

## 시작하기

Enterprise Server 설치 및 마이그레이션 안내서 v9.7



## 참고, 주의 및 경고

① | **노트:** "참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

△ | **주의:** "주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

⚠ | **경고:** "경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.

© 2017 Dell Inc. All rights reserved. Dell, EMC 및 기타 상표는 Dell Inc. 또는 자회사의 상표입니다. 기타 상표는 각 소유자의 상표일 수 있습니다.

Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 및 Dell Data Guardian 문서 세트에 사용된 등록된 상표 및 상표, 즉 Dell™, Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc. Cylance® 및 CylancePROTECT의 상표이고 Cylance 로고는 미국에서 Cylance, Inc.의 등록된 상표입니다. 상표입니다. McAfee® 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc.의 상표 또는 등록 상표입니다. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® 및 Xeon®은 미국 및 기타 국가에서 Intel Corporation의 등록 상표입니다. Adobe®, Acrobat®, 및 Flash®는 Adobe Systems Incorporated의 등록 상표입니다. Authen Tec® 및 Eikon®은 Authen Tec의 등록 상표입니다. AMD®는 Advanced Micro Devices, Inc.의 등록 상표입니다. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, Visual C++®는 미국 및/또는 기타 국가에서 Microsoft Corporation의 상표 또는 등록 상표입니다. VMware®는 미국 또는 기타 국가에서 VMware, Inc.의 등록 상표 또는 상표입니다. Box®는 Box의 등록 상표입니다. DropboxSM은 Dropbox, Inc.의 서비스 표시입니다. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® 및 Google™ Play는 미국 및 기타 국가에서 Google Inc.의 상표 또는 등록 상표입니다. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud@SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® 및 Siri®는 미국 및/또는 기타 국가에서 Apple, Inc.의 서비스 표시, 상표, 또는 등록 상표입니다. GO ID®, RSA®, SecurID®는 Dell EMC의 등록 상표입니다. EnCase™ 및 Guidance Software®는 Guidance Software의 상표 또는 등록 상표입니다. Entrust®는 미국 및 기타 국가에서 Entrust®, Inc.의 등록 상표입니다. InstallShield®는 미국, 중국, 유럽 공동체, 홍콩, 일본, 대만, 및 영국에서 Flexera Software의 등록 상표입니다. Micron® 및 RealSSD®는 미국 및 기타 국가에서 Micron Technology, Inc.의 등록 상표입니다. Mozilla® Firefox®는 미국 및/또는 기타 국가에서 Mozilla Foundation의 등록 상표입니다. iOS®는 미국 및 기타 특정 국가에서 Cisco Systems, Inc.의 상표 또는 등록 상표이며, 라이선스 하에 사용됩니다. Oracle® 및 Java®는 Oracle 및/또는 Oracle 계열사의 등록 상표입니다. 기타 이름은 해당 소유자의 상표일 수 있습니다. SAMSUNG™은 미국 또는 기타 국가에서 SAMSUNG의 상표입니다. Seagate®는 미국 및/또는 기타 국가에서 Seagate Technology LLC의 등록 상표입니다. Travelstar®는 미국 및 기타 국가에서 HGST, Inc.의 등록 상표입니다. UNIX®는 The Open Group의 등록 상표입니다. VALIDITY™는 미국 및 기타 국가에서 Validity Sensors, Inc.의 상표입니다. VeriSign®과 기타 관련 상표는 미국 및 기타 국가에서 VeriSign, Inc.와 그 계열사 또는 자회사의 상표 또는 등록 상표이며, Symantec Corporation에 사용 허가된 상표 또는 등록 상표입니다. KVM on IP®는 Video Products의 등록 상표입니다. Yahoo!®는 Yahoo! Inc.의 등록 상표입니다. 본 제품은 7-Zip 프로그램을 일부 사용합니다. 소스 코드는 [www.7-zip.org](http://www.7-zip.org)에서 찾아볼 수 있습니다. 라이선스에는 GNU LGPL 라이선스 + unRAR 제한이 적용됩니다([www.7-zip.org/license.txt](http://www.7-zip.org/license.txt)).

### Enterprise Server 설치 및 마이그레이션 안내서

2017 - 04

개정 A01

<b>1 Dell Enterprise Server 소개</b> .....	<b>5</b>
Dell Enterprise Server 정보.....	5
Dell ProSupport에 문의.....	5
<b>2 Dell Enterprise Server 요구 사항 및 아키텍처</b> .....	<b>6</b>
Dell Enterprise Server 요구 사항.....	6
Dell Enterprise Server의 필수 조건.....	6
Dell Enterprise Server 하드웨어.....	6
Dell Enterprise Server 소프트웨어.....	7
Dell Enterprise Server 언어 지원.....	9
Dell Enterprise Server 아키텍처 디자인.....	9
<b>3 설치 전 구성</b> .....	<b>15</b>
구성.....	15
<b>4 설치 또는 업그레이드/마이그레이션</b> .....	<b>20</b>
설치 또는 업그레이드/마이그레이션을 시작하기 전에.....	20
신규 설치.....	20
백엔드 서버 및 새 데이터베이스 설치.....	21
기존 데이터베이스와 함께 백엔드 서버 설치.....	24
프론트 엔드 서버 설치.....	29
업그레이드/마이그레이션.....	30
업그레이드/마이그레이션을 시작하기 전에.....	30
백엔드 서버 업그레이드/마이그레이션.....	32
프론트 엔드 서버 업그레이드/마이그레이션.....	34
연결되지 않은 모드 설치.....	35
연결되지 않은 모드로 Enterprise Server 설치.....	38
Dell Enterprise Server 제거.....	38
<b>5 설치 후 구성</b> .....	<b>39</b>
EAS Management 설치 및 구성.....	39
EAS Device Manager 설치.....	39
EAS Mailbox Manager 설치.....	40
EAS 구성 유틸리티 사용.....	40
EAS 관리 설정 구성.....	40
Dell Security Server(DMZ Mode) 구성.....	41
Keytool을 사용하여 DMZ 도메인 인증서 가져오기.....	41
application.properties 파일 수정.....	42
APN 등록.....	42
Server 구성 도구.....	43
새 인증서 또는 업데이트된 인증서 추가.....	43
Dell Manager 인증서 가져오기.....	45
ID 인증서 가져오기.....	46

Server SSL 인증서 또는 Mobile Edition의 설정 구성.....	47
Data Guardian 또는 이메일 서비스에 대한 SMTP 설정 구성.....	47
데이터베이스 이름, 위치 또는 자격 증명 변경.....	47
데이터베이스 마이그레이션.....	48
<b>6 관리 작업.....</b>	<b>50</b>
Dell 관리자 역할 지정.....	50
Dell 관리자 역할로 로그인.....	50
클라이언트 액세스 라이선스 업로드.....	50
정책 커밋.....	50
Dell Compliance Reporter 구성.....	51
Compliance Reporter로 SQL 인증 구성.....	51
Compliance Reporter로 Windows 인증 구성.....	51
백업 실행.....	52
Enterprise Server 백업.....	52
SQL Server 백업.....	52
PostgreSQL Server 백업.....	52
<b>7 Dell 구성 요소 설명.....</b>	<b>53</b>
<b>8 SQL Server 모범 사례.....</b>	<b>55</b>
<b>9 인증서.....</b>	<b>56</b>
자체 서명 인증서 생성 및 CSR(Certificate Signing Request) 생성.....	56
새 키 쌍 및 자체 서명 인증서 생성.....	56
인증 기관에서 서명된 인증서 요청.....	57
루트 인증서 가져오기.....	57
인증서를 요청하는 방법의 예.....	58
인증서 관리 콘솔을 사용하여 인증서를 .PFX로 내보내기.....	59
SSL에 신뢰할 수 없는 인증서가 사용되었을 때 Security Server에 신뢰할 수 있는 서명 인증서 추가.....	59



# Dell Enterprise Server 소개

## Dell Enterprise Server 정보

Enterprise Server는 Dell 솔루션의 보안 관리 제품입니다. Remote Management Console을 사용하면 관리자가 기업 전체에 걸쳐 끝점, 정책 적용 및 보호 상태를 모니터링할 수 있습니다.

Enterprise Server의 특징은 다음과 같습니다.

- 장치들의 중앙 집중식 관리
- 역할 기반의 보안 정책 생성 및 관리
- 관리자 지원 장치 복구
- 관리 임무 구분
- 보안 정책 자동 배포
- 구성 요소 간 통신 시 신뢰할 수 있는 경로
- 고유한 암호화 키 생성 및 자동 보안 키 에스스로
- 중앙 집중화된 준수 감사 및 보고

## Dell ProSupport에 문의

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

또한, [dell.com/support](https://dell.com/support)에서 Dell Data Protection 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 코드를 준비하십시오.

미국 외부의 전화 번호는 [Dell ProSupport 국제 전화 번호](#)를 확인하십시오.



# Dell Enterprise Server 요구 사항 및 아키텍처

이 섹션은 Dell Data Protection 구현에 관한 하드웨어 및 소프트웨어 요구 사항 및 아키텍처 디자인 권장사항에 대해 설명합니다.

## Dell Enterprise Server 요구 사항

Dell Enterprise Server 구성요소에는 Dell 설치 미디어에서 제공하는 소프트웨어에 추가로 하드웨어 및 소프트웨어 요구 사항이 있습니다. 설치 또는 업그레이드/마이그레이션 작업을 계속하기 전에 설치 환경이 이 요구 사항을 충족하는지 확인하십시오.

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

## Dell Enterprise Server의 필수 조건

다음 표는 Dell Enterprise Server를 설치하기 전에 준비해야 하는 소프트웨어의 세부 사항입니다. 다음의 필수 소프트웨어 설치를 위한 링크와 지침은 [사전 설치 구성](#)에서 자세히 설명합니다.

설치 프로그램이 항목을 설치한다고 기록되어 있지 않은 한, 설치가 시작되기 전에 각 해당 소프트웨어 항목을 설치해야 합니다. 그렇지 않으면 설치가 실패합니다.

## Dell Enterprise Server 하드웨어

### 필수 조건

- **Visual C++ 2010 재배포 가능 패키지**  
설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.
- **Visual C++ 2013 재배포 가능 패키지**  
설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.
- **Visual C++ 2015 재배포 가능 패키지**  
설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.
- **.NET Framework 버전 3.5 SP1**
- **.NET Framework 버전 4.5**  
Microsoft는 .NET Framework 버전 4.5용 보안 업데이트를 게시했습니다.
- **SQL Native Client 2012**  
SQL Server 2012 또는 SQL Server 2016을 사용하는 경우.  
설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.

다음 표에는 Dell Enterprise Server의 **최소** 하드웨어 요구 사항이 자세히 나와 있습니다. 배포 규모를 바탕으로 한 조정과 관련한 추가 정보는 [Dell Enterprise Server 아키텍처 디자인](#)을 참조하십시오.

## 하드웨어 요구 사항

### 프로세서

Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 등급을 포함한 최소 Modern Dual-Core CPU(2 GHz+)

단일 서버 구성을 위한 Modern Quad-Core CPU(2 GHz+)

### RAM

최소 8GB, 구성에 따라 다름

단일 서버 구성에 필요한 16GB

### 사용 가능한 디스크 공간

약 1.5GB의 사용 가능한 디스크 공간(및 가상 페이지징 공간)

단일 서버 구성에 필요한 20GB 이상의 사용 가능한 공간(및 가상 페이지징 공간)

### 네트워크 카드

10/100/1000 네트워크 인터페이스 카드

### 기타

TCP/IPv4 설치 및 등록

## Dell Enterprise Server 소프트웨어

다음 표에는 Dell Enterprise Server 및 프록시 서버의 소프트웨어 요구 사항이 자세히 나와 있습니다.

① **노트:** 설치 전에 UAC를 비활성화해야 합니다. 서버를 재부팅해야만 변경 사항이 적용됩니다. Windows Server 2012 R2 및 Windows Server 2016에서는 설치 프로그램이 UAC를 비활성화합니다.

