행**을 클릭하고 **`move cacerts cacerts.old`**를 입력합니다.
3. 시스템 경로에 Keytool을 추가합니다. 명령 프롬프트에 다음 명령을 입력합니다.

   `set path=%path%;<Dell Java Install Dir>\bin`
4. 인증서를 생성하려면 다음과 같이 Keytool을 실행합니다.

   `keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias` Dell **`-keystore .\cacerts`**
5. Keytool에 정보를 입력하라는 메시지가 표시되면 다음과 같이 입력합니다.

   노트:

   편집하기 전 구성 파일을 백업해 두십시오. 지정된 매개 변수만 변경해야 합니다. 이러한 파일에서 태그를 포함한 다른 데이터를 변경할 경우 시스템 손상 및 오류가 발생할 수 있습니다. 이러한 파일에서 허가되지 않은 매개 변수를 변경하여 문제가 발생하는 경우 Security Management Server를 다시 설치하지 않는 이상 문제가 해결되지 않을 수 있습니다.

- *키 저장소 암호*: 암호를 입력하고(지원되지 않는 문자 <>;&" ') 구성 요소 **conf** 파일의 변수를 다음과 같이 동일한 값으로 설정합니다.

  <Compliance Reporter install dir>\conf\eserver.properties. eserver.keystore.password = 값 설정

  <Device Server install dir>\conf\application.properties. keystore.password = 값 설정

<Security Server install dir>\conf\application.properties. keystore.password = 값 설정

- *정규화된 서버 이름*: 사용하는 구성 요소가 설치된 서버의 정규화된 이름을 입력합니다. 이 정규화된 이름에는 호스트 이름과 도메인 이름이 포함됩니다(예: server.domain.com).
- *부서*: 적절한 값을 입력합니다(예: 보안부).
- *조직*: 적절한 값을 입력합니다(예: Dell).
- *시 또는 지역*: 적절한 값을 입력합니다(예: Dallas).
- *시 또는 도*: 축약형이 아닌 시 또는 도의 전체 이름을 입력합니다(예: Texas).
- 2문자로 이루어진 국가 코드
- 정보가 정확한지 확인을 요청하는 메시지가 표시됩니다. 정확하다면, **yes**라고 입력합니다.

  그렇지 않다면, **no**라고 입력합니다. Keytool에 이전에 입력된 각 값이 표시됩니다. **입력**을 클릭하여 해당 값을 채택하거나 값을 변경한 후 **입력**을 클릭합니다.
- *별칭 키 암호*: 여기에서 다른 암호를 입력하지 않을 경우 이 암호에 기본적으로 키 저장소 암호가 적용됩니다.

인증 기관에서 서명된 인증서 요청

새 키 쌍 및 자체 서명 인증서 생성에서 만든 자체 서명 인증서에 대해 CSR(Certificate Signing Request)을 생성하려면 이 절차를 사용합니다.

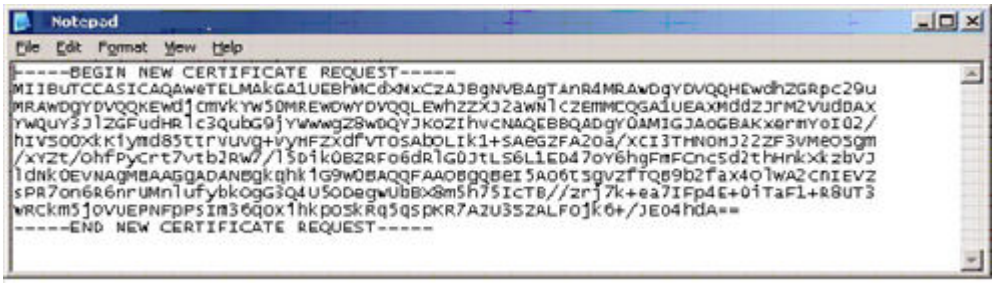
1. 이전에 <**certificatealias**>에 사용된 값과 동일한 값으로 대체합니다.

   ```
   keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
   <csr-filename>
   ```

   예: **keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file** Dell**.csr**

   .csr 파일에는 CA에서 인증서를 만드는 동안 사용될 BEGIN/END 쌍이 포함됩니다.

