Dell Security Management Server Virtual

Quick Start and Installation Guide v10.2.4

참고, 주의 및 경고

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.

Dell Encryption, Endpoint Security Suite Enterprise 및 Data Guardian 문서 세트에 사용된 등록된 상표 및 상표, 즉 Dell™ 및 Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc. Cylance®, CylancePROTECT의 상표이고 Cylance 로고는 미국 및 다른 국가에서 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® 및 Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Azure®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and 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. Dropbox 는 Dropbox, Inc의 서비스 표시입니다. Google™, Android™, Google™ Chrome™, Gmail™ 및 Google™ Play는 미국 및 기타 국가에서 Google Inc.의 상표 또는 등록 상표입니다. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®과 iPod nano®, Macintosh® 및 Safari®는 미국 및/또는 기타 국가에서 Apple, Inc.의 서비스 표시, 상표, 또는 등록 상표입니다. EnCase™ 및 Guidance Software®는 Guidance Software의 상표 또는 등록 상표입니다. Entrust®는 미국 및 기타 국가에서 Entrust®, 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. Travelstar®는 미국 및 기타 국가에서 HGST, Inc.의 등록 상표입니다. UNIX®는 The Open Group의 등록 상표입니다. VALIDITY™는 미국 및 기타 국가에서 사용되는 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. Bing®는 Microsoft Inc. Ask®의 등록 상표입니다. Ask®는 IAC Publishing, LLC의 등록 상표입니다. 기타 이름은 해당 소유자의 상표일 수 있습니다.

2019 - 05

Rev. A01

Contents

1

퀵 스타트 가이드

이 퀵 스타트 가이드는 숙련된 사용자가 Dell Server를 가동하여 신속하게 실행할 수 있도록 합니다. 일반적으로 Dell Server를 먼저 설치한 다음 클라이언트를 설치하는 것이 좋습니다.

자세한 지침은 Security Management Server Virtual 설치 가이드를 참조하십시오.

Dell Server 사전 요구 사항에 대한 자세한 내용은 Security Management Server Virtual 사전 요구 사항, 관리 콘솔 사전 요구 사항 및 프록시 모드 사전 요구 사항을 참조하십시오.

기존 Dell Server를 업데이트하는 방법에 대한 자세한 내용은 Security Management Server Virtual 업데이트를 참조하십시오.

설치

1 Dell Data Security 파일이 저장된 디렉토리를 탐색한 다음 더블 클릭하여 VMware Security Management Server Virtual **v10.x.x Build x.ova**로 가져옵니다.

> **노트: 현재 OVA는 SHA256 서명을 가지고 있으므로 VMware 씩 클라이언트 내에서 가져올 수 없습니다. 자세한 정보는 https://kb.vmware.com/s/article/2151537를 참조하십시오.**

2 Security Management Server Virtual 전원 켜기

3 화면의 지침을 따릅니다.

구성

사용자를 활성화하기 전에 Security Management Server Virtual 터미널에서 다음과 같은 구성 작업을 완료해야 합니다.

- SMTP 설정 구성
- 기존 인증서 가져오기 또는 새 서버 인증서 등록
- Security Management Server Virtual 업데이트
- 포트 22에서 SFTP를 지원하는 FTP 클라이언트를 설치하고 파일 전송(FTP) 사용자 설정을 참조하십시오.

  조직에 외부 방향 장치가 있는 경우에는 프록시 모드 설치 및 구성을 참조하십시오.

Management Console 열기

다음 주소에서 Management Console 열기: https://server.domain.com:8443/webui/

기본 자격 증명은 **superadmin/changeit**입니다.

지원되는 웹 브라우저의 목록은 Management Console Prerequisites를 참조하십시오.

관리 작업

Management Console을 시작하지 않았으면 바로 시작합니다. 기본 자격 증명은 **superadmin/changeit**입니다.

관리자 역할은 최대한 빨리 할당하는 것이 좋습니다. 이 작업을 지금 완료하려면 Dell 관리자 역할 지정을 참조하십시오.

*AdminHelp*를 시작하려면 Management Console 오른쪽 상단 모서리에 있는 "?"를 클릭합니다. *시작하기* 페이지가 표시됩니다. **도메인 추가**를 클릭합니다.

고객을 위해 기준 정책이 설정된 상태지만 다음과 같은 특정 요구 사항에 따라 수정해야 합니다(라이선스 및 권한에 따라 모두 활성화 가능).

- 정책 기반 암호화가 공통 키 암호화로 활성화됩니다.
- 자체 암호화 드라이브가 포함된 컴퓨터 암호화
- BitLocker 관리를 사용하지 않음
- 고급 위협 방지가 켜지지 않았습니다.
- 위협 차단이 비활성화되어 있습니다.
- 외부 미디어를 암호화하지 않습니다.
- 포트는 포트 제어로 관리되지 않습니다.
- 설치된 전체 디스크 암호화 장치는 암호화되지 않습니다.
- Data Guardian이 비활성화되어 있습니다.

AdminHelp 주제 *정책 관리*에서 기술 그룹 및 정책 설명으로 가십시오.

퀵 스타트 작업이 완료되었습니다.

2

상세 설치 가이드

이 설치 가이드는 초보자를 위한 Security Management Server Virtual 설치 및 구성 가이드입니다. 일반적으로 Security Management Server Virtual을 먼저 설치한 다음 클라이언트를 설치하는 것이 좋습니다.

기존 Security Management Server Virtual을 업데이트하는 방법에 대한 자세한 내용은 Security Management Server Virtual 업데이트를 참조하십시오.

Security Management Server Virtual 정보

Management Console을 사용하면 관리자가 기업 전체에 걸쳐 엔드포인트, 정책 적용 및 보호 상태를 모니터링할 수 있습니다. 프록시 모드는 Security Management Server Virtual에서 사용할 수 있는 프론트 엔드 DMZ Mode 옵션을 제공합니다.

Security Management Server Virtual의 특징은 다음과 같습니다.

- 최대 3,500대 장치에 대한 중앙 집중화된 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 에스크로
- 중앙 집중화된 준수 감사 및 보고
- 자체 서명 인증서의 자동 생성

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.

요구 사항

Security Management Server Virtual

Hardware

The recommended disk space for Security Management Server Virtual is 80 GB.

Virtualized Environment

Security Management Server Virtual v10.2.3 has been validated with the following virtualized environments.

Dell currently supports hosting the Dell Security Management Server or Dell Security Management Server Virtual within a Cloud-hosted Infrastructure as a Service (IaaS) environment, such as Amazon Web Services, Azure, and several other vendors. Support for these environments will only be limited to the functionality of the application server hosted within these Virtual Machines, the administration and security of these Virtual Machines will be up to the administrator of the IaaS solution.

Additional infrastructure requirements (Active Directory, as well as SQL Server for the Dell Security Management Server) are still required for proper functionality.