① **노트:** Dell Policy Proxy의 레지스트리 위치(설치된 경우): HKLM\SOFTWARE\Wow6432Node\Dell

① **노트:** Windows Server의 레지스트리 위치: HKLM\SOFTWARE\Dell

### Dell Enterprise Server - 백엔드 서버 및 Dell 프론트 엔드 서버

- **Windows Server 2008 R2 SP0-SP1 64비트**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2008 SP2 64비트**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition



## Exchange ActiveSync Servers

Mobile Edition을 사용하려는 경우에는 다음과 같은 Exchange ActiveSync Server들이 지원됩니다. 이 구성요소는 사용자의 프론트 엔드 Exchange Server에 설치됩니다.

- Exchange ActiveSync 12.0 - Exchange Server 2007의 구성 요소
- Exchange ActiveSync 12.1 - Exchange Server 2007 SP1의 구성 요소
- Exchange ActiveSync 14.0 - Exchange Server 2010의 구성 요소
- Exchange ActiveSync 14.1 - Exchange Server 2010 SP1의 구성 요소

**Microsoft Message Queuing(MSMQ)**을 Exchange Server에서 설치/구성되어야 합니다.

## LDAP 리포지토리

- Active Directory 2008
- Active Directory 2008 R2
- Active Directory 2012

## Dell Enterprise Server 구성요소를 위한 권장 가상 환경

Dell Enterprise Server는 가상 환경에서 설치가 가능합니다. 다음과 같은 환경만 사용하는 것이 좋습니다.

Dell Enterprise Server v9.7은 Hyper-V Server(전체 또는 코어 설치)를 통해 검증되었고 Windows Server 2012 R2 또는 Windows Server 2016에서는 역할로 검증되었습니다.

- Hyper-V Server(전체 또는 코어 설치)
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 하드웨어가 최소 Hyper-V 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 1세대 가상 머신으로 실행되어야 함
  - 자세한 내용은 <https://technet.microsoft.com/en-us/library/hh923062.aspx>를 참조하십시오.

Dell Enterprise Server v9.7은 VMware ESXi 5.5 및 VMware ESXi 6.0을 통해 검증되었습니다. 잠재적인 취약성을 해결하기 위해 모든 패치와 업데이트가 VMware ESXi에 바로 적용되었는지 확인하십시오.

**① | 노트: VMware ESXi 및 Windows Server 2012 R2 또는 Windows Server 2016을 사용하는 경우 VMXNET3 이더넷 어댑터를 권장합니다.**

- VMware ESXi 5.5
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 <http://www.vmware.com/resources/compatibility/search.php>를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 <http://pubs.vmware.com/vsphere-55/index.jsp>를 참조하십시오.
- VMware ESXi 6.0
  - 64비트 x86 CPU 필요



- 2코어 이상의 호스트 컴퓨터
- 8GB 이상의 RAM 권장
- 운영 체제가 필요 없음
- 지원되는 호스트 운영 체제의 전체 목록은 <http://www.vmware.com/resources/compatibility/search.php>를 참조하십시오.
- 하드웨어가 최소 VMware 요구 사항을 충족해야 함
- 전용 이미지 리소스를 위한 4GB 이상의 RAM
- 자세한 내용은 <http://pubs.vmware.com/vsphere-60/index.jsp>를 참조하십시오.

① | **노트:** Dell Enterprise Server를 호스팅하는 SQL Server 데이터베이스는 별도의 컴퓨터에서 실행되어야 합니다.

#### 데이터베이스

- **SQL Server 2008 및 SQL Server 2008 R2** - Standard Edition/Enterprise Edition
- **SQL Server 2008 SP4(KB3045311 포함)** - Standard Edition/Enterprise Edition
- **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

① | **노트:** Express Edition은 제품 환경에 지원되지 않습니다. Express Edition은 POC 및 평가용으로만 사용할 수 있습니다.

#### Dell Data Protection Remote Management Console 및 Compliance Reporter

- Internet Explorer 11.x 이상
- Mozilla Firefox 41.x 이상
- Google Chrome 46.x 이상

① | **노트:** 브라우저에서 쿠키를 허용해야 합니다.

## Dell Enterprise Server 언어 지원

Remote 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	

## Dell Enterprise Server 아키텍처 디자인

Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 및 Data Guardian 솔루션은 확장성이 뛰어난 제품으로서 기업 규모와 암호화할 끝점 수에 따라 확장이 가능합니다. 이 섹션에서는 엔드포인트 수가 5,000 ~ 60,000대일 경우 아키텍처 확장을 위한 몇 가지 지침에 대해 알아보겠습니다.

① | **노트:** 기업의 엔드포인트 수가 50,000대 이상일 경우에는 Dell ProSupport에게 문의하십시오.



**① 노트:**

각 섹션의 구성요소는 대부분 환경에서 최적의 성능을 발휘할 수 있는 최소 하드웨어 사양을 나타냅니다. 따라서 이 구성요소에 충분한 리소스를 할당하지 못할 경우 응용 프로그램의 성능 저하나 기능 문제가 발생할 수 있습니다.

**엔드포인트 수가 최대 5,000대인 경우**

이 아키텍처는 엔드포인트 수가 1~5,000대인 대부분 중소기업에 적합합니다. 모든 Dell Enterprise Server 서버 구성요소를 단일 서버에 설치할 수 있습니다. 프론트-엔드 서버는 선택에 따라 정책을 게시하거나 인터넷을 통해 엔드포인트를 활성화할 목적으로 DMZ에 배치할 수 있습니다.

**아키텍처 구성요소**

**Dell Enterprise Server**

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

**Single-Server 구성**

16GB; 20GB 이상의 사용 가능한 공간(및 가상 페이징 공간); Modern Quad-Core CPU (2 GHz+)

**Front-End Server로 사용할 경우 서버 구성**

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

**Dell External Front-End Server**

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

**SQL Server**

SQL Server 2008, SQL Server 2008 R2 및 SQL Server 2008 SP4(KB3045311 포함) Standard Edition/Enterprise Edition

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

**엔드포인트 수가 5,000 ~ 20,000대인 경우**

이 아키텍처는 엔드포인트 수가 5,000 ~ 20,000대인 환경에 적합합니다. 추가되는 부하를 분산할 목적으로 프론트-엔드 서버를 증설할 경우 약 15,000 ~ 20,000대의 엔드포인트를 처리할 수 있습니다. 프론트-엔드 서버는 선택에 따라 정책을 게시하거나 인터넷을 통해 엔드포인트를 활성화할 목적으로 DMZ에 배치할 수 있습니다.

**아키텍처 구성요소**

**Dell Enterprise Server**



구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

### **Dell 내부 프론트 엔드 서버(1대) 및 Dell 외부 프론트 엔드 서버(1대)**

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

### **SQL Server**

SQL Server 2008, SQL Server 2008 R2 및 SQL Server 2008 SP4(KB3045311 포함) Standard Edition/Enterprise Edition

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

### **엔드포인트 수가 20,000 ~ 40,000대인 경우**

이 아키텍처는 엔드포인트 수가 20,000 ~ 40,000대인 환경에 적합합니다. 프론트-엔드 서버를 증설하여 추가되는 부하를 분산할 수 있습니다. 각 프론트-엔드 서버는 약 15,000 ~ 20,000대의 엔드포인트를 처리할 수 있습니다. 프론트-엔드 서버는 선택에 따라 인터넷을 통해 엔드포인트를 활성화하거나 엔드포인트에 정책을 게시할 목적으로 DMZ에 배치할 수 있습니다.

### **아키텍처 구성요소**

#### **Dell Enterprise Server**

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

### **Dell 내부 프론트 엔드 서버(2대) 및 Dell 외부 프론트 엔드 서버(1대)**

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

### **SQL Server**

SQL Server 2008, SQL Server 2008 R2 및 SQL Server 2008 SP4(KB3045311 포함) Standard Edition/Enterprise Edition

SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition



### 엔드포인트 수가 40,000 ~ 60,000대인 경우

이 아키텍처는 엔드포인트 수가 40,000 ~ 60,000대인 환경에 적합합니다. 프론트-엔드 서버를 증설하여 추가되는 부하를 분산할 수 있습니다. 각 프론트-엔드 서버는 약 15,000 ~ 20,000대의 엔드포인트를 처리할 수 있습니다. 프론트-엔드 서버는 선택에 따라 인터넷을 통해 엔드포인트를 활성화하거나 엔드포인트에 정책을 게시할 목적으로 DMZ에 배치할 수 있습니다.

#### ① 노트:

기업의 엔드포인트 수가 50,000대 이상일 경우에는 Dell ProSupport에게 문의하십시오.

### 아키텍처 구성요소

#### Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

#### Dell 내부 프론트 엔드 서버(2대) 및 Dell 외부 프론트 엔드 서버(1대)

Windows Server 2008 R2 SP0-SP1 64비트/Windows Server 2008 SP2 64비트 - Standard 또는 Enterprise Edition

Windows Server 2012 R2 - Standard 또는 Datacenter Edition

Windows Server 2016 - Standard 또는 Datacenter Edition

구성에 따라 최소 8GB; +1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간); Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium 또는 AMD 상응 용량을 포함한 Modern Dual-Core CPU minimum(2 GHz+)

#### SQL Server

SQL Server 2008, SQL Server 2008 R2 및 SQL Server 2008 SP4(KB3045311 포함) Standard Edition/Enterprise Edition

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

### 고가용성을 고려한 설계

이 아키텍처는 뛰어난 가용성을 바탕으로 최대 60,000대까지 엔드포인트를 지원합니다. Dell Enterprise Server는 active/passive 구성으로 2대가 설치됩니다. 보조 Dell Enterprise Server로 장애 조치가 이루어지면 기본 노드의 서비스가 중단되고 DNS 별칭(CNAME)은 보조 노드를 가리키게 됩니다. 보조 노드에서 서비스를 시작하고 원격 관리 콘솔을 실행해 응용 프로그램이 제대로 작동하는지 확인합니다. 보조(passive) 노드의 서비스는 정기 유지 보수 및 패칭 도중 우발적으로 시작될 수도 있으므로 "수동"으로 설정해서는 안 됩니다.

그 밖에 기업은 SQL Cluster 데이터베이스 서버를 선택할 수도 있습니다. 이 구성에서는 Dell Enterprise Server가 클러스터 IP 또는 호스트 이름을 사용하도록 설정해야 합니다.



① **노트:**

데이터베이스 복제는 지원되지 않습니다.

클라이언트 트래픽은 내부의 프론트-엔드 서버 3대로 분산됩니다. 또한 선택에 따라 인터넷을 통해 엔드포인트를 활성화하거나 엔드포인트에 정책을 게시할 목적으로 다수의 프론트-엔드 서버를 DMZ에 배치할 수 있습니다.

**가상화**

Dell Enterprise Server는 가상 환경에서 설치가 가능합니다. 다음과 같은 환경만 사용하는 것이 좋습니다.

Dell Enterprise Server v9.7은 Hyper-V Server(전체 또는 코어 설치)를 통해 검증되었고 Windows Server 2012 R2 또는 Windows Server 2016에서는 역할로 검증되었습니다.

- Hyper-V Server(전체 또는 코어 설치)
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 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.aspx>를 참조하십시오.

Dell Enterprise Server v9.7은 VMware ESXi 5.5 및 VMware ESXi 6.0을 통해 검증되었습니다. 잠재적인 취약성을 해결하기 위해 모든 패치와 업데이트가 VMware ESXi에 바로 적용되었는지 확인하십시오.

① **노트: VMware ESXi 및 Windows Server 2012 R2 또는 Windows Server 2016을 사용하는 경우 VMXNET3 이더넷 어댑터를 권장합니다.**

- VMware ESXi 5.5
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 <http://www.vmware.com/resources/compatibility/search.php>를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 <http://pubs.vmware.com/vsphere-55/index.jsp>를 참조하십시오.
- VMware ESXi 6.0
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 <http://www.vmware.com/resources/compatibility/search.php>를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 <http://pubs.vmware.com/vsphere-60/index.jsp>를 참조하십시오.

① **노트: Dell Enterprise 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 모든 데이터베이스 인덱스를 재작성하고 통계도 수집해야 합니다.



## 설치 전 구성

시작하기 전에 Enterprise Server와 관련된 모든 최신 해결 방법이나 알려진 문제를 확인하려면 *Dell Enterprise Server 기술 관련 문서*를 읽으십시오.