   .CSR 파일 예

2. 조직이 인증 기관에서 SSL 서버 인증서를 취득하는 데 사용하는 절차를 따르십시오. 서명할 <csr 파일 이름>의 내용을 전송합니다.

   노트:

   유효한 인증서를 요청하는 방법은 여러 가지가 있습니다. 예제 방법은 **인증서를 요청하는 방법의 예**에 나와 있습니다.
3. 서명된 인증서를 받으면 파일에 저장하십시오.
4. 가져오기 프로세스 중 오류가 발생할 경우에 대비하여 이 인증서를 백업해 두는 것이 좋습니다. 이렇게 백업해 두면 프로세스를 다시 시작하지 않아도 됩니다.

루트 인증서 가져오기

루트 인증서 인증 기관이 Verisign(Verisign Test 제외)인 경우 다음 절차로 건너 뛰어 서명된 인증서를 가져오십시오.

인증 기관 루트 인증서는 서명된 인증서의 유효성을 검사합니다.

1. 다음 중 **하나를** 수행하십시오.

- 인증 기관 루트 인증서를 다운로드하고 파일에 저장합니다.
- 엔터프라이즈 디렉터리 서버 루트 인증서를 얻습니다.

2. 다음 중 **하나를** 수행하십시오.
   - Compliance Reporter, Security Server 또는 Device Serverr에 대한 SSL을 활성화하려는 경우, 구성 요소 **conf** 디렉터리로 변경합니다.
   - Security Management Server와 엔터프라이즈 서버 사이에서 SSL을 활성화하려면 <**Dell install dir>\Java Runtimes \jre1.x.x_xx\lib\security**로 변경합니다(JRE cacerts의 기본 암호는 **changeit**).
3. 다음과 같이 Keytool을 실행하여 루트 인증서를 설치합니다.

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

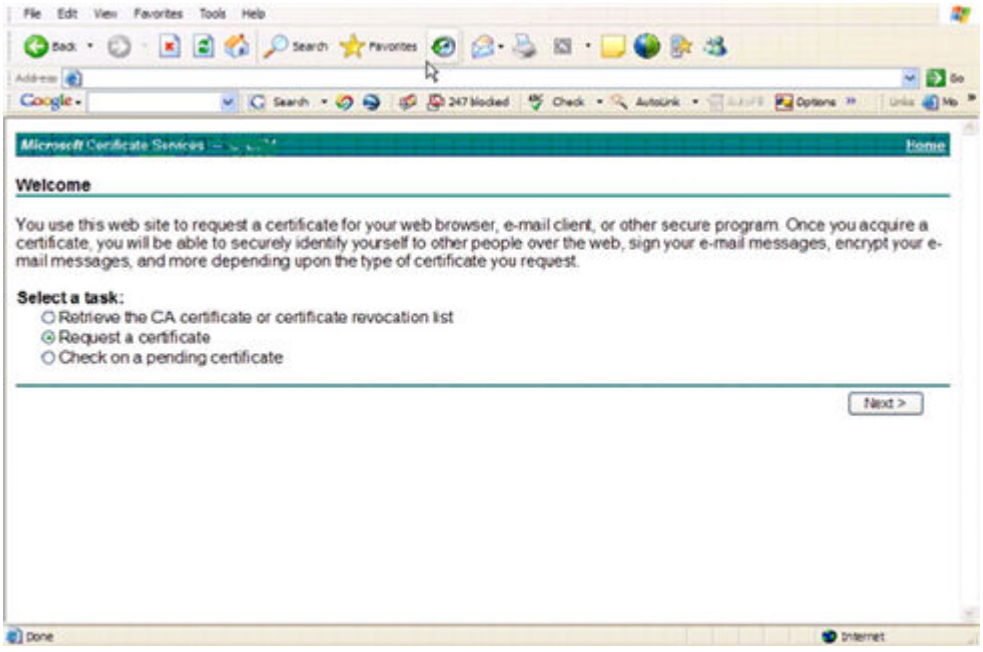
예: **keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer**

인증서를 요청하는 방법의 예

조직에서 내부적으로 설정한 인증서를 요청하는 방법을 예로 들면 웹 브라우저를 사용하여 Microsoft CA Server에 액세스하는 방법이 있습니다.