Virtualized Environments

- VMware Workstation 12.5
  - 64-bit CPU required
  - 8GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware Workstation 14.0
  - 64-bit CPU required
  - 8 GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware Workstation 14.1
  - 64-bit CPU required
  - 8 GB RAM required
  - 80 GB Hard Drive Space
  - Host computer with at least two cores
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware ESXi 6.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

Virtualized Environments

- VMware ESXi 6.0
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- VMware ESXi 5.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An Operating System is not required
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - See https://kb.vmware.com/s/article/1003746 for more information

- Hyper-V Server (Full or Core installation)
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum required
  - 80 GB Hard Drive Space
  - An operating system is not required
  - Hardware must conform to minimum Hyper-V requirements
  - Must be run as a Generation 1 Virtual Machine

NOTE: For information on setting up Hyper-V, follow instructions for Endpoint Operating Systems: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v or for Server Operating Systems: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Management Console

Internet 브라우저

노트:
브라우저에서 쿠키를 허용해야 합니다.

다음 표에 지원되는 Internet 브라우저가 나와 있습니다.

Internet 브라우저

- Internet Explorer 11.x 이상

- Mozilla Firefox 41.x 이상
- Google Chrome 46.x 이상

프록시 모드

하드웨어

다음 표에는 *최소* 하드웨어 요구 사항이 자세히 나와 있습니다.

프로세서

Modern Dual-Core CPU(1.5Ghz +)

RAM

최소 2GB 전용 RAM/4GB 전용 RAM 권장

사용 가능한 디스크 공간

1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간)

네트워크 카드

10/100/1000 네트워크 인터페이스 카드

기타

IPv4, IPv6 또는 IPv4와 IPv6의 조합 지원

소프트웨어

다음 표에는 프록시 모드 서버 설치 전에 먼저 설치해야 하는 소프트웨어가 자세히 나와 있습니다.

사전 요구 사항

- **Windows Installer 4.0 이상**

  설치를 수행할 서버에 Windows Installer 4.0 이상이 설치되어 있어야 합니다.

- **Microsoft Visual C++ 2010 재배포 가능 패키지**

  설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.

- **Microsoft .NET Framework 버전 4.5.2**

  Microsoft는 .NET Framework 버전 4.5.2용 보안 업데이트를 게시했습니다.

노트:

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

Windows Server의 레지스트리 위치: HKLM\SOFTWARE\Dell

다음 표에는 프록시 모드 서버의 소프트웨어 요구 사항이 자세하게 나와 있습니다.

운영 체제

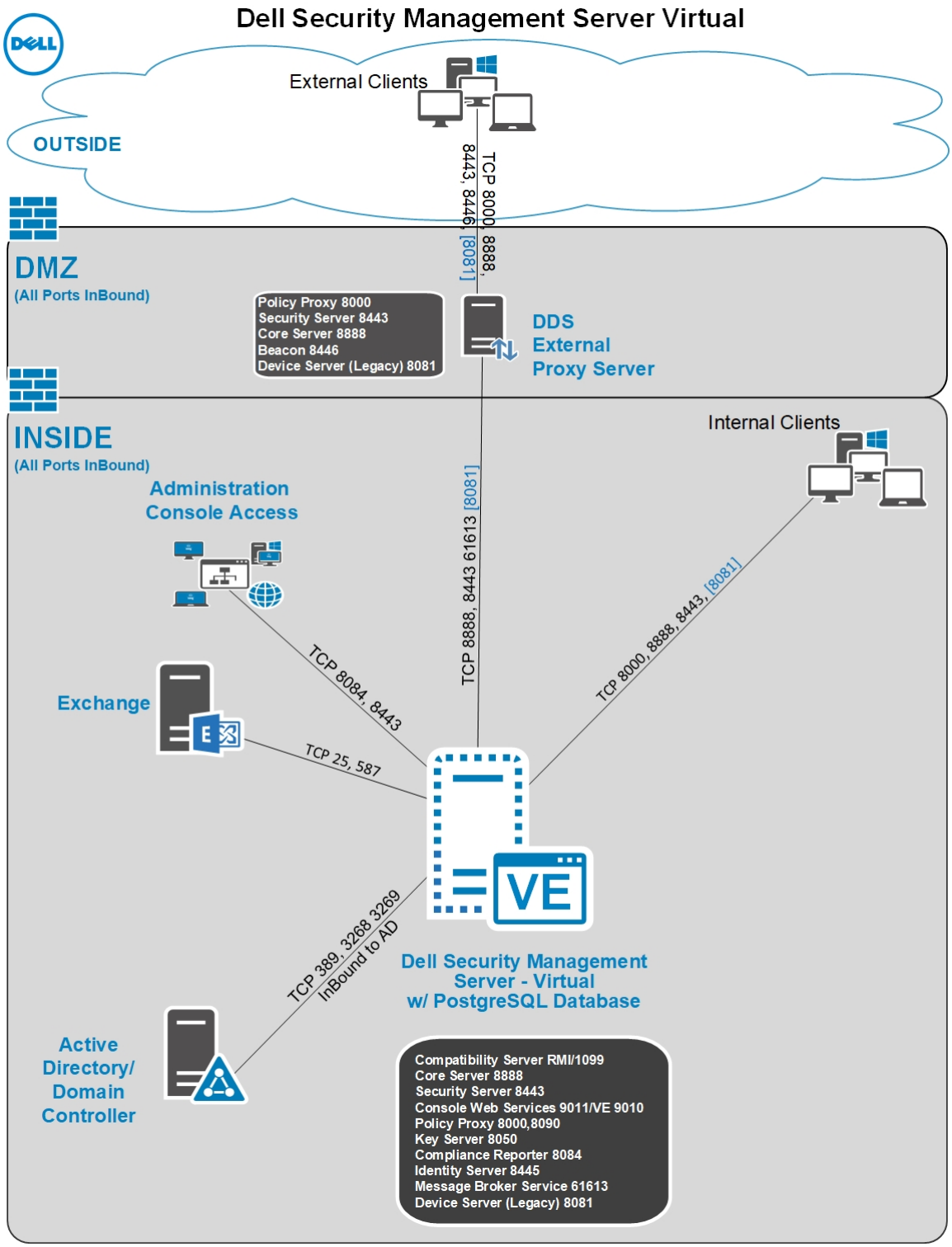
- **Windows Server 2019**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **LDAP 리포지토리**
  - Active Directory 2008 R2
  - Active Directory 2012 R2
  - Active Directory 2016

Security Management Server Virtual 아키텍처 디자인

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

아키텍처 구성요소

아래는 Dell Security Management Server Virtual의 기본 배포입니다.



OVA 파일 다운로드 및 설치

초기에 설치할 때 Security Management Server Virtual은 가상 컴퓨터에서 실행되는 소프트웨어를 전달하는 OVA(Open Virtual Application) 파일로 제공됩니다. OVA 파일은 www.dell.com/support의 다음과 같은 Dell Data Security 제품의 '제품 지원' 페이지에서 볼 수 있습니다.