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

### 구성

- 1 Internet Explorer 보안 강화 구성(ESC)이 활성화되어 있다면 해제하십시오. 서버 URL을 브라우저 보안 옵션의 신뢰할 수 있는 사이트에 추가하십시오. 다음, 서버를 다시 부팅하십시오.
- 2 각 구성요소에 대해 다음 포트들을 여십시오.

#### 내부:

Active Directory 통신: TCP/389

이메일 통신(옵션): 25

#### 프론트 엔드 방향(필요한 경우):

외부 Dell Policy Proxy에서 Dell Message Broker로 통신: TCP/61616 및 STOMP/61613

백엔드 Dell Security Server로 통신: HTTPS/8443

백엔드 Dell Core Server로 통신: HTTPS/8888 및 9000

RMI 포트 통신 - 1099

백엔드 Dell Device Server로 통신: HTTP(S)/8443 - Dell Enterprise Server가 v7.7 이상인 경우 Dell Enterprise Server가 v7.7 미만인 경우, HTTP(S)/8081.

비콘 서버: HTTP/8446(Data Guardian을 사용하는 경우)

#### 외부(필요한 경우):

SQL 데이터베이스: TCP/1433

Remote Management Console: HTTPS/8443

LDAP: TCP/389/636(로컬 도메인 컨트롤러), TCP/3268/3269(글로벌 카탈로그), TCP/135/49125+(RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084(설치 시 자동으로 구성됨)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 및 9000(8888은 설치 시 자동으로 구성됨)



Dell Device Server: HTTP(S)/8443(Dell Enterprise Server v7.7 이상) 또는 HTTP(S)/8081 (Dell Enterprise Server v7.7 미만)

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

클라이언트 인증: HTTPS/8449(Server Encryption을 사용하는 경우)

클라이언트 통신, Advanced Threat Prevention을 사용하는 경우: HTTPS/TCP/443

**이 노트:**

출고 시 Enterprise Edition 클라이언트 권한을 부여받거나 라이선스를 구매하는 경우 도메인 컨트롤러에서 GPO를 설정하여 권한 부여를 사용하도록 설정합니다(Enterprise Edition 실행 서버와 다를 수 있음). 아웃바운드 포트 443을 사용하여 서버와 통신할 수 있는지 확인하십시오. 어떠한 이유로든 포트 443이 차단된 경우 권한 부여 기능이 작동하지 않습니다. 자세한 내용은 [Enterprise Edition 고급 설치 안내서](#)를 참조하십시오.

### Dell 데이터베이스 생성

- 3 아직 SQL 데이터베이스를 Dell Enterprise Server에 맞게 구성하지 않았다면 설치 프로그램이 설치 중에 대신 데이터베이스를 생성해 줍니다. Dell Enterprise Server를 설치하기 전 데이터베이스를 설정하고 싶은 경우, 아래의 지침을 따라 SQL 관리 스튜디오의 SQL 데이터베이스와 SQL 사용자를 생성합니다. **데이터베이스가 없을 경우 설치 프로그램이 데이터베이스를 대신 생성해 주므로 이 지침은 선택 사항입니다.**

Dell Enterprise Server를 설치할 때 **기존 데이터베이스와 함께 백엔드 서버 설치**의 지침을 따르십시오.

Dell Enterprise Server는 SQL 및 Windows 인증용으로 준비되어 있습니다. SQL 인증이 기본 인증 방법입니다.

데이터베이스를 생성한 후 db\_owner 권한이 있는 Dell 데이터베이스 사용자를 생성하십시오. db\_owner는 아무런 제약 없이 사용 권한 할당, 데이터베이스 백업과 복원, 개체 생성과 삭제, 사용자 계정 및 역할의 관리가 가능합니다. 그리고 이 사용자가 저장된 절차를 실행할 권한/특권을 지니고 있는지 확인하십시오.

Dell Enterprise Server를 설치한 후 비기본 SQL 서버 인스턴스를 사용할 때 Server 구성 도구의 데이터베이스 탭에 있는 인스턴스의 동적 포트를 지정해야 합니다. 자세한 내용은 [Server 구성 도구](#)를 참조하십시오. 또는, SQL 서버 브라우저 서비스를 활성화하고 UDP 포트 1434가 열려있는지 확인합니다. 자세한 정보는 [https://msdn.microsoft.com/en-us/library/hh510203\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx)를 참조하십시오.

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\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx)를 참조하십시오.

SQL Management Studio에서 SQL 데이터베이스와 SQL 사용자를 생성하려면 다음 중 하나를 선택하십시오.

#### Windows 인증을 사용하여 새 Windows SQL Server 데이터베이스를 생성합니다.

- a **시작 > 모든 프로그램 > Microsoft SQL Server > Management Studio**를 클릭합니다.
- b 데이터베이스 폴더를 마우스 오른쪽 버튼으로 클릭한 후 새 데이터베이스를 클릭합니다. 데이터베이스 속성 대화상자가 표시됩니다.
- c 데이터베이스 이름을 입력하고 **확인**을 클릭합니다.
- d **보안** 폴더를 확장하고 **로그인**을 마우스 오른쪽 버튼으로 클릭합니다.
- e **새 로그인**을 클릭하여 새 데이터베이스의 소유자를 생성합니다.
- f **이름** 필드에 사용자 이름을 입력합니다.
- g 인증 옵션은 **Windows 인증**을 선택합니다.
- h **사용자 매핑**을 선택한 후 새 데이터베이스를 강조 표시합니다.
- i 데이터베이스 역할(db\_owner)을 선택하고 **확인**을 클릭합니다.





또는

**SQL Server 인증을 사용하여 새 SQL Server 데이터베이스를 생성합니다.**

- a 시작 > 모든 프로그램 > **Microsoft SQL Server > Management Studio**를 클릭합니다.
- b *데이터베이스* 폴더를 마우스 오른쪽 버튼으로 클릭한 후, **새 데이터베이스**를 클릭합니다. *데이터베이스* 속성 대화상자가 표시됩니다.
- c 데이터베이스 이름을 입력하고 **확인**을 클릭합니다.
- d *보안* 폴더를 확장하고 **로그인**을 마우스 오른쪽 버튼으로 클릭합니다.
- e **새 로그인**을 클릭하여 새 데이터베이스의 소유자를 생성합니다.
- f *이름* 필드에 사용자 이름을 입력합니다.
- g 인증 옵션은 *SQL Server 인증*을 선택합니다. 암호를 입력하고 확인합니다.
- h **암호 만료 강제 적용**의 선택을 해제합니다.
- i **사용자 매핑**을 선택한 후 새 데이터베이스를 강조 표시합니다.
- j 데이터베이스 역할(db\_owner)을 선택하고 **확인**을 클릭합니다.

#### Visual C++ 2010/2013/2015 재배포 가능 패키지 설치

- 4 *아직 설치하지 않았다면* Visual C++ 2010, 2013 및 2015 재배포 가능 패키지를 설치하십시오. 원하는 경우 Dell Enterprise Server 설치 프로그램이 이 구성요소를 설치하게 할 수 있습니다.

Windows Server 2008 및 Windows Server 2008 R2 - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555>

#### .NET Framework 4.5 설치

- 5 *아직 설치하지 않았다면* .NET Framework 4.5를 설치하십시오.

Windows Server 2008 및 Windows Server 2008 R2 - <https://www.microsoft.com/en-us/download/details.aspx?id=42643>

#### SQL Native Client 2012 설치

- 6 *SQL Server 2012 또는 SQL Server 2016을 사용하는 경우*, SQL Native Client 2012를 설치합니다. 원하는 경우 Dell Enterprise Server 설치 프로그램이 이 구성요소를 설치하게 할 수 있습니다.

<http://www.microsoft.com/en-us/download/details.aspx?id=35580>

#### Microsoft CA(MSCEP) 구성

이 단계는 Mobile Edition에서 iOS를 사용하려는 경우에 MSCEP를 실행하는 서버에서만 완료해야 합니다.

- 7 MSCEP를 구성합니다.

Windows Server 2008 R2는 Enterprise Edition이어야 합니다. **Standard Edition에서는 MSCEP 역할을 설치할 수 없습니다.**

- a 서버 관리자를 엽니다. 왼쪽 메뉴에서 **서버 역할**을 선택하고 **Active Directory 인증서 서비스** 확인란을 선택합니다. 다음을 클릭합니다. 역할 추가 마법사가 다음 단계로 안내합니다.

AD CS > *역할 서비스*에서 **인증 기관**과 **인증 기관 웹 등록** 역할 서비스의 확인란을 선택합니다. **웹 서버 IIS에 필요한 역할 서비스 추가**를 선택합니다(메시지가 나타날 경우). 다음을 클릭합니다.

AD CS > *설치 유형*에서 **독립 실행형**을 선택합니다. 다음을 클릭합니다.

AD CS > *CA 유형*에서 **하위 CA**를 선택합니다. 다음을 클릭합니다.

AD CS > *개인 키*에서 **새 개인 키 만들기**를 선택합니다. 다음을 클릭합니다.

AD CS > *개인 키* > *암호화*에서 **RSA#Microsoft Software Key Storage Provider, 2048** 및 **SHA1**의 기본값을 유지합니다. 다음을 클릭합니다.



AD CS > 개인 키 > CA 이름에서 모든 기본값을 유지합니다. 다음을 클릭합니다.

AD CS > 개인 키 > 인증서 요청에서 부모 CA에 인증서 요청을 보낼을 선택합니다. 검색 기준: CA 이름을 선택합니다. 부모 CA를 검색하여 선택합니다. 다음을 클릭합니다.

AD CS > 인증서 데이터베이스에서 기본값을 유지합니다. 다음을 클릭합니다.

웹 서버(IIS)에서 다음을 클릭합니다.

웹 서버(IIS) > 역할 서비스에서 기본값을 유지합니다. 다음을 클릭합니다.

확인에서 설치를 클릭합니다.

결과에서 결과를 검토하고 닫기를 클릭합니다.

서버 관리자 > 역할에서 Active Directory 인증서 서비스 아래의 역할 서비스 추가를 선택합니다.

역할 서비스 선택창이 표시되면 네트워크 장치 등록 서비스의 확인란을 선택합니다. 다음을 클릭합니다.

네트워크 장치 등록 서비스가 로컬 서버의 IIS\_IUSRS의 사용자 그룹에 대한 인증서 요청을 승인할 때 사용해야 하는 사용자 계정을 추가합니다. 형식은 도메인\사용자 이름입니다. 확인을 클릭합니다.

사용자 계정 지정 창에서, 방금 IIS\_IUSRS 그룹에 추가된 사용자를 선택합니다. 다음을 클릭합니다.

등록 기관 정보 지정 창에서 원하는 대로 필수 정보와 선택적 정보 추가의 기본값을 유지합니다. 다음을 클릭합니다.

등록 기관에 대한 암호문 구성 창에서 기본값을 유지합니다. 다음을 클릭합니다.

설치 선택 사항 확인 창에서 설치를 클릭합니다.

설치 결과창에서 결과를 검토하고 닫기를 클릭합니다.

서버 관리자를 닫습니다.

- b 레지스트리 키를 다음과 같이 수정하십시오.

```
HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
```

```
"EnforcePassword"=dword:00000000
```

- c IIS 관리자를 엽니다. \<ServerName> \Sites\Default Web Site\CertSrv\mscep\_admin으로 이동합니다.

인증서를 열고 익명 인증을 활성화합니다.

- d 시작 > 실행을 클릭합니다. certsrv.msc를 입력하고 입력을 클릭합니다.

certsrv 창이 표시되면 서버 이름을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택하고 정책 모듈 탭을 클릭합니다.

속성을 클릭하고 가능하면 인증서 템플릿의 설정에 따르면 그렇지 않은 경우 자동으로 인증서 발급 확인을 클릭합니다.

- e IIS 관리자를 닫습니다.

- f 서버를 다시 시작합니다. 확인을 위해, Internet Explorer를 열고 주소 표시줄에

http://server.domain.com/certsrv/mscep\_admin/을 입력합니다.

MSCEP Windows Server 2008 R2 설치를 종료합니다.

### Windows Server 2012 R2 또는 Windows Server 2016:

- a "Active Directory 인증서 서비스(AD CS)의 네트워크 장치 등록 서비스(NDES)" 문서의 지침을 따르십시오.