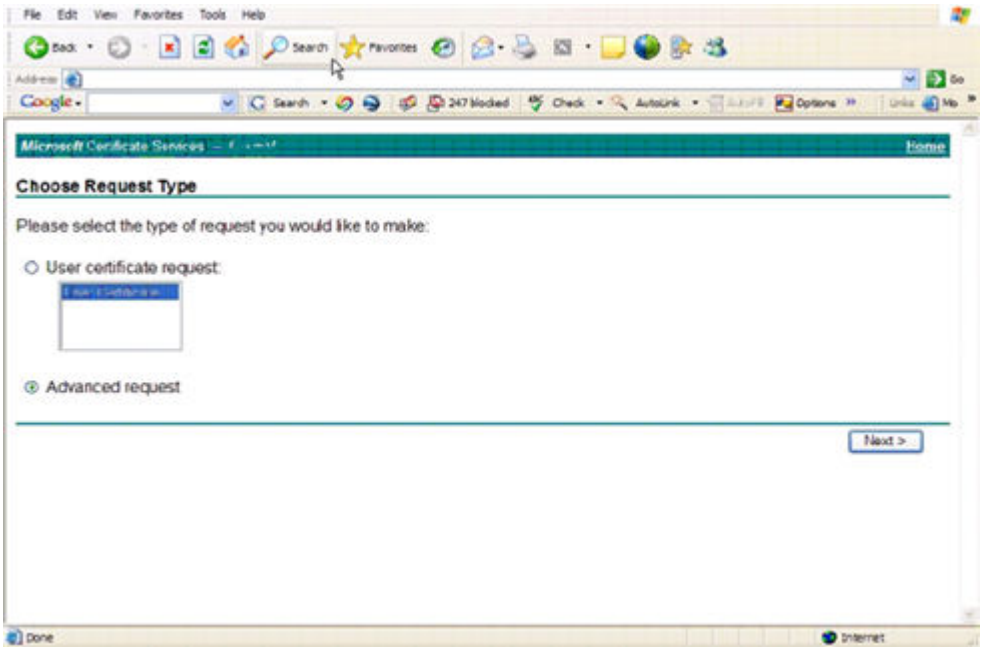
1. Microsoft CA Server를 탐색합니다. IP 주소는 조직이 제공합니다.
2. **인증서 요청**을 선택하고 **다음**을 클릭합니다.

   Microsoft 인증서 서비스



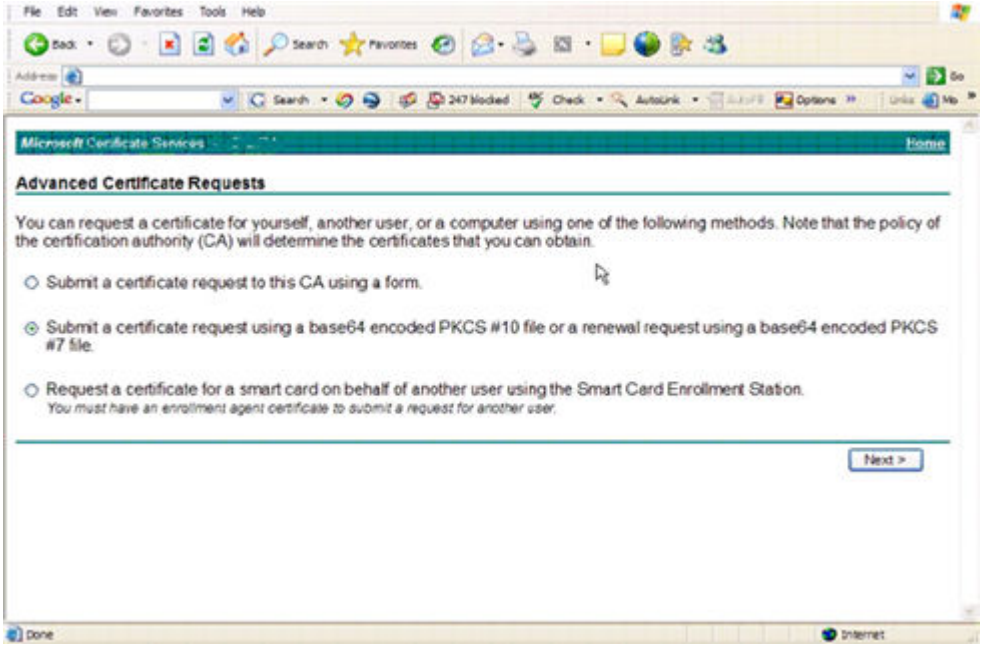
3. **고급 요청**을 선택하고 **다음**을 클릭합니다.