- 암호화

- Endpoint Security Suite Enterprise
- Data Guardian

OVA 파일을 다운로드하려면 다음을 수행하십시오.

1 위에 나열된 해당 제품의 *드라이버 및 다운로드* 페이지를 탐색합니다.
2 **드라이버 및 다운로드**를 클릭합니다.
3 해당 VMware ESXi 버전을 선택합니다.
4 해당 번들을 다운로드합니다.

OVA 파일을 설치하려면 다음을 수행하십시오.

시작하기 전에, 모든 시스템 및 가상 환경의 요구 사항이 충족되었는지 확인하십시오.

1 Dell 설치 미디어에서 *Security Management Server Virtual v9.x.x Build x.ova*를 찾아 더블 클릭하여 VMware로 가져옵니다.

> **노트: VMware 대신 Hyper-V를 사용하는 경우, Windows 10에 대한 지침을 따르십시오. https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ 서버 기반 운영 체제의 경우, 다음 지침을 따르십시오. https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server. VMware 대신 ESXi를 사용하는 경우 다음 지침을 따르십시오. https://kb.vmware.com/s/article/2109708 .**

2 화면의 지침을 따릅니다.

> **노트: VMware를 사용하면서 가져오기 작업이 실패할 경우 OVA 파일을 가져오기 위해 웹 클라이언트를 경로로 제안하십시오. 자세한 내용은 https://kb.vmware.com/s/article/2151537를 참조하십시오.**

3 Security Management Server Virtual의 전원을 켭니다.
4 라이센스 계약에 사용되는 언어를 선택한 후 **EULA 표시**를 선택합니다.
5 계약서를 읽고 **EULA 동의**를 선택합니다.
6 사용 가능한 업데이트가 있는 경우 **채택**을 선택합니다.
7 **연결된 모드** 또는 **연결되지 않은 모드**를 선택합니다.

> **노트:**
> **연결되지 않은 모드**를 선택하면 절대로 연결된 모드로 변경할 수 없습니다.
>
> 연결되지 않은 모드는 인터넷과 보호되지 않은 LAN 또는 기타 네트워크에서 Dell Server를 격리합니다. 모든 업데이트는 수동으로 수행해야 합니다. 연결되지 않은 모드 및 정책에 대한 자세한 내용은 *AdminHelp*를 참조하십시오.

8 *delluser 암호 설정* 화면에서, 현재(기본) 암호인 **delluser**를 입력하고 고유한 암호를 입력한 후 다시 한번 입력한 다음 **적용**을 선택합니다.

암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

> **노트: 취소를 선택하거나 키보드에서 ESC 키를 누르면 기본 암호를 유지하는 것이 가능합니다.**

9 **닫기**를 선택하여 호스트 이름 구성 창으로 진입합니다.
10 *호스트 이름 구성* 대화상자에서 백스페이스 키를 사용하여 기본 호스트 이름을 제거합니다. 고유한 호스트 이름을 입력하고 **확인**을 선택합니다.
11 *네트워크 설정 구성* 대화상자에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.

- (기본 설정) DHCP(IPv4)사용
- (권장 설정) *DHCP 사용* 필드에서 스페이스바를 눌러 X를 제거한 다음 해당하는 경우 다음 주소를 수동으로 입력합니다.

  고정 IP

네트워크 마스크

기본 게이트웨이

DNS 서버 1

DNS 서버 2

DNS 서버 3

정적 구성을 위해 IPv6 또는 IPv4를 선택할 수 있습니다.

- **노트: 고정 IP를 사용할 경우 DNS 서버에 호스트 항목도 만들어야 합니다.**

12 시간대 확인 메시지가 표시되면 **확인**을 선택합니다.

13 첫 번째 부팅 구성이 완료되었음을 나타내는 메시지가 표시되면 **확인**을 선택합니다.

14 SMTP 설정 구성.

15 기존 인증서 가져오기 또는 새 서버 인증서 등록.

16 Security Management Server Virtual을 업데이트합니다.

17 포트 22에서 SFTP를 지원하는 FTP 클라이언트를 설치하고 파일 전송(FTP) 사용자 설정을 참조하십시오.

Security Management Server Virtual 설치 작업이 완료됩니다.

Management Console 열기

다음 주소에서 Management Console 열기: https://server.domain.com:8443/webui/

기본 자격 증명은 **superadmin/changeit**입니다.

지원되는 웹 브라우저의 목록은 Management Console Prerequisites를 참조하십시오.

프록시 모드 설치 및 구성

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

노트: 환경 내에서 보호된 Office 파일을 허용하거나 강제로 적용할 때 Data Guardian이 보호하는 모든 파일에 콜백 비콘을 삽입하는 Data Guardian 콜백 비콘을 지원하기 위해 이 설치 과정의 일부로 비콘 서비스가 설치됩니다. 이렇게 하면 프론트 엔드 서버와 모든 위치의 모든 장치 사이에서 통신을 할 수 있습니다. 콜백 비콘을 사용하기 전에 필요한 네트워크 보안이 구성되어 있는지 확인합니다.

이 설치를 수행하려면 DMZ 서버의 정규화된 호스트 이름이 필요합니다.

1 Dell 설치 미디어에서 Security Management Server 디렉토리로 이동합니다. Security Management Server-x64를 Security Management Server Virtual을 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 라이센스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.

7 32자 제품 키를 입력하고 **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\Dell에 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.
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
14 설치가 완료되면 **마침**을 클릭합니다.

기본 터미널 구성 작업

주 메뉴에서 기본 구성 작업에 액세스합니다.

시스템 대시보드 확인

Dell Server 서비스의 상태를 확인하려면 주 메뉴에서 **시스템 대시보드**를 선택합니다.

시스템 정보 위젯에는 현재 버전, 호스트 이름, IP 주소는 물론 CPU, 메모리 및 디스크의 사용량이 표시됩니다.

버전 내역 위젯에는 버전이 지정된 데이터베이스 스키마 변경 사항이 표시됩니다. 데이터는 '정보' 테이블에서 가져오고 시간을 기준으로 정렬되어 최신 버전이 맨 위에 표시됩니다.

다음 표는 *서비스 상태* 위젯의 각 서비스 및 기능에 대해 설명합니다.

이름	설명
Message Broker	Enterprise Server 버스
Identity Server	도메인 인증 요청을 처리합니다.
Compatibility Server	엔터프라이즈 아키텍처를 관리하는 서비스입니다.
Security Server	Active Directory와의 통신 및 명령을 제어하는 메커니즘을 제공합니다.
Compliance Reporter	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다.
Core Server	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 이 서비스는 "에이전트" 기반 장치에서 수집한 모든 활성화, 정책 및 인벤토리도 관리합니다.
Core Server HA (높은 가용성)	엔터프라이즈 아키텍처를 관리할 때 HTTPS 연결에 대한 보안과 성능을 향상시킨 높은 가용성의 서비스입니다.
Inventory Server	인벤토리 대기열을 처리합니다.
Forensic Server	Forensic API를 위한 웹 서비스를 제공합니다.
Policy Proxy	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다.