- b 레지스트리 키를 다음과 같이 수정하십시오.

```
HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
```

"EnforcePassword"=dword:00000000

- c IIS 관리자를 엽니다. `\\<ServerName>\Sites\Default Web Site\CertSrv\mscep_admin`으로 이동합니다.

인증서를 열고 **익명 인증**을 활성화합니다.

- d **시작 > 실행**을 클릭합니다. `certsrv.msc`를 입력하고 **입력**을 클릭합니다.

`certsrv` 창이 표시되면 서버 이름을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택하고 **정책 모듈** 탭을 클릭합니다.

**속성**을 클릭하고 **가능하면 인증서 템플릿의 설정에 따르고 그렇지 않은 경우 자동으로 인증서 발급 확인**을 클릭합니다.

- e IIS 관리자를 닫습니다.

- f 서버를 다시 시작합니다. 확인을 위해, Internet Explorer를 열고 주소 표시줄에

`http://server.domain.com/certsrv/mscep_admin/`을 입력합니다.

MSCEP Windows Server 2012 R2/Windows Server 2016 설치를 종료합니다.

### Microsoft Message Queuing(MSMQ) 설치/구성

**이 과정은 Mobile Edition을 사용하려고 하는 경우에만 완료해야 합니다.** 이는 EAS Device Manager 및 EAS Mailbox Manager에서 통신할 수 있도록 하기 위한 필수 조건입니다.

- 8 Windows Server 2008 또는 Windows Server 2008 R2의 경우(Exchange 환경을 호스팅하는 서버) – <http://msdn.microsoft.com/en-us/library/aa967729.aspx>

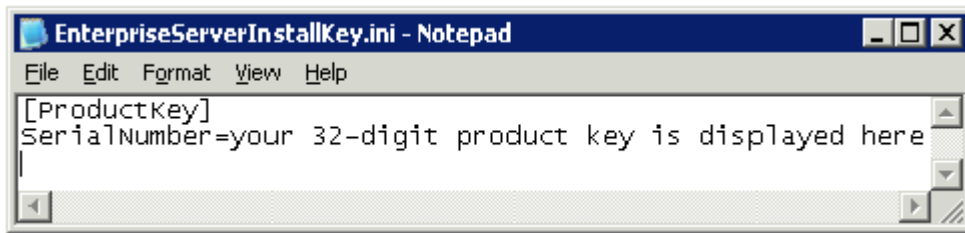
또는

Windows Server 2012 R2:

- a 서버 관리자를 엽니다.
- b **관리 > 역할 및 기능 추가**로 이동합니다.
- c 시작하기 전 화면에서 **다음**을 클릭합니다.
- d **역할 기반 또는 기능 기반 설치**를 선택하고 **다음**을 클릭합니다.
- e 기능을 설치할 서버를 선택하고 **다음**을 클릭합니다.
- f 서버 역할은 선택하지 마십시오. **다음**을 클릭합니다.
- g 기능에서 **Message Queuing**을 선택하고 **설치**를 클릭합니다.

### 선택 사항

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



서버의 사전 설치 구성이 완료되었습니다. 계속해서 **설치 또는 업그레이드/마이그레이션**합니다.

## 설치 또는 업그레이드/마이그레이션

이 장에서는 다음과 같은 작업을 위한 지침을 제공합니다.

- **새 설치** - Dell Enterprise 서버를 새로 설치합니다.
- **업그레이드/마이그레이션** - 작동 중인 기존의 Dell Enterprise Server v8.0 이상에서 업그레이드합니다.
- **Dell Enterprise 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.

Dell Enterprise Server 설치와 관련된 모든 최신 해결 방법이나 알려진 문제를 확인하려면 *Enterprise Server 기술 관련 문서*를 읽어 보십시오.

사용자 계정 컨트롤(UAC)이 활성화되어 있으면 이를 비활성화해야 합니다. Windows Server 2012 R2에서는 설치 프로그램이 UAC를 비활성화합니다. 서버를 재부팅해야만 변경 사항이 적용됩니다.

설치 중에 Windows 또는 SQL 인증 자격 증명이 있어야만 데이터베이스를 설정할 수 있습니다. Windows 인증을 선택할 경우 로그인한 사용자의 자격 증명이 사용됩니다. 사용자에게 시스템 관리자 권한과 SQL 데이터베이스를 생성하고 관리할 수 있는 권한(데이터베이스 생성, 사용자 추가, 권한 지정)이 있어야 합니다. SQL 인증의 경우에도 사용되는 계정에 같은 권한이 필요합니다. 이 자격 증명은 설치 중에만 사용됩니다. 설치된 제품은 이 자격 증명을 사용하지 않습니다.

또한 설치 중에 Dell 서비스에서 SQL Server에 액세스하는 데 사용할 서비스 런타임 인증 자격 증명을 지정해야 합니다. 사용자 계정에는 SQL Server 권한 기본 스키마(dbo) 및 Database Role Membership(dbo\_owner, public)이 있어야 합니다.

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

Dell 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 C:\ProgramData\Dell\Dell Data Protection\Installer Logs 디렉토리에 있습니다.

## 신규 설치

백엔드 서버를 설치할 때 다음 두 옵션 중 하나를 선택하십시오.

- **백엔드 서버 및 새 데이터베이스 설치** - 새 Dell Enterprise Server와 새 데이터베이스를 설치합니다.
- **기존 데이터베이스와 함께 백엔드 서버 설치** - 스키마 버전이 설치할 Dell Enterprise Server 버전과 일치하는 경우 Dell Enterprise Server를 새로 설치하고 **사전 설치 구성** 도중에 생성된 SQL 데이터베이스에 연결하거나 v9.x 이상인 기존 SQL 데이터베이스에 연결할 수 있습니다. v8.x 이상의 데이터베이스는 최신 버전의 Server 구성 도구를 사용하여 최신 스키마로 마이그레이션해야 합니다.

다. Server 구성 도구로 데이터베이스 마이그레이션의 지침을 보려면 [데이터베이스 마이그레이션](#)을 참조하십시오. 최신 Server 구성 도구를 가져오거나 v8.0 이전의 데이터베이스를 마이그레이션하려면 Dell ProSupport에 문의하십시오.

① **노트:**

Dell Enterprise Server v8.x 이상을 사용하고 있는 경우 [백엔드 서버 업그레이드/마이그레이션](#)의 지침을 참조하십시오.

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

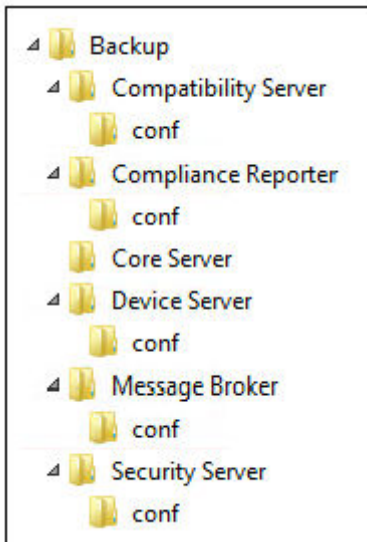
- [프론트 엔드 서버 설치](#) - 백엔드 서버와 통신할 프론트 엔드 서버를 설치합니다.

## 백엔드 서버 및 새 데이터베이스 설치

- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Dell Enterprise Server-x64를 Enterprise Server를 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 InstallShield 마법사 대화상자에서, 설치 언어를 선택한 후 **확인**을 클릭합니다.
- 4 필수 구성요소가 아직 설치되어 있지 않으면, 필수 구성요소가 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.
- 5 시작 대화상자에서 **다음**을 클릭합니다.
- 6 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.
- 7 선택적으로 **사전 설치 구성**에서 **9단계**를 완료한 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 Dell Enterprise Server를 기본 위치인 C:\Program Files\Dell에 설치하려면 **다음**을 클릭합니다. 그렇지 않으면, **변경**을 클릭하여 다른 위치를 선택하고 **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 수동으로 서버를 복원하는 데 필요한 전체 정보에서 중요한 역할을 합니다.

① **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.  
**찾아보기**를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 [Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 참조하십시오.

**다음**을 클릭합니다.

**① 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 저장소에 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

**다음**을 클릭합니다.

**① 노트:**

기본적으로 인증서 유효 기간은 1년입니다.

- 12 Server Encryption(SE)에서, 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.  
**찾아보기**를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 [Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 참조하십시오.

**다음**을 클릭합니다.



**① 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 저장소에 가져오기**를 선택하고 다음을 클릭합니다.  
*자체 서명 인증 대화상자*에 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.

**① 노트:**

기본적으로 인증서 유효 기간은 1년입니다.

- 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 다음을 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.

**① 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 Data Protection 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 증명(사용자 이름 및 암호 필드를 수정할 수 없음)이 인증에 사용됩니다(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 다음을 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 인증**을 선택하고 다음을 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 Dell Enterprise Server에서 작업할 때 Dell 서비스에서 사용됩니다.

또는

- **SQL 서버 인증**

아래의 자격 증명을 사용해 **SQL 서버 인증**을 선택하고 Dell Enterprise Server에서 작업할 때 사용할 Dell 서비스에 대한 SQL 서버 자격 증명을 입력하고 다음을 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. 서버를 다시 부팅할 필요는 없습니다.

## 기존 데이터베이스와 함께 백엔드 서버 설치

### ① 노트:

Dell Enterprise Server v8.x 이상을 사용하고 있는 경우 백엔드 서버 업그레이드/마이그레이션의 지침을 참조하십시오.

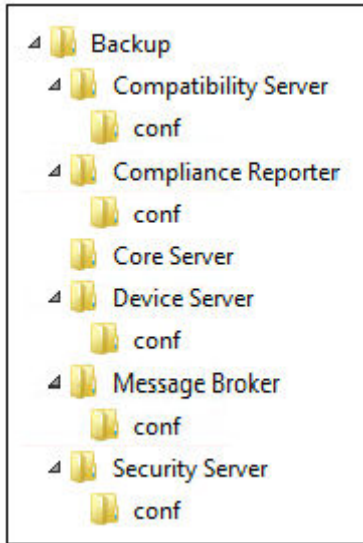
스키마 버전이 설치할 Dell Enterprise Server 버전과 일치하는 경우 Dell Enterprise Server를 새로 설치하고 사전 설치 구성 도중에 생성된 SQL 데이터베이스에 연결하거나 v9.x 이상인 기존 SQL 데이터베이스에 연결할 수 있습니다.

v8.x 이상의 데이터베이스는 최신 버전의 Server 구성 도구를 사용하여 최신 스키마로 마이그레이션해야 합니다. Server 구성 도구로 데이터베이스 마이그레이션의 지침을 보려면 **데이터베이스 마이그레이션**을 참조하십시오. 최신 Server 구성 도구를 가져오거나 **v8.0 이전의 데이터베이스를 마이그레이션하려면** Dell ProSupport에 문의하십시오.

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

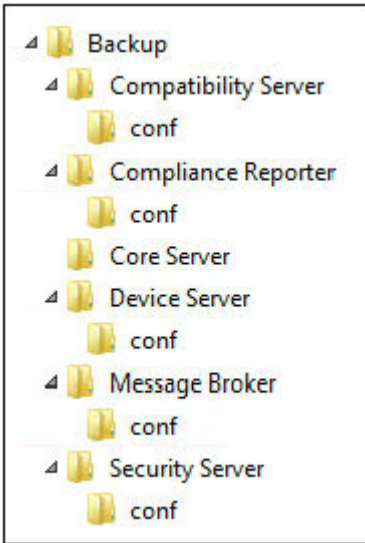




- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Dell Enterprise Server-x64를 Enterprise Server를 설치할 서버의 루트 디렉토리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). **복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.**
- 2 **setup.exe**를 더블 클릭합니다.
- 3 *InstallShield 마법사* 대화상자에서, 설치 언어를 선택한 후 **확인**을 클릭합니다.
- 4 필수 구성요소가 아직 설치되어 있지 않으면, 필수 구성요소가 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.
- 5 *시작* 대화상자에서 **다음**을 클릭합니다.
- 6 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.
- 7 선택적으로 **사전 설치 구성**에서 **9단계**를 완료한 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 Dell Enterprise Server를 기본 위치인 C:\Program Files\Dell에 설치하려면 **다음**을 클릭합니다. 그렇지 않으면, **변경**을 클릭하여 다른 위치를 선택하고 **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 수동으로 서버를 복원하는 데 필요한 전체 정보에서 중요한 역할을 합니다.