   요청 유형 선택



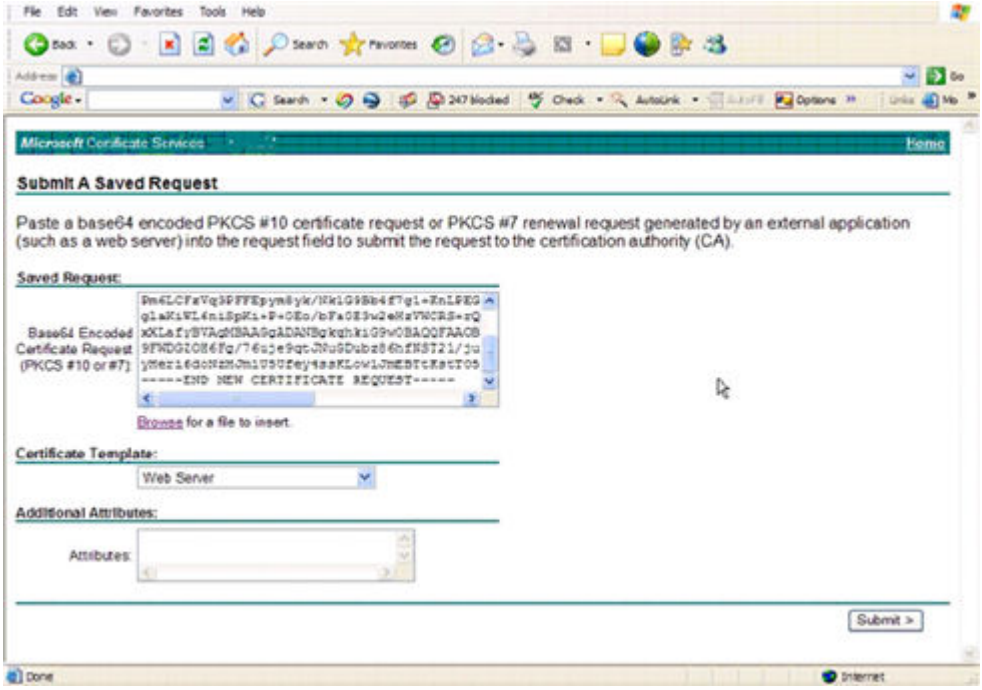
4. **base64로 인코딩된 PKCS #10 파일을 사용하여 인증서 요청을 제출** 옵션을 선택하고 **다음**을 클릭합니다.