필요한 경우 자동으로 서비스가 모니터링되고 다시 시작됩니다.

노트: 데이터베이스 사용자 지정 프로세스가 실패하면 서버가 실행 실패 상태로 전환됩니다. 데이터베이스 사용자 지정 로그를 확인하려면 주 메뉴에서 로그 보기를 선택합니다.

호스트 이름 변경

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **호스트 이름**을 선택합니다.
2 백스페이스 키를 사용하여 기존 호스트 이름을 제거하고 새 호스트 이름으로 바꾼 다음 **확인**을 선택합니다.

네트워크 설정 변경

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **네트워크**를 선택합니다.
2 *네트워크 설정 구성* 화면에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.
   - (기본 설정) DHCP(IPv4) 사용
   - (권장 설정) *DHCP 사용*에서 스페이스바를 눌러 X를 제거한 다음 해당하는 경우 다음 주소를 수동으로 입력합니다.

고정 IP

네트워크 마스크

기본 게이트웨이

DNS 서버 1

DNS 서버 2

DNS 서버 3

정적 구성을 위해 IPv6 또는 IPv4를 선택할 수 있습니다.

노트:
고정 IP를 사용할 경우 DNS 서버에 호스트 항목을 만들어야 합니다.

DMZ 서버 지원 설정

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **DMZ 서버 지원**을 선택합니다.
2 스페이스바를 눌러 DMZ 서버 지원 사용 필드에 **X**를 입력합니다.
3 DMZ 서버의 정규화된 도메인 이름을 입력하고 **확인**을 선택합니다.

노트: DMZ 서버를 활용하려면, Install and Configure Proxy Mode 위의 프록시 서버 설치 지침을 참조하십시오.

시간대 변경

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **시간대**를 선택합니다.
2 *시간대* 화면에서, 화살표 키를 사용하여 원하는 시간대를 강조 표시하고 **Enter**를 선택합니다.

Update Security Management Server Virtual

For information about a specific update, see *Security Management Server Virtual Technical Advisories*, located at dell.com/support. To see the version and installation date of an update that is already applied, check the *System Dashboard*.

To receive email notifications when Dell Server updates are available, see Configure SMTP Settings.

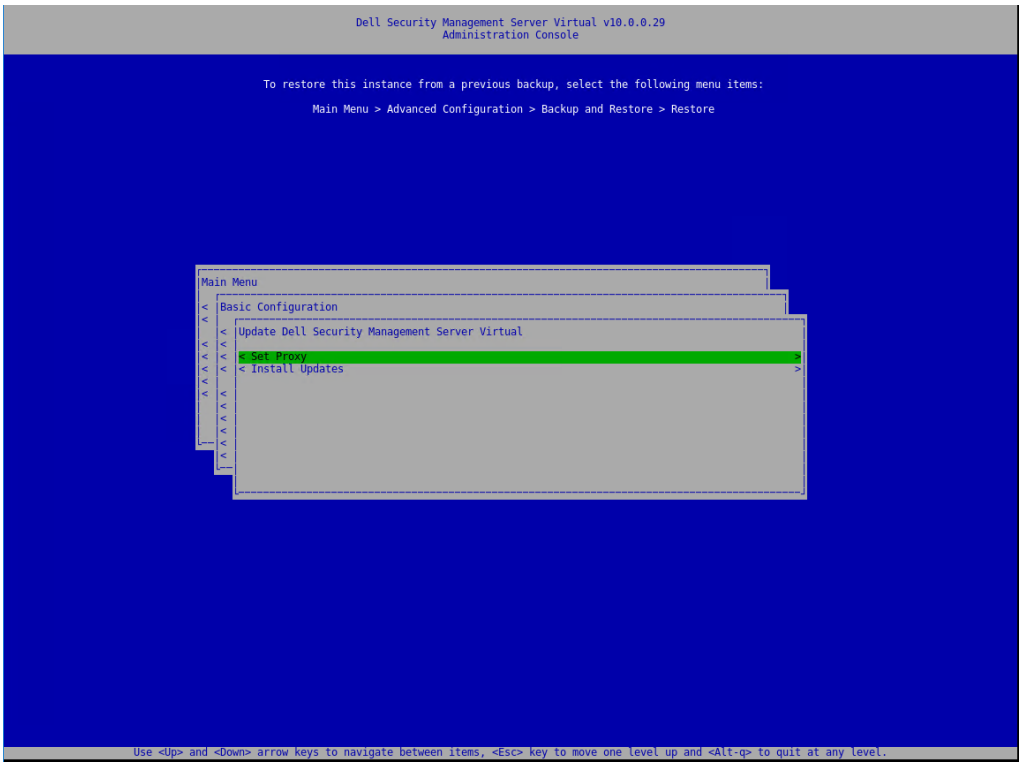
If policy changes have been made but not committed in the Management Console, commit the policy changes before updating the Dell Server:

1 As a Dell administrator, log in to the Management Console.
2 In the left menu, click **Management** > **Commit**.
3 Enter a description of the change in the Comment field.
4 Click **Commit Policies**.
5 When the commit is complete, log off the Management Console.

Update Security Management Server Virtual (Connected Mode)

1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.

2 From the **Basic Configuration** menu, select **Update Dell Security Management Server Virtual**.



NOTE: The version number may differ from the attached screen capture.

3 Select the desired action:

- Set Proxy Settings - Select this option to set the proxy settings for downloading updates.

  In the *Configure Proxy Settings* screen, press the space bar to enter an **X** in *Use Proxy*. Enter the HTTPS, and HTTP. If firewall authentication is required, press the space bar to enter an **X** in Authentication Required. Enter the user name and password, and select **OK**.

  NOTE: This Set Proxy option also now updates the proxy settings for the various java-based applications for pulling On-The-Box licenses as well as communication to the Endpoint Security Suite Enterprise SaaS and the Dell/Credant back-end infrastructure.

- When selecting **Install Updates**, the Security Management Server Virtual queries the built-in, default Ubuntu repositories and dist.ddspproduction.com, Dell's custom repository containing application updates.

  NOTE: Dell queries dist.ddspproduction.com through port 443 and port 80 for all Ubuntu updates. Any available updates are downloaded. The proxy settings defined in Set Proxy are used for port 443 and port 80 connections for download.