**① | 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 가져오기를 선택하고 다음을 클릭합니다. **찾아보기**를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 [Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 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 저장소에 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.



① **노트:**

기본적으로 인증서 유효 기간은 1년입니다.

12 Server Encryption(SE)에서, 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. **찾아보기**를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 [Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 참조하십시오.

**다음**을 클릭합니다.

① **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 저장소에 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

**다음**을 클릭합니다.

① **노트:**

기본적으로 인증서 유효 기간은 1년입니다.

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.

① **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 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 필드를 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.

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

- **Windows 인증을 사용하려면**

**아래의 자격 증명을 사용해 Windows 인증**을 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.

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 Enterprise Server의 올바른 버전을 재설치하고 업그레이드할 최신 설치 프로그램을 실행한 *이후에만* 사용해야 합니다.
- **데이터베이스 마이그레이션 없이 진행** 옵션은 데이터베이스를 완전히 구성하지 않은 상태에서 Enterprise Server를 설치합니다. 데이터베이스 구성은 Server 구성 도구를 사용하여 수동으로 나중에 완료해야 하고 추가 수동 변경이 필요합니다.

- b 데이터베이스 스키마가 현재 버전의 스키마이지만 Dell Enterprise Server backend에 연결되어 있지 않은 경우, **복구로 간주합니다**. 다음 대화상자가 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.

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 Dell Enterprise Server와 함께 사용하기 위한 프론트 엔드(DMZ 모드) 옵션을 제공합니다. DMZ에 Dell 구성요소를 배포하려면, 구성요소가 공격으로부터 적절히 보호를 받을 수 있는지 확인해야 합니다.

① **노트:** 보호된 Office 모드를 실행할 때 Data Guardian이 보호하는 모든 파일에 콜백 비콘을 삽입하는 Data Guardian 콜백 비콘을 지원하기 위해 이 설치 과정의 일부로 비콘 서비스가 설치됩니다. 이렇게 하면 Dell 프론트 엔드 서버와 모든 위치의 모든 장치 사이에서 통신을 할 수 있습니다. 콜백 비콘을 사용하기 전에 필요한 네트워크 보안이 구성되어 있는지 확인합니다. 기본적으로 콜백 비콘 활성화 정책이 활성화됩니다.

설치를 수행하려면 DMZ 서버의 정규화된 호스트 이름이 필요합니다.

- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Dell Enterprise Server-x64를 Enterprise Server를 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 *InstallShield 마법사* 대화상자에서, 설치 언어를 선택한 후 **확인**을 클릭합니다.
- 4 필수 구성요소가 아직 설치되어 있지 않으면, 필수 구성요소가 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.
- 5 *시작* 대화상자에서 **다음**을 클릭합니다.
- 6 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.
- 7 제품 키를 입력합니다.
- 8 **프론트 엔드 설치**를 선택하고 **다음**을 클릭합니다.
- 9 프론트 엔드 서버를 기본 위치인 C:\Program Files\Dell에 설치하려면 **다음**을 클릭합니다. 그렇지 않으면, **변경**을 클릭하여 다른 위치를 선택하고 **다음**을 클릭합니다.
- 10 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. **찾아보기**를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다. 지침은 [Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 참조하십시오.

**다음**을 클릭합니다.

① **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 저장소에 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

다음

**노트:**

기본적으로 인증서 유효 기간은 1년입니다.

- 11 *프론트 엔드 서버 설정* 대화상자에서, 백 엔드 서버의 정규화된 호스트 이름이나 DNS 별칭을 입력하고 **Enterprise Edition**을 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

Dell Enterprise Server v8.0 이상을 Dell Enterprise Server v9.x로 업그레이드할 수 있습니다. 서버 버전이 v8.0 보다 오래된 경우, 먼저 v8.0으로 업그레이드한 다음 v9.x로 업그레이드해야 합니다.

## 업그레이드/마이그레이션을 시작하기 전에

시작하기 전에 모든 **사전 설치 구성**이 완료되었는지 확인하십시오. Mobile Edition을 배포하는 경우에 이 과정이 특히 중요합니다.

Dell Enterprise Server 설치와 관련된 모든 최신 해결 방법이나 알려진 문제를 확인하려면 *Enterprise Server 기술 관련 문서*를 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 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, Dell Enterprise Server와 클라이언트 모두 가장 최신 버전으로 업데이트할 것을 권장합니다.

Dell Enterprise Server v9.x는 다음을 지원합니다.

- Enterprise Edition:
  - Windows 클라이언트 v7.x/8.x
  - Mac 클라이언트 v7.x/8.x
  - SED 클라이언트 v8.x
  - Authentication v8.x
  - BitLocker Manager v7.2x+ 및 v8.x
  - Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Dell Enterprise Server v8.x 이상에서 업그레이드/마이그레이션합니다. (v8.x 이전 Dell Enterprise Server에서 마이그레이션하는 경우, Dell ProSupport에 연락하여 도움을 요청합니다.)

사용자의 Dell Enterprise 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 Dell Enterprise Server와 그 구성요소들을 업그레이드/마이그레이션한 후에 클라이언트 설치/업그레이드를 수행하는 것입니다.

### 정책 변경사항 적용

- 1 Dell 관리자 계정으로 원격 관리 콘솔에 로그인합니다.
- 2 왼쪽 메뉴에서 **관리** > **커밋**을 클릭합니다.
- 3 설명 필드에 변경에 대한 설명을 입력합니다.
- 4 **정책 커밋**을 클릭합니다.
- 5 커밋이 완료되면, Remote 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.

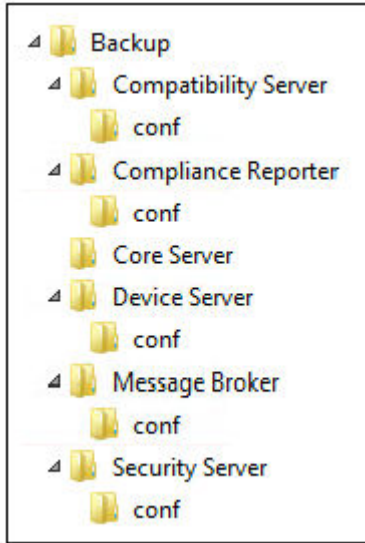
### 기존 설치 백업

- 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.

### ① 노트:

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

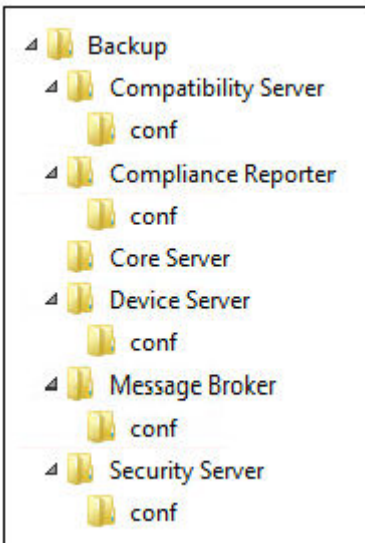




## 백엔드 서버 업그레이드/마이그레이션

- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Enterprise Server-x64를 Enterprise Server를 설치할 서버의 루트 디렉토리에 **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 *InstallShield 마법사* 대화상자에서, 설치 언어를 선택한 후 **확인**을 클릭합니다.
- 4 시작 대화상자에서 **다음**을 클릭합니다.
- 5 라이선스 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 필드를 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 다음을 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 다음을 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 백업되었습니다를 선택하고 다음을 클릭합니다.

10 설치를 클릭하고 설치를 시작합니다.

진행률 대화상자에 업그레이드 과정 상태가 표시됩니다.

11 설치가 완료되면 마침을 클릭합니다.

마이그레이션이 끝나면 Dell 서비스가 다시 시작됩니다. 서버를 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 디렉토리>\conf\secretKeyStore를 새 설치 정보

<Compatibility Server 설치 디렉토리>\conf\secretKeyStore에 복사하여 붙여넣습니다.

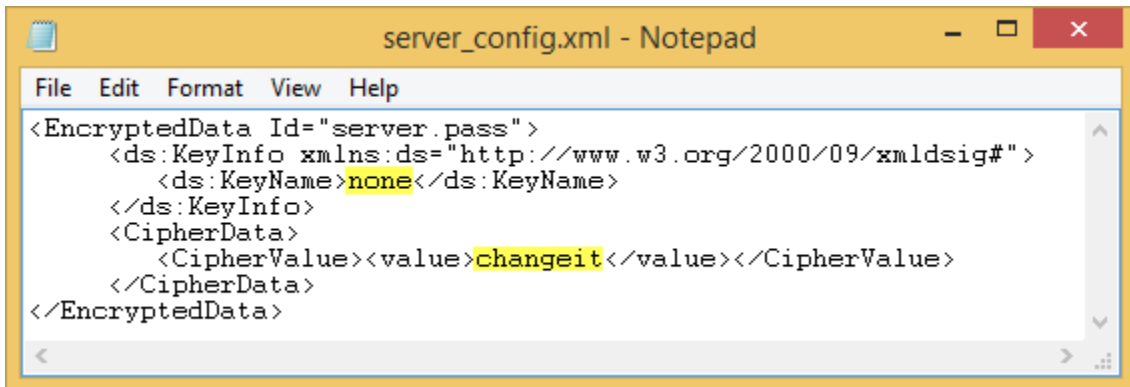
13 새 설치에서, <Compatibility Server 설치 디렉토리>\conf\server\_config.xml을 열고 server.pass 값을 다음과 같이 백업된 <Compatibility Server 설치 디렉토리>\conf\server\_config.xml의 값으로 교체합니다.

server.pass에 대한 지침:

암호를 알고 있는 경우, 의 견본 server\_config.xml 파일을 참조하여 다음과 같이 수정하십시오.

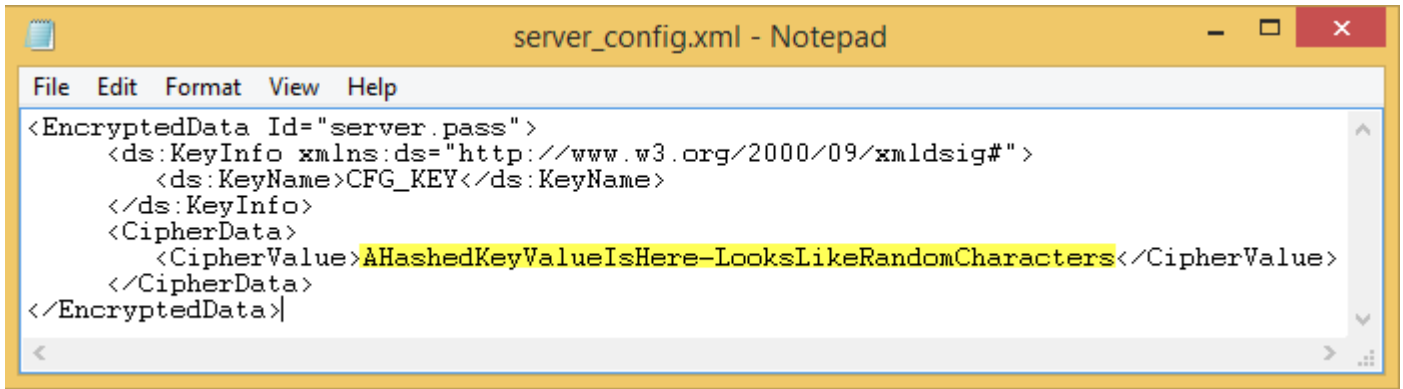
- KeyName을 CFG\_KEY 값에서 none으로 편집합니다.
- 일반 텍스트 암호를 입력하고 이를 <value> </value>로 묶습니다. 이 예에서는 <value>changeit</value>과 같습니다.
- Dell Enterprise Server가 시작되면, 일반 텍스트 암호가 해시되고 이 해시값이 일반 텍스트를 대체합니다.

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.