고급 인증서 요청



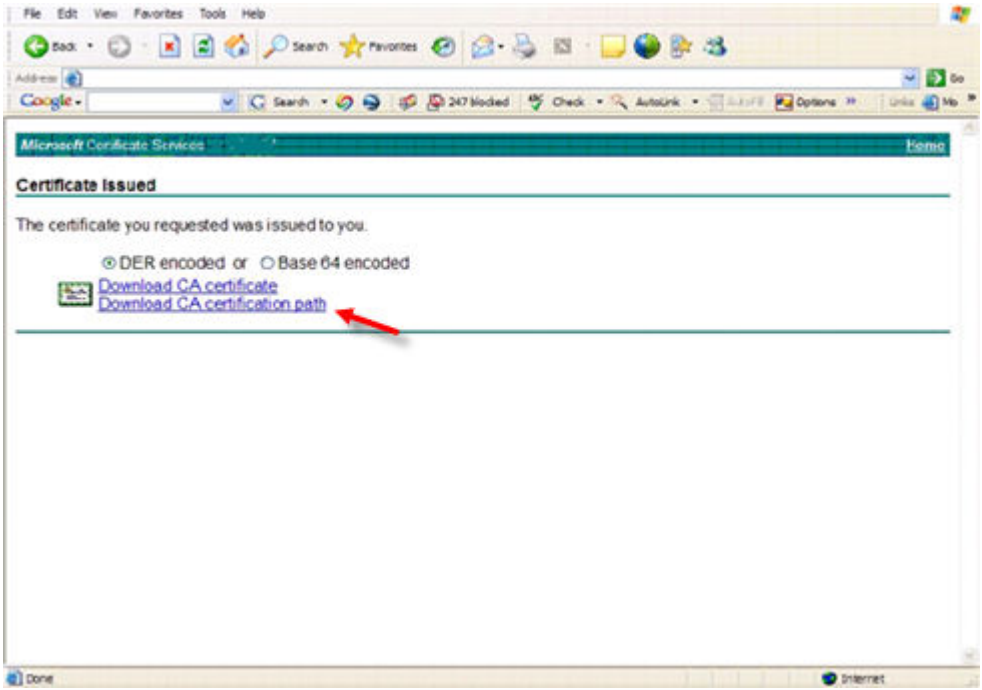
5. 텍스트 상자에 CSR 요청의 내용을 붙여 넣습니다. **Web Server**의 인증서 템플릿을 선택하고 **제출**을 클릭합니다.

저장된 요청 제출



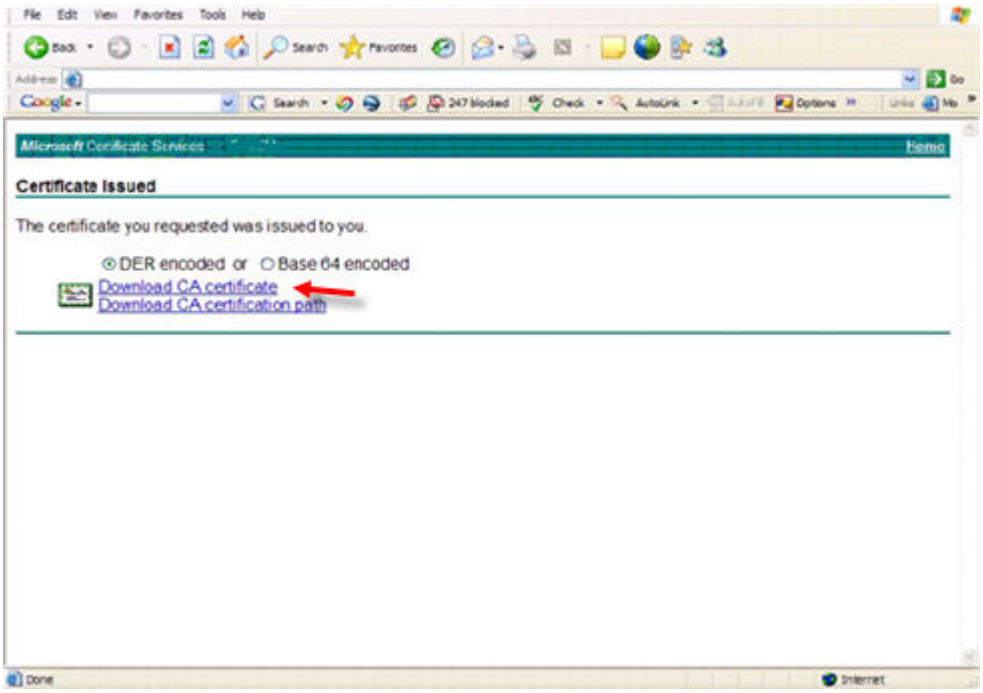
6. 인증서를 저장합니다. **DER 인코딩**을 선택하고 **CA 인증서 다운로드**를 클릭합니다.

CA 인증서 다운로드



7. 인증서를 저장합니다. **DER 인코딩**을 선택하고 **CA 인증서 경로 다운로드**를 클릭합니다.