Update Security Management Server Virtual (Disconnected Mode)

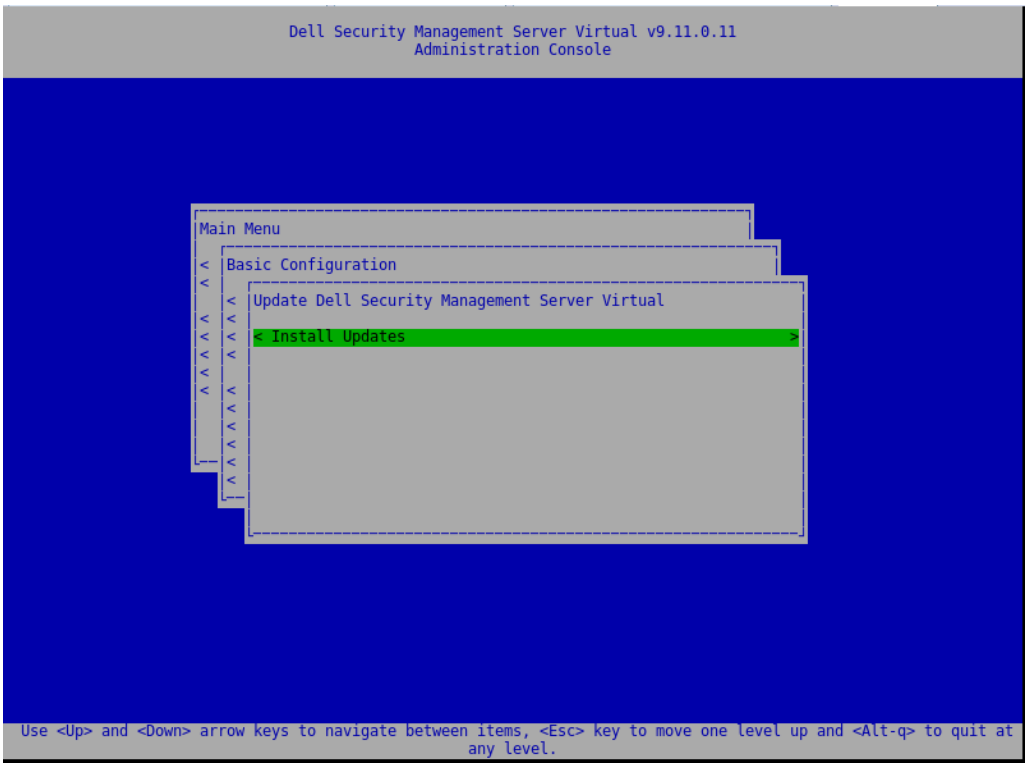
1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.

2 Obtain the .deb file that contains the latest Dell Server update from Dell ProSupport.

3 Store the .deb file in the /updates folder on the secure FTP server of the Dell Server.
Ensure that the FTP client supports SFTP on port 22, and an FTP user is set up. See Set up File Transfer (FTP) Users.

4 From the **Basic Configuration** menu, select **Update Security Management Server Virtual**.

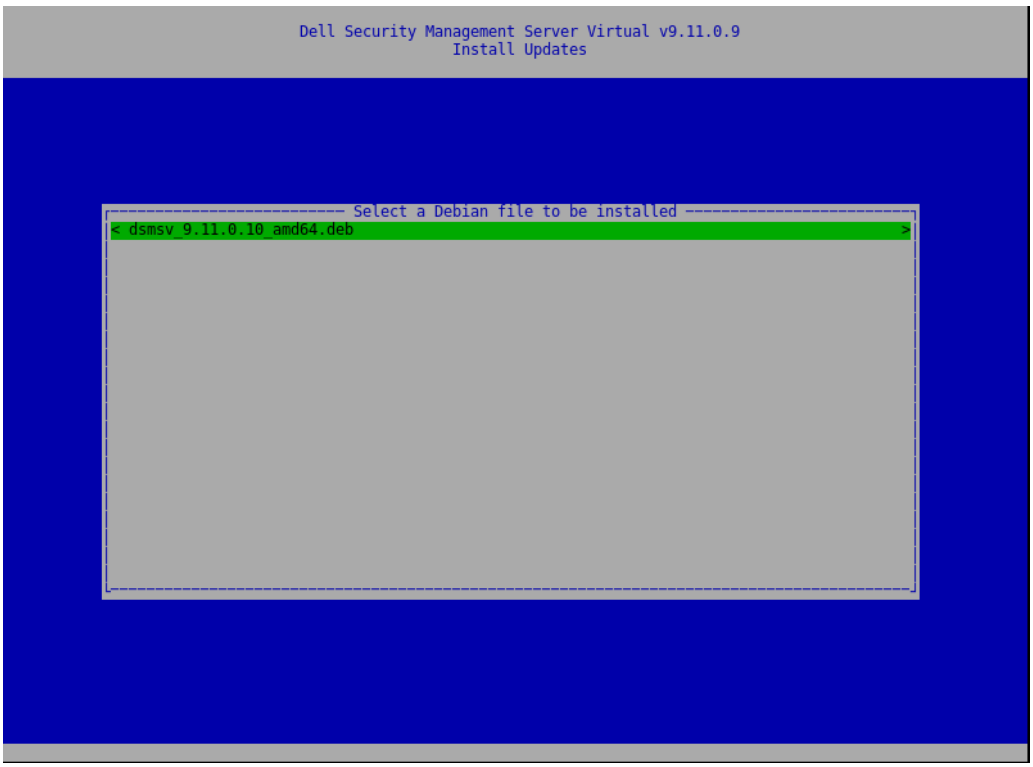
5 Select **Intall Updates** and press **Enter**.



NOTE: The version number may differ from the attached screen capture.

If the .deb file does not display, ensure that the .deb file is stored in the proper location.

6 Select the .deb update file you want to install and press **Enter**.



NOTE: The version number may differ from the attached screen capture.

사용자 암호 변경

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

다음 사용자의 암호를 변경할 수 있습니다.

- delluser(터미널 관리자) - 이 사용자는 Dell Server 터미널 및 해당 메뉴의 액세스 권한이 있습니다.
- dellconsole(셸 액세스) - 이 사용자는 Dell Server 셸의 액세스 권한이 있습니다. Shell 액세스는 네트워크 관리자가 네트워크 연결성을 확인하고 이에 대한 문제를 해결하는 데 사용할 수 있습니다.
- dellsupport(Dell ProSupport 관리자) - 이 사용자는 'sudo' 권한을 가지고 있으며 이 권한은 드물게 사용됩니다. 보안 목적을 위해, 이 계정의 암호를 관리할 수 있습니다.

1 *기본 구성* 메뉴에서 **사용자 암호 변경**을 선택합니다.
2 *사용자 암호 변경* 화면에서, 변경할 사용자 암호를 선택하고 **Enter**를 선택합니다.
3 *암호 설정* 화면에서, 현재 암호를 입력하고 새 암호를 입력한 후 다시 한번 새 암호를 입력한 다음 **확인**을 선택합니다.
암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

노트:
다른 사용자 계정을 선택하려면 키보드의 "스페이스바" 키를 눌러 선택 목록을 표시합니다.