#### ① 노트:

나중이라도 server\_config.xml의 server.pass 값을 편집하여 Dell Enterprise Server 암호를 변경하려 하지 마십시오. 이 값을 변경하면, 데이터베이스에 대한 액세스 권한을 잃습니다.

백엔드 서버 마이그레이션 작업이 완료됩니다.

## 프론트 엔드 서버 업그레이드/마이그레이션

① **노트:** v9.5부터 비콘 서비스가 기본 호스트 이름과 8446 포트를 사용하여 이 업그레이드의 일부로 설치됩니다. 비콘 서비스는 보호된 Office 모드를 실행할 때 Data Guardian에서 보호하는 모든 파일에 콜백 비콘을 삽입하는 Data Guardian 콜백 비콘을 지원합니다. 이렇게 하면 Dell 프론트 엔드 서버와 모든 위치의 모든 장치 사이에서 통신을 할 수 있습니다. 기본적으로 콜백 비콘 활성화 정책이 활성화됩니다. 콜백 비콘을 사용하기 전에 필요한 네트워크 보안이 구성되어 있는지 확인합니다.

- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Enterprise Server-x64를 Enterprise Server를 설치할 서버의 루트 디렉토리에 압축 해제합니다(복사/붙여넣기 또는 드래그/드롭은 안 됨). 복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.
  - 2 setup.exe를 더블 클릭합니다.
  - 3 InstallShield 마법사 대화상자에서, 설치 언어를 선택한 후 확인을 클릭합니다.
  - 4 필수 구성요소가 아직 설치되어 있지 않으면, 필수 구성요소가 설치된다는 메시지가 표시됩니다. 설치를 클릭합니다.
  - 5 시작대화상자에서 다음을 클릭합니다.
  - 6 라이선스 계약을 읽고 조건을 수락한 후 다음을 클릭합니다.
  - 7 프로그램 설치 준비 완료 대화상자에서 설치를 클릭합니다  
진행률 대화상자에 설치 과정 상태가 표시됩니다.
  - 8 설치가 완료되면 마침을 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 서버를 다시 부팅할 필요가 없습니다.



# 연결되지 않은 모드 설치

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

명령줄에서 연결되지 않은 모드로 Enterprise 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 버튼이 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 라이선스 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 - Enterprise 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



## 매개 변수

SSL\_ORGNAME

SSL\_UNITNAME

SSL\_COUNTRY - 선택 사항, 기본값 = "US"

SSL\_STATENAME

SSOS\_TYPE=*n* - 여기에서 *n*이 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 서버, 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 로그인한 사용자의 인증 자격 증명을 사용하여 SQL Server에 대한 인증을 한다는 것을 지정합니다. SQL 인증을 사용하려면 이 값을 1로 설정합니다.

**① | 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 증명입니다.

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 Enterprise Server에서 작업할 때 Dell 서비스에서 사용됩니다. Windows 인증을 사용하려면 이 값을 0으로 설정합니다. SQL 인증을 사용하려면 이 값을 1로 설정합니다.

**① | 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, public**을 가지고 있어야 합니다.

SQL\_EE\_USERNAME - 필수. Windows 인증에서는 DOMAIN\username 형식을 사용합니다. SQL 인증에서는 사용자 이름을 지정합니다.

## 매개 변수

SQL\_EE\_PASSWORD - 필수. Windows 또는 SQL 사용자 이름과 연관된 암호를 지정합니다.

SQL 인증을 사용하는 경우(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 로그인 이 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.

**① | 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.

TIGAPORT - 선택 사항.

SMTP\_PORT - 선택 사항.

ACTIVEMQ\_TCP - 선택 사항.

ACTIVEMQ\_STOMP - 선택 사항.



## 연결되지 않은 모드로 Enterprise Server 설치

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

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

## Dell Enterprise Server 제거

- 1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Dell Enterprise Server-x64를 Enterprise Server의 설치를 제거할 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 시작 대화상자에서 **다음**을 클릭합니다.
- 4 **프로그램 제거** 대화상자에서 **제거**를 클릭합니다. 진행률 대화상자에 제거 과정 상태가 표시됩니다.
- 5 제거가 완료되면 **마침**을 클릭합니다.



## 설치 후 구성

Dell Enterprise Server 구성과 관련된 최신 해결 방법이나 알려진 문제를 확인하려면 *Enterprise Server 기술 관련 문서*를 읽어 보십시오.

Dell Enterprise Server를 처음으로 설치하든 기존 설치를 업그레이드하든, 환경의 일부 구성 요소를 구성해야 합니다.

## EAS Management 설치 및 구성

Mobile Edition을 사용하려는 경우 이 섹션을 완료해야 합니다. 그렇지 않으면 이 섹션을 생략하고 [Dell Security Server\(DMZ Mode\) 구성](#)으로 계속 진행하십시오.

### 필수 조건

- EAS Mailbox Manager 서비스의 로그인 계정에는 Exchange ActiveSync 정책을 만들거나 수정하고, 사용자 사서함에 정책을 할당하며, ActiveSync 장치에 대한 정보를 쿼리할 권한이 있어야 합니다.
- 파일을 수정하고 서비스를 다시 시작하려면 EAS 구성 유틸리티를 관리자 권한으로 실행해야 합니다.
- Dell Policy Proxy로의 네트워크 연결이 필요합니다.
- Dell Policy Proxy의 FQDN을 활성화합니다.
- Dell Policy Proxy 포트 번호를 활성화합니다.
- Exchange 환경을 호스팅하는 서버에 이미 MSMQ(Microsoft Message Queuing)가 설치/구성되어 있어야 합니다. 그렇지 않은 경우에는 [Microsoft Message Queuing\(MSMQ\) 설치/구성](#)을 참조하십시오.

### 배포 프로세스 중

Exchange ActiveSync를 사용하여 Mobile Edition을 통해 모바일 장치를 관리하려면 Exchange Server 환경을 구성해야 합니다.

## EAS Device Manager 설치

- 1 Dell 설치 미디어에서 EAS Management 폴더를 찾습니다. EAS Device Manager 폴더에서, setup.exe를 *Exchange Client Access Server*에 복사합니다.
- 2 **setup.exe**를 더블 클릭하여 설치를 시작합니다. 해당 환경에 *Exchange Client Access Server*가 둘 이상 있을 경우 각 서버에서 이 설치 프로그램을 실행하십시오.
- 3 설치할 언어를 선택하고 **확인**을 클릭합니다.
- 4 **시작** 화면이 표시되면 **다음**을 클릭합니다.
- 5 라이선스 계약을 읽고 약관에 동의한 후 **다음**을 클릭합니다.
- 6 **다음**을 클릭하여 EAS Device Manager를 기본 위치인 C:\inetpub\wwwroot\Dell\EAS Device Manager\에 설치합니다.
- 7 **설치 시작 준비** 화면에서 **설치**를 클릭합니다.  
상태 창에 설치 진행률이 표시됩니다.
- 8 원하는 경우, 확인란을 선택하여 Windows 설치 프로그램 로그를 표시하고 **마침**을 클릭합니다.



# EAS Mailbox Manager 설치

- 1 Dell 설치 미디어에서 EAS Management 폴더를 찾습니다. EAS Mailbox Manager 폴더에서 setup.exe를 Exchange Mailbox Server에 복사합니다.
- 2 **setup.exe**를 더블 클릭하여 설치를 시작합니다. 해당 환경에 Exchange Mailbox Server가 둘 이상 있을 경우 각 서버에서 이 설치 프로그램을 실행하십시오.
- 3 설치할 언어를 선택하고 **확인**을 클릭합니다.
- 4 시작화면이 표시되면 **다음**을 클릭합니다.
- 5 라이선스 계약을 읽고 약관에 동의한 후 **다음**을 클릭합니다.
- 6 **다음**을 클릭하여 EAS Mailbox Manager를 기본 위치인 C:\Program Files\Dell\EAS Mailbox Manager\에 설치합니다.
- 7 로그인 정보 화면에서, 이 Service에 로그인할 사용자 계정의 자격 증명을 입력합니다.  
사용자 이름: DOMAIN\Username  
  
암호: 이 사용자 이름과 연관된 암호  
  
**다음**을 클릭합니다.
- 8 **설치 시작 준비** 화면에서 **설치**를 클릭합니다.  
상태 창에 설치 진행률이 표시됩니다.
- 9 원하는 경우, 확인란을 선택하여 Windows 설치 프로그램 로그를 표시하고 **마침**을 클릭합니다.

## EAS 구성 유틸리티 사용

- 1 동일한 컴퓨터에서 **시작 > Dell > EAS 구성 유틸리티 > EAS 구성**으로 이동하여 EAS 구성 유틸리티를 실행합니다.
  - 2 **설정**을 클릭하여 EAS Management 설정을 구성합니다.
  - 3 다음 정보를 입력합니다.  
Dell Policy Proxy의 FQDN  
  
Dell Policy Proxy 포트(기본 포트는 8090)  
  
Dell Policy Proxy 폴링 간격(기본값은 1분)  
  
보고 전용 모드에서 EAS Device Manager를 실행하려면 확인란을 선택합니다(배포 중 권장 사항).
- ① **노트:**  
보고 전용 모드에서는 알려지지 않은 장치/사용자가 Exchange ActiveSync에 액세스할 수 있도록 허용하지만 해당 트래픽을 계속 보고합니다. 배포가 정상적으로 완료되면 이 설정을 변경하여 보안을 강화할 수 있습니다.
- 4 **확인**을 클릭합니다.
  - 5 확인 메시지가 표시됩니다. **예**를 클릭하여 IIS 및 EAS Mailbox Manager 서비스를 다시 시작합니다.
  - 6 완료되면 **끝내기**를 클릭합니다.

## EAS 관리 설정 구성

배포가 정상적으로 완료되고 보안을 강화할 준비가 되면 다음 단계를 따르십시오.

- 1 **시작 > Dell > EAS 구성 유틸리티 > EAS 구성**으로 이동하여 EAS 구성 유틸리티를 실행합니다.
- 2 **설정**을 클릭하여 EAS Management 설정을 구성합니다.
- 3 다음 정보를 입력합니다.



Dell Policy Proxy의 FQDN

Dell Policy Proxy 포트(기본 포트는 8090)

Dell Policy Proxy 폴링 간격(기본값은 1분)

보고 전용 모드에서 EAS Device Manager를 실행한다는 확인란을 선택 해제합니다.

확인을 클릭합니다.

- 4 확인 메시지가 표시됩니다. 예를 클릭하여 IIS 및 EAS Mailbox Manager 서비스를 다시 시작합니다.
- 5 완료되면 **끝내기**를 클릭합니다.

## Dell Security Server(DMZ Mode) 구성

Dell 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 Dell Security Server의 Java 키 저장소에 추가하기 위해 약간의 수동 절차가 필요합니다.

신뢰할 수 있는 인증서를 사용하고 있는 경우, 이 섹션을 생략하고 [APN 등록](#)으로 이동하십시오.

① **노트:** DMZ와 개인 네트워크 서버 모두에 대해 신뢰할 수 있는 인증 기관의 도메인 인증서를 사용할 것을 강력히 권장합니다.

## Keytool을 사용하여 DMZ 도메인 인증서 가져오기

### ① 중요:

Keytool 지침을 따르기 전에 기존 Security Server의 cacerts 파일을 백업하십시오. 구성 오류가 발생할 경우, 저장된 파일로 되돌릴 수 있습니다.

### 전제 사항

- Security Server가 신뢰할 수 없는 인증서와 함께 설치되었습니다.
- Security Server(DMZ Mode)가 서명 인증서(Entrust, Verisign 등)를 사용하여 설치되었습니다.
- .pfx 인증서 파일이 유효합니다. 인증서를 .pfx로 변환해야 할 경우 Certificate Management Console을 사용하여 PFX에 인증서 내보 내기를 참조하십시오.

### 프로세스

- 1 시스템 경로에 Keytool을 추가합니다.

```
set path=%path%;<Dell Java Install Dir>\bin
```

- 2 Keytool을 사용하여, 가져오고자 하는 신뢰할 수 있는 도메인 인증서의 콘텐츠를 나열합니다. 나열된 별칭을 기록합니다.

```
keytool -list -v -keystore "
```

- 3 Keytool을 사용하여, 서명 인증서의 콘텐츠를 Security Server의 cacerts 파일로 가져옵니다.

```
keytool -importkeystore -v -srckeystore "
```

-srcalias의 경우, 서명 인증서에서 내보낸 콘텐츠로부터 이 정보를 수집해야 할 것입니다.