CA 인증서 경로 다운로드



8. 변환된 서명 기관 인증서를 가져옵니다. 명령 프롬프트로 돌아갑니다. 유형:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9. 서명 기관 인증서를 가져왔으므로 서버 인증서를 가져올 수 있습니다(신뢰 체인을 구축할 수 있음). 유형:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

   자체 서명 인증서의 별칭을 사용하여 CSR 요청과 서버 인증서를 연결합니다.

10. cacerts 파일 목록에 서버 인증서의 **인증서 체인 길이**가 **2**라는 정보가 표시됩니다. 즉, 자체 서명된 인증서가 아님을 나타냅니다. 유형:

```
keytool -list -v -keystore cacerts
```

    체인에서 두 번째 인증서의 인증서 지문은 가져온 서명 기관 인증서(목록의 서버 인증서 아래에도 나열됨)입니다.

인증서 관리 콘솔을 사용하여 인증서를 .PFX로 내보내기

MMC에서 인증서를 .crt 파일 형태로 가지고 있다면, Security Server가 DMZ 모드에서 사용될 *때와* Dell Manager 인증서를 Dell Server 구성 도구로 가져올 때 Keytool에서 사용하기 위해 이 파일을 .pfx 파일로 변환해야 합니다.

1. Microsoft 관리 콘솔을 엽니다.
2. **파일** > **스냅인 추가/제거**를 클릭합니다.
3. **추가**를 클릭합니다.
4. *독립 실행형 스냅인 추가* 창에서 **인증서**를 선택하고 **추가**를 클릭합니다.
5. **컴퓨터 계정**을 선택하고 **다음**을 클릭합니다.
6. *컴퓨터 선택* 창에서 **로컬 컴퓨터(이 콘솔이 실행되고 있는 컴퓨터)**를 선택하고 **완료**를 클릭합니다.
7. **닫기**를 클릭합니다.
8. **확인**을 클릭합니다.
9. *콘솔 루트* 폴더에서 *인증서(로컬 컴퓨터)*를 확장합니다.
10. *개인* 폴더로 이동하고 원하는 인증서를 찾습니다.
11. 원하는 인증서를 강조 표시하고 **모든 작업 > 내보내기**를 오른쪽 단추로 클릭합니다.
12. 인증서 내보내기 마법사가 열리면 **다음**을 클릭합니다.
13. **예, 개인 키를 내보냅니다**를 선택하고 **다음**을 클릭합니다.

14. **개인 정보 교환 - PKCS #12(.PFX)**를 선택한 후 **가능한 경우 인증서 경로에 모든 인증서를 포함** 및 **모든 확장된 속성 내보내기** 하위 옵션을 선택합니다. **다음**을 클릭합니다.
15. 암호를 입력하고 확인합니다. 원하는 암호를 사용할 수 있습니다. 다른 사람은 쉽게 기억할 수 없지만 나는 수월하게 기억할 수 있는 암호를 선택합니다. **다음**을 클릭합니다.
16. **찾아보기**를 클릭하여 파일을 저장할 위치를 찾습니다.
17. *파일 이름*에는 파일을 저장할 이름을 입력합니다. **저장**을 클릭합니다.
18. **다음**을 클릭합니다.
19. **마침**을 클릭합니다.

    내보내기가 성공적으로 수행되었다는 메시지가 표시됩니다. MMC를 닫습니다.

SSL에 신뢰할 수 없는 인증서가 사용되었을 때 Security Server에 신뢰할 수 있는 서명 인증서 추가

1. Security Server 서비스가 실행되고 있다면 중지합니다.
2. cacerts 파일을 <Security Server install dir>\conf\에 백업합니다.

   Keytool을 사용하여 다음을 완료합니다.
3. 신뢰할 수 있는 PFX를 텍스트 파일로 내보내고 별칭을 기록합니다.

   ```
   keytool -list -v -keystore "
   ```
4. PFX를 <Security Server install dir>\conf\의 cacerts 파일로 가져옵니다.

   ```
   keytool -importkeystore -v -srckeystore "
   ```
5. <Security Server install dir>\conf\application.properties의 keystore.alias.signing 값을 수정합니다.

   ```
   keystore.alias.signing=AliasNamePreviouslyDocumented
   ```

   Security Server 서비스를 시작합니다.