SFTP(Secure File Transfer) 사용자 설정

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

1 *기본 구성* 메뉴에서 **SFTP**를 선택합니다.
2 *SFTP* 화면에서 SFTP 사용자를 추가하고 암호를 정의하려면 사용자 *상태* 필드에서 **Enter** 키를 누르거나 아래 화살표 키를 누릅니다. 스페이스바 키를 누르면 기존 사용자를 업데이트 또는 삭제할 수 있습니다. SFTP 사용자를 비활성화하려면 사용자를 선택하고 **삭제**를 선택한 다음 SFTP 확인 화면에서 **예**를 선택합니다.
3 SFTP 사용자의 사용자 이름과 암호를 입력합니다.
암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

4 SFTP 사용자 입력을 완료한 후 **적용**을 선택합니다.

SSH 사용

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

Support 관리자 로그인, 셸 액세스, 터미널 명령줄 인터페이스에 SSH를 사용할 수 있습니다.

1 *기본 구성* 메뉴에서 **SSH**를 선택합니다.
2 SSH를 사용할 사용자를 강조 표시하고 스페이스바를 눌러 **X**를 입력한 후 **확인**을 선택합니다.

서비스 시작 또는 중지

이 작업은 필요할 경우에만 수행합니다.

1 모든 서비스를 동시에 시작하거나 중지하려면 *기본 구성* 메뉴에서 **애플리케이션 시작** 또는 **애플리케이션 중지**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.

노트:
서버 상태 변경은 완료되기까지 최대 2분이 소요될 수 있습니다.

어플라이언스 재부팅

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서 **어플라이언스 재부팅**을 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후, Security Management Server Virtual에 로그인합니다.

어플라이언스 종료

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서, 아래로 스크롤하여 **어플라이언스 종료**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후, Security Management Server Virtual에 로그인합니다.

고급 터미널 구성 작업

주 메뉴에서 고급 구성 작업에 액세스할 수 있습니다.

로그 회전 구성

노트: 아래의 지침은 로그 회전을 지원하는 Dell Security Management Server Virtual의 애플리케이션을 위한 로그 회전을 정의합니다.

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

기본적으로 매일 로그 회전을 사용하도록 설정되어 있습니다. 기본 로그 회전을 변경하려면 *고급 구성* 메뉴에서 **로그 회전 구성**을 선택합니다.

로그 회전을 사용하지 않으려면 스페이스바를 눌러 '*회전 없음*' 필드에 **X**를 입력하고 **확인**을 선택합니다.

로그 회전을 사용하도록 설정하려면 다음 단계를 따르십시오.

1 회전을 일별, 주별, 월별로 사용하려면 스페이스바를 사용하여 해당 필드에 **X**를 입력하십시오. 주별 회전의 경우 드롭다운 메뉴에서 해당 요일을 선택합니다. 월별 회전의 경우 해당 날짜를 입력합니다.
2 *Logrotate 시간* 필드에 회전 시간을 입력합니다.
3 **확인**을 선택합니다.

백업 및 복구

백업은 언제든지 구성하거나 수행할 수 있으며 이 작업을 수행하지 않아도 Security Management Server Virtual을 사용할 수 있습니다. Dell은 정규적인 백업 프로세스를 구성하도록 권장합니다. 자세한 정보는 다음을 참조하십시오. http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Dell Server에 저장해 디스크 용량이 90%에 도달하면 새 백업이 저장되지 않습니다. 이메일 알림이 구성된 경우 디스크 할당 공간이 부족하다는 이메일 알림이 수신됩니다.

노트:
디스크 파티션 공간을 보존하고 백업이 자동으로 삭제되지 않도록 하려면 스토리지에서 불필요한 백업을 제거하십시오.

백업은 기본적으로 매일 실행됩니다. 조직에 필요한 백업 및 적절한 스토리지 공간 사용 요구사항에 따라 적절한 빈도로 외부 보안 FTP 서버에 백업을 저장할 것을 권장합니다.

백업 스케줄을 구성하려면, *고급 구성* 메뉴에서 **백업 및 복원 > 구성**을 선택하고 다음 단계를 따르십시오.

1 매일, 주별 또는 월별 백업을 사용하려면 스페이스바를 눌러 해당 필드에 **X**를 입력합니다. 주별 또는 월별 백업의 경우 해당 날짜 또는 요일을 숫자로 입력합니다(여기서, 월요일=1). 백업을 사용하지 않으려면 스페이스바를 눌러 *백업 없음* 필드에 **X**를 입력하고 **확인**을 선택합니다.

2 *백업 시간*. 필드에 백업 시간을 입력합니다.

3 **확인**을 선택합니다.

백업을 즉시 수행하려면, *고급 구성* 메뉴에 **백업 및 복원 > 지금 백업**을 선택합니다. 백업 확인 메시지가 표시되면 **확인**을 선택합니다.

노트:
복원 작업을 시작하려면 먼저 모든 Dell Server 서비스를 실행해야 합니다. 서버 상태를 확인합니다. 서비스가 모두 실행되고 있지 않은 경우 서비스를 다시 시작하십시오. 자세한 내용은 서비스 시작 또는 중지를 참조하십시오. ***모든*** 서비스가 실행되는 ***경우에만*** 복원을 시작하십시오.

백업에서 복원하려면, *고급 구성* 메뉴에서 **백업 및 복원 > 복원**을 선택하고 복원할 백업 파일을 선택합니다. 확인 메시지가 나타나면 **예**를 선택합니다.

재부팅된 후 백업이 복원됩니다.

보안 FTP 서버에 백업 저장

FTP 서버에 백업을 저장하려면 FTP 클라이언트가 포트 22에서 SFTP를 지원해야 합니다.

조직의 백업 요구사항에 따라 다음과 같은 방법으로 백업을 다운로드할 수 있습니다.

- 수동
- 자동화된 스크립트
- 조직의 승인된 백업 솔루션

조직의 백업 솔루션을 사용하여 백업을 다운로드하려면 백업 솔루션 벤더로부터 자세한 지침을 받으십시오.

노트:
Dell Server는 Linux Debian Ubuntu x64를 기반으로 합니다.

dellsupport로 Dell Server에 로그온하고 `sudo` 명령을 사용하여 백업 솔루션을 구성합니다.

`sudo` <백업 솔루션 벤더의 지침>

다음 폴더의 내용을 백업합니다.

/backup(필수)

/certificates(권장)

/support(선택 사항)

sudo 프로세스가 완료되면 **exit**를 입력하고 로그인 프롬프트가 표시될 때까지 **Enter**를 누릅니다.

SMTP 설정 구성

이메일 알림을 **수신하거나** Data Guardian을 사용하려면 다음 단계에 따라 SMTP 설정을 구성하십시오. 이메일 알림은 수신자에게 Dell Server 상태 오류 상태, 암호 업데이트, Dell Server 업데이트 가용성, 클라이언트 라이센스 문제에 대해 알려줍니다.

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

SMTP 설정을 구성하려면 다음 단계를 따르십시오.

1 *고급 구성* 메뉴에서 **이메일 알림**을 선택합니다.