-destalias의 경우, 사용자가 선택하는 모든 위치가 될 수 있습니다.

- 4 \conf\ 디렉토리의 현재 cacerts 파일을 백업하고 이것을 Security Server에 새로 생성된 cacerts 파일로 교체합니다.



# application.properties 파일 수정

서명 인증서의 별칭을 명시하도록 application.properties 파일을 수정합니다.

- 1 \conf\application.properties로 이동합니다.
- 2 다음 정보를 수정합니다.  
keystore.alias.signing=<-destalias의 경우 위 3단계 값으로 이 값을 변경>
- 3 Dell Security Server 서비스를 다시 시작합니다.

## APN 등록

iOS 장치와 함께 Mobile Device Security용 Mobile Edition을 사용할 계획이라면 다음과 같은 용도로 APN 등록 마법사를 사용해야 합니다.

- CSR 생성
- Apple 푸시 인증서 생성
- 푸시 인증서 업로드

iOS 장치와 함께 Mobile Device Security용 Mobile Edition을 사용하지 않을 계획이라면 이 섹션을 생략하고 [Server 구성 도구](#)로 계속 진행하십시오.

Apple Push Notification 서비스(APN)는 iOS 장치와의 안전한 무선 통신을 가능하게 해줍니다. APN은 iOS 장치가 Dell Enterprise Server와 통신을 하도록 메시지를 전송하는 데 사용됩니다. APN은 해당 장치에 메시지만 전송하고 데이터는 전송하지 않습니다.

### 프로세스

- 1 브라우저를 열고 <https://<Security Server의 FQDN>:8443/csrweb>으로 이동합니다.
- 2 APN 등록 마법사 로그인 대화상자에서, 사용자의 Dell 관리자 자격 증명을 입력하고 **로그인**을 클릭합니다.
- 3 사용자가 수행해야 할 단계를 설명하는 대화상자가 표시됩니다. **다음**을 클릭합니다.

#### I단계: CSR 생성

- 4 다음 정보를 입력합니다.

이메일: 이메일 주소로는 모든 UPN이 가능하지만, APN 인증서를 보존할 관리자의 계정을 사용할 것을 권장합니다.

공통 이름: 이메일 주소와 관련된 공통 이름을 입력합니다.

**CSR 생성**을 클릭합니다.

- 5 CSR을 생성한 후, 해당 파일을 쉽게 액세스할 수 있는 위치에 저장합니다.
- 6 **다음**을 클릭합니다.

#### II단계: Apple 푸시 인증서를 생성합니다.

- 7 **Apple 푸시 인증서 포털** 링크를 클릭합니다. 사용자의 Apple ID와 암호로 로그인합니다.
- 8 이용 약관을 읽고 동의 의사를 표시하고 **동의**를 클릭합니다.
- 9 **찾아보기**를 클릭한 후 방금 생성한 CSR을 **업로드**합니다.
- 10 *제3자 서버를 위한 인증서* 페이지에서 **다운로드**를 클릭합니다. 쉽게 액세스할 수 있는 위치에 파일을 저장합니다.
- 11 APN 등록 마법사로 돌아가서 **다음**을 클릭합니다.

#### III단계: 푸시 인증서 업로드

- 12 다음 정보를 입력합니다(**I단계: CSR 생성**에서 사용한 것과 동일한 자격 증명을 사용함).

이메일:

공통 이름:

푸시 인증서 파일: **찾아보기**를 클릭하여 **7단계**에서 저장한 파일을 찾습니다. **업로드**를 클릭합니다.

13 확인 메시지가 표시됩니다. **마침**을 클릭합니다.

Dell Enterprise Server에 APN 인증서 등록이 완료되었습니다.

## Server 구성 도구

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

Dell Server 구성 도구를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

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

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

Dell Server 구성 도구를 실행하려면 **시작 > 프로그램 > Dell > Enterprise Edition > Server 구성 도구 > Server 구성 도구 실행**으로 이동합니다.

Dell Server 구성 도구가 C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs에 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 등에만 적합합니다. 프로덕션 환경이라면은 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: Dell Device Server 등)
- .NET 응용 프로그램(Dell Core Server)
- 부팅 전 인증을 위해 사용하는 스마트 카드의 유효성 검사(Dell Security Server)
- Dell Manager로 보내는 정책 번들에 서명할 때 사용할 개인 암호화 키 가져오기 Dell Manager는 자체 암호화 드라이브 또는 BitLocker Manager가 탑재된 원격 관리 Enterprise Edition 클라이언트에 대해 SSL 유효성을 검사합니다.
- 클라이언트 워크스테이션:
  - BitLocker Manager를 실행하는 워크스테이션
  - Enterprise Edition을 실행하는 워크스테이션(Windows 클라이언트)
  - Endpoint Security Suite를 실행하는 워크스테이션
  - Endpoint Security Suite Enterprise를 실행하는 워크스테이션

**사용할 인증서 유형과 관련된 정보:**



스마트 카드를 사용해 부팅 전 인증을 실행하려면 Dell 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 구성요소에 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 Dell Security Server Java 키 저장소로 가져옵니다. 자세한 내용은 자체 서명 인증서 생성 및 CSR(Certificate Signing Request) 생성을 참조하십시오. 전체 신뢰 체인을 가져와야 합니다.

Dell Manager:

- Microsoft 키 저장소 워크스테이션의 "Trusted Root Certification Authorities(안전한 루트 인증서 인증 기관)"에 "Root Agency" 서명 인증서를 삽입합니다(생성된 자체 서명 인증서에서).
- 서버측 SSL 유효성 검사의 동작을 수정합니다. 서버측 SSL 신뢰 유효성 검사를 끄려면 설정 탭에서 **신뢰 체인 검사 비활성화**를 선택합니다.

인증서를 만드는 방법은 *Express*(빠른 생성)와 *Advanced*(고급)의 두 가지가 있습니다.

**한 가지** 방법을 선택합니다.

- **빠른 생성** - 모든 구성요소에 대해 자체 서명 인증서를 생성하려면 이 방법을 선택합니다. 가장 쉬운 방법이지만 자체 서명된 인증서는 파일럿, POC 등에 적합합니다. 프로덕션 환경이라면 Dell은 공용 CA-서명 또는 도메인-서명 인증서를 권장합니다.
- **고급** - 각 구성요소를 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, Enterprise Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.
- 3 상단 메뉴에서 **구성 > 저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

인증서 설정이 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, Enterprise Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.
- 4 상단 메뉴에서 **구성 > 저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

인증서 설정이 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, Enterprise 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. 다음을 클릭합니다.

기존 인증서 위치를 탐색하여 기존 인증서와 연결된 암호를 입력하고 다음을 클릭합니다.

완료되면 **마침**을 클릭합니다.

- **자체 서명 인증서 생성** - 해당되는 경우, Enterprise 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. 다음을 클릭합니다.

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

완료되면 **마침**을 클릭합니다.

- **현재 설정 사용** - Dell Enterprise 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 하나를 선택합니다.

- **인증서 선택** - 기존 인증서를 사용하려면 이 옵션을 선택합니다. 다음을 클릭합니다.

기존 인증서 위치를 탐색하여 기존 인증서와 연결된 암호를 입력하고 다음을 클릭합니다.

완료되면 **마침**을 클릭합니다.

- **자체 서명 인증서 생성** - 해당되는 경우, Enterprise Server를 설치할 때 생성된 자체 서명 인증서의 정보가 사용될 것입니다.

다음을 클릭합니다.

완료되면 **마침**을 클릭합니다.

인증서 설정이 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. 서비스가 열리면 각 Dell Service로 이동하여 **서비스 시작**을 클릭합니다.

## Dell Manager 인증서 가져오기

배포 계획 중 자체 암호화 드라이브 또는 BitLocker Manager가 탑재된 원격 관리 Enterprise Edition 클라이언트가 포함된 경우에는 새로 생성한(또는 기존) 인증서를 가져와야 합니다. Dell Manager 인증서는 Enterprise Edition 원격 관리 클라이언트 및 BitLocker Manager로 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 추가창에서 **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 버튼으로 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** 필드에 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 > 관리자 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.

## ID 인증서 가져오기

배포 시 Server Encryption이 포함된 경우, 새로 생성한(또는 기존) 인증서를 가져와야 합니다. ID 인증서는 클라이언트 서버로 보내는 정책 번들 서명에 사용하는 개인 키를 보호합니다. 이 인증서는 다른 인증서와 별도로 존재할 수 있습니다.

- 1 상단 메뉴에서 **작업 > ID 인증서 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 로그인되어 있는 계정의 자격 증명을 계속 사용하려면 **다음**을 클릭합니다.
- 5 상단 메뉴에서 **구성 > 저장**을 선택합니다. 메시지가 나타나면 "저장"을 확인합니다.

# Server SSL 인증서 또는 Mobile Edition의 설정 구성

Server 구성 도구에서 **설정** 탭을 클릭합니다.

## Dell Manager:

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

## SCEP:

Mobile Edition을 사용하는 경우, SCEP를 호스팅하는 서버의 URL을 입력합니다.

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.

# Data Guardian 또는 이메일 서비스에 대한 SMTP 설정 구성

Server 구성 도구에서 **SMTP** 탭을 클릭합니다.

이 탭에서는 Data Guardian에 대한 SMTP 설정을 구성합니다. SMTP 설정을 Data Guardian 이외의 다른 목적으로 구성해야 할 경우, "라이선스 이메일 알림에 SMTP 서버 사용" 관리자 도움말 항목을 참조하십시오.

다음 정보를 입력합니다.

- 1 호스트 이름: 필드에 사용자의 SMTP 서버의 FQDN을 입력합니다(예: smtpservername.domain.com).
- 2 사용자 이름: 필드에 메일 서버에 로그인할 사용자 이름을 입력합니다. 형식은 DOMAIN\jdoe, jdoe 또는 조직에서 요구하는 대로 사용할 수 있습니다.
- 3 암호: 필드에 사용자 이름과 연결된 암호를 입력합니다.
- 4 출처 주소: 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: 필드에 포트 번호를 입력합니다(일반적으로 25).
- 6 인증: 메뉴에서 "참" 또는 "거짓"을 선택합니다.

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 이름, 위치 또는 자격 증명 변경

Server 구성 도구에서 **데이터베이스** 탭을 클릭합니다.

- 1 서버 이름: 필드에 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: 필드에 포트 번호를 입력합니다.

비기본 SQL 서버 인스턴스를 사용할 때 *서버* 필드에서 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\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx)를 참조하십시오.

3 데이터베이스: 필드에 데이터베이스 이름을 입력합니다.

4 인증: 필드에서 **Windows 인증** 또는 **SQL Server 인증**을 선택합니다. Windows 인증을 선택하면 Windows에 로그인하는 데 사용한 자격 증명이 인증에 사용됩니다(사용자 이름 및 암호 필드를 수정할 수 없음).

5 사용자 이름: 필드에 이 데이터베이스와 관련된 적절한 사용자 이름을 입력합니다.

6 암호: 필드에 UserName 필드에 나열된 사용자 이름의 암호를 입력합니다.

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 Dell Enterprise 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.

#### ① 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\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx)를 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

최신 버전의 Server 구성 도구를 사용하여 v8.x 데이터베이스를 최신 스키마로 마이그레이션할 수 있습니다. 최신 Server 구성 도구를 가져오거나 v8.0 이전의 데이터베이스를 마이그레이션하려면 Dell ProSupport에 문의하십시오.

Server 구성 도구에서 **데이터베이스** 탭을 클릭합니다.


1 기존 Dell 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.

① 노트: 오류 메시지는 로 식별되며, 데이터베이스 작업이 실패했고 데이터베이스가 올바르게 마이그레이션되려면 먼저 정정 작업을 수행해야 함을 나타냅니다. **마침**을 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.



## 관리 작업

### Dell 관리자 역할 지정

- 1 Dell 관리자로 <https://server.domain.com:8443/webui/>에서 Remote Management Console에 로그인합니다. 기본 자격 증명은 **superadmin/changeit**입니다.
- 2 왼쪽 창에서 **채우기 > 도메인**을 클릭합니다.
- 3 사용자를 추가할 도메인을 클릭합니다.
- 4 도메인 세부 정보 페이지에서 **멤버** 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 Remote Management ConsoleEnterprise Server에서 로그아웃합니다.
- 2 Remote Management ConsoleEnterprise Server에 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 관리**를 클릭합니다.
- 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 설명 필드에 변경에 대한 설명을 입력합니다.

- 3 정책 커밋을 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.
- 3 두 가지 인증 방식이 지원됩니다. 구성을 위해 다음 중 하나를 선택합니다.
  - [Compliance Reporter로 SQL 인증 구성](#)
  - [Compliance Reporter로 Windows 인증 구성](#)

## Compliance Reporter로 SQL 인증 구성

v8.1의 경우, 데이터 원본이 처음부터 사전 구성되어 있습니다. 따라서 별도의 구성이 필요하지 않습니다. 데이터 원본 변경이 필요한 경우 아래의 단계를 수행하십시오.

- 1 데이터 원본을 설정하려면 상단 메뉴에서 **설정**을 클릭합니다. 왼쪽 메뉴에서 **데이터 원본**을 클릭합니다.
- 2 Dell 데이터베이스에 로그인하기 위해 사용자 이름을 입력합니다.
- 3 Dell 데이터베이스에 로그인하기 위해 암호를 입력합니다.
- 4 Dell 데이터베이스에 로그인하기 위해 호스트 이름을 입력합니다.
- 5 Dell 데이터베이스에 로그인하기 위해 데이터베이스 이름을 입력합니다.
- 6 허용되는 유향 연결의 최대 수를 입력합니다. 기본값은 2입니다.
- 7 허용되는 연결(활성)의 최대 수를 입력합니다. 기본값은 10입니다.
- 8 최대 대기 시간을 입력합니다(연결을 대기하는 최대 밀리초 수). -1은 무한대입니다.
- 9 데이터베이스 URL을 확인하고 Dell Compliance Reporter와 Dell 데이터베이스 사이의 연결을 테스트하려면, **연결 테스트**를 클릭합니다.
- 10 **업데이트**를 클릭합니다. 내용을 취소하려면 취소를 클릭합니다.  
관리 작업이 완료되었습니다. 이 장의 나머지 부분은 Windows 인증에 관한 내용이므로 Dell Compliance Reporter에 SQL 인증을 사용할 경우 이 내용은 무시해도 좋습니다.

**필요한 경우**, 계속해서 [자체 서명된 인증서를 생성하고 인증서 서명 요청을 생성하거나 Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 수행하십시오.

## Compliance Reporter로 Windows 인증 구성

v8.1의 경우, 데이터 원본이 처음부터 사전 구성되어 있습니다. 따라서 별도의 구성이 필요하지 않습니다. 데이터 원본 변경이 필요한 경우 아래의 단계를 수행하십시오.

- 1 Dell 데이터베이스에 로그인하기 위해 사용자 이름을 입력합니다.
- 2 암호는 공백으로 남겨두십시오. 도메인 사용자가 로그인하면, 그 암호가 데이터베이스로 전달됩니다.
- 3 Dell 데이터베이스에 로그인하기 위해 호스트 이름을 입력합니다.
- 4 Dell 데이터베이스에 로그인하기 위해 데이터베이스 이름을 입력합니다.
- 5 허용되는 유향 연결의 최대 수를 입력합니다. 기본값은 2입니다.
- 6 허용되는 연결(활성)의 최대 수를 입력합니다. 기본값은 10입니다.
- 7 최대 대기 시간을 입력합니다(연결을 대기하는 최대 밀리초 수). -1은 무한대입니다.
- 8 데이터베이스 URL을 확인하고 Dell Compliance Reporter와 Dell 데이터베이스 사이의 연결을 테스트하려면 **연결 테스트**를 클릭합니다.
- 9 **업데이트**를 클릭합니다. 내용을 취소하려면 취소를 클릭합니다.  
관리 작업이 완료되었습니다. **필요한 경우**, 계속해서 [자체 서명된 인증서를 생성하고 인증서 서명 요청을 생성하거나 Certificate Management Console을 사용하여 PFX에 인증서 내보내기](#)를 수행하십시오.



# 백업 실행

재난 복구를 목적으로 매주 야간에 다음 위치에 대한 백업을 실행해야 합니다.

## Enterprise 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\gkresource.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 Dell 데이터베이스에 데이터베이스 모범 사례를 사용하고 조직의 재해 복구 계획에 Dell 소프트웨어를 포함시킬 것을 권장합니다.

SQL Server 모범 사례에 대한 추가 정보는 [다음 목록은 SQL Server 모범 사례로서 Dell Data Protection 설치 시 구현하지 않았다면 반드시 구현해야 합니다.](#)를 참조하십시오.

## PostgreSQL Server 백업

감사 이벤트가 PostgreSQL Server에 저장되며, 정기적으로 백업해야 합니다. 백업 지침은 <https://www.postgresql.org/docs/9.5/static/backup.html>을 참조하십시오.

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

## Dell 구성 요소 설명

다음 표는 각 구성요소와 그 기능에 대한 설명입니다.

이름	설명	필요한 분야
Compliance Reporter	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다.  Dell Enterprise Server의 구성요소.	보고
Key Server	Kerberos API를 사용하여 클라이언트 연결을 협상, 인증 및 암호화합니다.  주요 데이터를 가져오기 위해 SQL 데이터베이스 액세스가 필요합니다.  Dell Enterprise Server의 구성요소.	Dell 관리자 유틸리티
Server 구성 도구	Core Server 및 Compatibility Server/ Security Server와의 데이터베이스 통신을 구성합니다. 설치 시 데이터베이스를 초기화하거나 데이터베이스를 더 새로운 스키마로 마이그레이션하는 데 사용됩니다. Dell 서비스를 제어할 때 사용됩니다.  Dell Enterprise Server의 구성요소.	모두
Remote Management Console/Enterprise Server Console	전체 엔터프라이즈 배포를 위한 관리 콘솔 및 제어 센터입니다.  Dell Enterprise Server의 구성요소.	모두
Core Server	정책 흐름, 라이선스 및 사전 부팅 인증을 위한 등록, SED 관리, BitLocker 관리자, 위협 차단 및 고급 위협 차단을 관리합니다. Compliance Reporter 및 Remote Management Console을 통해 사용할 인벤토리 데이터를 프로세스합니다. 인증 데이터를 수집하고 보관합니다. 역할 기반 액세스를 관리합니다.  Dell Enterprise Server의 구성요소.	모두
Security Server	Policy Proxy와 통신합니다. 포렌직 키 검색, 클라이언트 활성화, Data Guardian 제품, SED-PBA 통신을 관리하고, Remote Management Console에 인증을 위한 ID 확인을 포함한 인증 또는 조정을 위한 Active Directory 통신도 관리합니다. SQL 데이터베이스 액세스가 필요합니다.  Dell Enterprise Server의 구성요소.	모두
Compatibility Server	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이	모두



이름	설명	필요한 분야
	터, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 이 서비스의 사용자 그룹에 기반하여 데이터를 프로세스합니다.	
	Dell Enterprise Server의 구성요소.	
Message Broker 서비스	Enterprise Server의 서비스 간 통신을 처리합니다. Policy Proxy 큐에 대한 Compatibility Server가 생성한 정책 정보 단계를 제공합니다.  SQL 데이터베이스 액세스가 필요합니다.  Dell Enterprise Server의 구성요소.	모두
Device Server	활성화 및 암호 복구를 지원합니다.  Dell Enterprise Server의 구성요소.	Mac용 Enterprise Edition Windows용 Enterprise Edition Handheld Shields CREDActivate
Device Server 플러그인	여러 구성요소를 지원합니다.  Dell Enterprise Server의 구성요소.	모두
Identity Server	도메인 인증 요청을 처리합니다.  Active Directory 계정이 필요합니다.  Windows 인증 사용 시 SQL에 액세스할 때 사용된 계정이어야 합니다.  Dell Enterprise Server의 구성요소.	모두
Policy Proxy	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다.  Dell Enterprise Server의 구성요소.	Mac용 Enterprise Edition Windows용 Enterprise Edition Mobile Device Security용 Mobile Edition
Security Token Services(STS)	Dell Enterprise Server 사용자 인터페이스와 Dell 백 엔드 서비스 사이에 보안 인증 채널을 생성하는 것을 돕는 데 사용됩니다.	모두
EAS Device Manager	무선 기능을 가능하게 해줍니다. Exchange Client Access Server에 설치됩니다.	모바일 장치의 Exchange ActiveSync를 관리합니다.
EAS Mailbox Manager	Exchange Mailbox Server에 설치되는 메일박스 에이전트입니다.	모바일 장치의 Exchange ActiveSync를 관리합니다.

## SQL Server 모범 사례

다음 목록은 SQL Server 모범 사례로서 Dell Data Protection 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.

- Microsoft SQL Server 2008 - <http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - [http://technet.microsoft.com/en-us/library/ms190969\(v=sql.105\).aspx](http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx)

- 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 2008 - <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29>
- Microsoft SQL Server 2012 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.110\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.110))
- Microsoft SQL Server 2014 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.120\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.120))
- Microsoft SQL Server 2016 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.130\)](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 2008 - <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29>
- 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>

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



## 인증서

# 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 개발 및 테스트 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 할 것입니다.

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 Dell Compliance Reporter, Dell Security Server 또는 Dell Device Server의 **conf** 디렉토리로 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.

### ① 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 **Dell Enterprise Server**를 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\eserver.properties. eserver.keystore.password = 값 설정
```

```
<Security Server install dir>\conf\eserver.properties. eserver.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 생성**에서 만든 자체 서명 인증서에 대해 CSR(Certificate Signing Request)을 생성하려면 이 절차를 사용합니다.

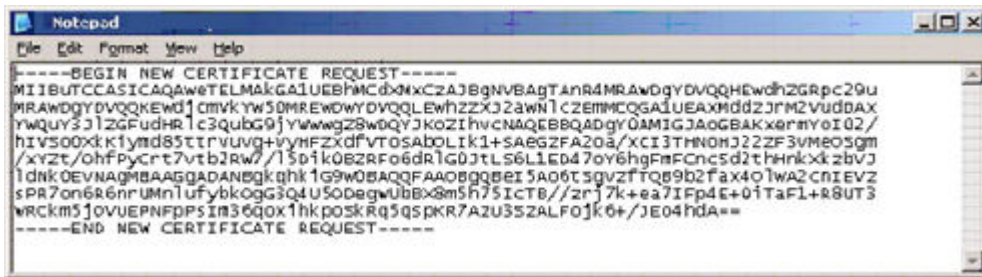
- 1 이전에 <**certificatealias**>에 사용된 값과 동일한 값으로 대체합니다.

```
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. 이와 같이 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.



- 다음 중 **하나**를 수행하십시오.
  - 인증 기관 루트 인증서를 다운로드하고 파일에 저장합니다.
  - 엔터프라이즈 디렉토리 서버 루트 인증서를 얻습니다.
- 다음 중 **하나**를 수행하십시오.
  - Dell Compliance Reporter, Dell Console Web Services, Dell Security Server 또는 Dell Device Server에 대한 SSL을 활성화하려는 경우, 구성 요소 **conf** 디렉토리로 변경합니다.
  - Dell Enterprise Server와 엔터프라이즈 서버 사이에서 SSL을 활성화하려면 <Dell install dir>\Java Runtimes\jre1.x.x\_xx\lib\security로 변경합니다(JRE cacerts의 기본 암호는 **changeit**).
- 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.

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

### Microsoft 인증서 서비스

- 고급 요청**을 선택하고 **다음**을 클릭합니다.

### 요청 유형 선택

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

### 고급 인증서 요청

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

### 저장된 요청 제출

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

### CA 인증서 다운로드

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

### CA 인증서 경로 다운로드

- 변환된 서명 기관 인증서를 가져옵니다. DOS 창으로 돌아갑니다. 유형:

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

- 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 2라는 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, Dell 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 버튼으로 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** 필드에 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.