2 이메일 알림 화면에서, 이메일 경고를 사용하려면 스페이스바를 눌러 *이메일 경고 사용* 필드에 **X**를 입력하십시오.

3 SMTP Server의 정규화된 도메인 이름을 입력합니다.

4 SMTP 포트를 입력합니다.
5 SMTP 사용자 입력
6 SMTP 암호 입력
7 *다음에서 알림 보내기* 필드에는 이메일 알림을 보낼 이메일 계정 ID를 입력합니다.
8 *다음으로 서버 상태 보내기* 필드에는 서버 상태 알림을 보낼 이메일 계정 ID를 입력합니다. 수신자는 쉼표 또는 세미콜론으로 구분합니다.
9 *다음으로 암호 변경 보내기* 필드에는 암호 변경 알림을 보낼 이메일 계정 ID를 입력합니다.
10 *다음으로 소프트웨어 업데이트 보내기* 필드에는 소프트웨어 업데이트 알림을 보낼 이메일 계정 ID를 입력합니다.
11 *서비스 경고 알림* 필드에서 스페이스바를 눌러 **X**를 입력한 후 알림 간격을 분 단위로 설정합니다. 시스템 상태 문제에 대한 알림이 전송된 후 알림 간격 시간이 경과하면 서비스 경고 알림이 트리거되고, 호스트 또는 서비스는 동일한 상태로 유지됩니다.
12 *보고서 요약* 필드에서 알림 보고서를 활성화하려면 원하는 간격(매일, 매주, 또는 매달)을 선택하고 스페이스바를 눌러 **X**를 입력합니다.
13 **확인**을 선택합니다.

기존 인증서 가져오기 또는 새 서버 인증서 등록

기존 인증서를 가져오거나 Security Management Server Virtual을 통해 인증서 요청을 생성할 수 있습니다.

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

기존 서버 인증서 가져오기

1 키 스토리지에서 기존 인증서와 전체 신뢰 체인을 내보냅니다.

> **노트: 내보내기 암호는 인증서를 Security Management Server Virtual으로 가져올 때 입력해야 하므로 기록해 두십시오.**

2 Dell Server의 FTP 서버에서 인증서를 **/certificates**에 저장합니다.
3 *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.
4 **기존 인증서 가져오기**를 선택합니다.
5 Dell Server에 설치할 인증서 파일을 선택합니다.
6 메시지가 표시되면 인증서 내보내기 암호를 입력하고 **확인**을 선택합니다.
7 가져오기가 완료되면 **확인**을 선택합니다.

> **노트: 추가 정보는 다음을 참조하십시오. http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

새 서버 인증서 등록

1 *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.
2 **새 서버 인증서**를 선택합니다.
3 **인증서 요청 생성**을 선택합니다.
4 *인증서 요청 생성* 필드를 입력합니다.

- 국가 이름: 2문자로 이루어진 국가 코드
- *시 또는 도*: 축약형이 아닌 시 또는 도의 전체 이름을 입력합니다(예: Texas).
- *지역 이름/구/군/시*. 적절한 값을 입력합니다(예: Dallas).
- *조직*: 적절한 값을 입력합니다(예: Dell).
- *부서*: 적절한 값을 입력합니다(예: 보안부).
- *일반 이름*: Dell Server의 정규화된 도메인 이름을 입력합니다. 이 정규화된 이름에는 호스트 이름과 도메인 이름이 포함됩니다(예: server.domain.com).
- *이메일 ID*: CSR이 전송될 이메일 주소를 입력합니다.

5 조직이 인증 기관에서 SSL 서버 인증서를 취득하는 데 사용하는 절차를 따르십시오. 서명할 CSR 파일의 내용을 전송합니다.
6 서명된 인증서를 수신하면 인증서를 .p7b 파일로 내보내고 전체 신뢰 체인을 .der 형식으로 다운로드합니다.
7 인증서 및 신뢰 체인의 백업 사본을 만듭니다.
8 인증서 파일과 해당되는 전체 신뢰 체인을 Dell Server의 FTP 서버에 업로드합니다.
9 *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.
10 **새 서버 인증서**를 선택합니다.
11 인증서 등록 완료를 선택합니다.
12 Dell Server에 설치할 인증서 파일을 선택합니다.
13 메시지가 나타나면 인증서 암호를 입력합니다(**changeit**).

Windows 기반 Encryption 클라이언트에서 신뢰 유효성 검사를 사용하려면 Enable Manager Trust Chain Check를 참조하십시오.

자체 서명 인증서 생성 및 설치

노트: 기본값으로 생성되는 자체 서명 인증서의 유효 기간은 10년입니다.

1 Dell Server *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.
2 **자체 서명 인증서 생성 및 설치**를 선택합니다.
3 사전 설치된 인증서를 새 인증서로 바꾸도록 확인하려면 **예**를 클릭합니다.
4 인증서 암호를 입력합니다(**changeit**).
5 새로운 인증서를 설치한 후 **확인**을 선택하고 서비스가 다시 시작되도록 기다립니다.

서비스가 자동으로 다시 시작됩니다.

데이터베이스 액세스 사용

이 작업은 언제든지 완료할 수 있습니다. Security Management Server Virtual 사용을 시작할 필요가 없습니다.

노트: 데이터베이스 액세스는 필요할 경우에만 사용하도록 설정하고 필요하지 않은 경우에는 사용하지 않도록 설정하는 것이 좋습니다.

1 *고급 구성* 메뉴에서 **데이터베이스 액세스**를 선택합니다.
2 스페이스바를 눌러 *데이터베이스 액세스 사용*에 **X**를 입력하고 **확인**을 선택합니다. 데이터베이스 암호를 아직 구성하지 않았다면 데이터베이스 암호 화면이 나타납니다.
3 데이터베이스 암호를 입력합니다.
4 데이터베이스 암호를 다시 입력합니다.
Dell Data Security 애플리케이션 구성 요소가 자동으로 중지됩니다.

Terminal 언어 설정 또는 변경

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 주 메뉴에서 **언어 설정**을 선택합니다.
2 화살표 키를 사용하여 선호하는 언어를 선택합니다.

로그 보기

다음과 같은 로그를 확인하려면, 주 메뉴에서 **로그 보기**를 선택합니다.

- 시스템 로그
  - Syslog 로그
  - 메일 로그
  - Auth 로그(SSH)
  - Postgres 로그
  - 모니터 로그
- 서버 로그
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- 관리 콘솔
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Databasecustomizer 로그

노트: 이 화면을 탐색하려면 다음을 수행하십시오.

- 키보드에서 오른쪽 alt 키를 길게 누른 채로 "/" 키를 누르면 로그의 끝으로 이동할 수 있습니다.
- 로그를 종료하려면, 키보드에서 왼쪽 Control 키를 누른 채로 "x" 키를 누릅니다.
- 화살표 키를 이용하면 탐색할 수 있습니다.
- page up 및 page down 키를 사용하면 한 번에 한 페이지씩 위로 또는 아래로 이동할 수 있습니다.
- 스페이스바를 이용하면 한 페이지에 로그를 단계별로 표시할 수 있습니다.

명령줄 인터페이스 열기

명령줄 인터페이스를 열려면, 주 메뉴에서 **셸 실행**을 선택합니다.

명령줄 인터페이스를 종료하려면, **exit**를 입력하고 **Enter**를 누릅니다.

시스템 스냅숏 로그 생성

Dell ProSupport용 시스템 스냅숏 로그를 생성하려면, 주 메뉴에서 **지원 도구**를 선택합니다.

1 *지원 부서 도구* 메뉴에서 **시스템 스냅숏 로그 생성**을 선택합니다.
2 파일이 생성되었다는 메시지가 표시되면 **확인**을 선택합니다.

3

유지 보수

불필요한 Security Management Server Virtual 백업을 제거하십시오.

가장 최근의 백업 10개만 보존됩니다. 디스크 파티션 공간이 10% 이하인 경우 백업이 더 이상 저장되지 않습니다. 이러한 상태가 발생하면 디스크 할당 공간이 부족하다는 이메일 알림이 수신됩니다.

4

문제 해결

이메일 알림이 구성된 상태에서 오류가 발생하면 이메일 알림이 수신됩니다. 이메일 알림의 정보를 기준으로 다음 단계를 따르십시오.

1 해당 로그 파일을 확인합니다.
2 필요하면 서비스를 다시 시작합니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.
3 시스템 스냅숏 로그를 생성합니다.
4 Dell ProSupport에 문의하십시오. 자세한 내용은 Dell ProSupport에 문의를 참조하십시오.

5

설치 후 구성

설치 후 조직에서 사용하는 Dell Data Security 솔루션을 바탕으로 환경의 일부 구성 요소를 구성해야 할 수 있습니다.

Security Management Server Virtual를 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.

Data Guardian용 구성

Data Guardian을 지원하도록 Dell Server를 구성하려면 Management Console에서 *보호된 Office 문서* 및 *클라우드 암호화* 정책 하나 또는 둘 다를 **설정**으로 설정하십시오.

Data Guardian 클라이언트를 설치하는 지침은 *Data Guardian 관리자 가이드* 또는 *Data Guardian 사용자 가이드*를 참조하십시오. Dell Data Guardian에서 외부 사용자에게 이메일을 보내도록 허용하고 생성자가 키 관리를 더욱 쉽게 하도록 관리자가 SMTP를 활성화하는 것을 권장합니다.

Manager 신뢰 체인 검사 검증

SED의 Security Management Server Virtual 또는 BitLocker Manager에 자체 서명 인증서가 사용되는 경우, 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 ***비활성화*** 상태로 유지해야 합니다. 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 활성화하기 전에 다음 조건을 충족시켜야 합니다.

- Entrust 또는 Verisign 등 루트 인증 기관이 서명한 인증서를 Dell Server로 가져와야 합니다. 기존 인증서 가져오기 또는 새 서버 인증서 등록을 참조하십시오.
- 인증서의 전체 신뢰 체인은 클라이언트 컴퓨터의 KeyStore에 저장되어야 합니다.

SSL/TLS 신뢰 유효성을 비활성화하려면 클라이언트 컴퓨터에서 다음 레지스트리 항목 값을 1로 변경하십시오.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

6

Management Console 관리자 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.

*AdminHelp*를 시작하려면 Management Console 오른쪽 상단 모서리에 있는 "?"를 클릭합니다. *시작하기* 페이지가 표시됩니다. **도메인 추가**를 클릭합니다.

고객을 위해 기준 정책이 설정된 상태지만 다음과 같은 특정 요구 사항에 따라 수정해야 합니다(라이선스 및 권한에 따라 모두 활성화 가능).

- 정책 기반 암호화가 공통 키 암호화로 활성화됩니다.
- 자체 암호화 드라이브가 포함된 컴퓨터 암호화
- BitLocker 관리를 사용하지 않음
- 고급 위협 방지가 켜지지 않았습니다.
- 위협 차단이 비활성화되어 있습니다.
- 외부 미디어를 암호화하지 않음
- 포트는 포트 제어로 관리되지 않습니다.
- 설치된 전체 디스크 암호화 장치는 암호화되지 않습니다.
- Data Guardian이 비활성화되어 있습니다.

정책 설명은 AdminHelp 주제 *정책 관리*를 참조하십시오.

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.

7

포트

다음 표는 각 구성요소와 그 기능에 대한 설명입니다.

이름	기본 포트	설명
Compliance Reporter	HTTP(S)/ 8084	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다.
Management Console	HTTPS/ 8443	전체 엔터프라이즈 배포를 위한 관리 콘솔 및 제어 센터입니다.
Core Server	HTTPS/ 8887(폐쇄)	정책 흐름, 라이센스 및 사전 부팅 인증을 위한 등록, SED 관리, 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.
Core Server HA (높은 가용성)	HTTPS/ 8888	높은 가용성 서비스가 Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, 및 Advanced Threat Prevention에 대한 HTTPS 연결의 증가된 보안 및 성능을 제공합니다.
Security Server	HTTPS/ 8443	Policy Proxy와 통신합니다. 포렌직 키 검색, 클라이언트 활성화, Data Guardian 제품 및 SED-PBA 통신을 관리합니다.
Compatibility Server	TCP/ 1099(폐쇄)	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이터를, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 사용자 그룹에 기반하여 데이터를 처리합니다.
Message Broker 서비스	TCP/ 61616(폐쇄) 및 STOMP/ 61613(폐쇄됨 또는 DMZ에 구성된 경우 61613 개방됨)	Dell Server의 서비스 간 통신을 처리합니다. Policy Proxy 큐에 대한 Compatibility Server가 생성한 정책 정보 단계입니다.
Identity Server	8445(폐쇄)	SED Management 인증을 포함한 도메인 인증 요구를 관리합니다.
Forensic Server	HTTPS/ 8448	적절한 권한을 소유한 관리자가 Management Console에서 데이터 잠금 해제 또는 복호화 작업을 위해 암호화 키를 가져올 수 있습니다. Forensic API에 필요함.
Inventory Server	8887	인벤토리 대기열을 처리합니다.

이름	기본 포트	설명
Policy Proxy	TCP/ 8000	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다. Encryption Enterprise(Windows 및 Mac)에 필요함
LDAP	389/636, 3268/3269 RPC - 135, 49125+	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.
클라이언트 인증	HTTPS/ 8449	클라이언트 서버가 Dell Server를 통해 인증하도록 허용합니다. Server Encryption에 필요함.
콜백 비콘	HTTP/TCP 8446	이를 통해 프론트 엔드 서버에서 Data Guardian을 보호된 Office 모드로 실행할 때 각 보호된 Office 파일에 콜백 비콘을 삽입할 수 있게 합니다.