Dell Data Guardian

Windows, Mac, 모바일 및 웹 사용자 가이드 v2.7

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

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.

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Windows, Mac, 모바일 및 웹 사용자 가이드

2019 - 06

개정 A01

목차

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

1 소개

*Dell Data Guardian 사용자 가이드*에는 Windows, Mac, 모바일 또는 웹 포털에 Data Guardian을 설치하고 사용하는 데 필요한 정보가 나와 있습니다.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

개요

관리자가 설정한 정책에 따라 Data Guardian은 다음과 같이 데이터를 보호합니다.

- 로컬에 저장되거나, 다양한 방식으로 다른 사용자와 공유되거나, 이동식 미디어에 저장되는 Office 문서. .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf 형식의 Office 문서를 보호할 수 있습니다.
- 기본 파일 보호 - 메모장과 같은 추가 애플리케이션 및 파일 형식
- 클라우드 기반 파일 공유 시스템 - Windows 컴퓨터 또는 모바일 장치는 클라우드 스토리지용 데이터를 수집하고 해당 데이터를 암호화한 다음, 암호화된 데이터를 클라우드에 업로드합니다.

  노트:
  관리자가 Data Guardian을 Office 문서와만 사용하는지, 클라우드 스토리지와만 사용하는지 양쪽 모두와 함께 사용하는지를 알려줄 것입니다. 관리자가 보호할 수 있는 추가 애플리케이션 및 파일 형식을 알려줄 것입니다.

다음과 같은 플랫폼에서 Data Guardian을 사용할 수 있습니다.

- Windows
- iOS
- Android
- Mac
- Data Guardian 웹 포털은 관리자가 설정한 경우입니다.

노트:
Mac용 Data Guardian은 플랫폼 간에 암호화된 파일을 열 수 있습니다. 일부 파일은 읽기 전용일 수 있습니다. Mac용 Data Guardian에 관한 대부분의 사용자 정보는 소프트웨어 내에 있는 온라인 도움말을 참조하십시오.

Identifier	**GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4**
Status	**In Translation**

Data Guardian을 위한 암호화 옵션

엔터프라이즈의 보안 수준을 기반으로 관리자는 저장된 데이터와 사용 중인 데이터를 보호할 수 있는 정책을 설정합니다. 관리자가 엔터프라이즈에 적용되는 정책을 알려줄 것입니다.

이 목록은 일부 암호화 옵션에 대한 개요 및 일부 플랫폼에 해당하는 정책 설정의 위치를 제공합니다.

모드 및 Office 문서

Office 문서 보호를 위해 정책이 설정되어 있을 수 있습니다. 암호화 동작은 플랫폼 및 모드에 따라 다를 수 있습니다. Mac의 경우 온라인 도움말을 참조하십시오.

모드	Office 문서
Windows 및 Mac용 모드 옵션: **옵트인 모드** - 보호할 Office 문서를 결정할 때 옵션이 일부 있습니다. • **Windows** 및 **Mac** - **Secure Documents** 폴더가 문서 폴더의 루트에 추가됩니다. 이는 파일을 암호화할 다른 방법을 제공합니다. **강제 보호 모드** - 사용자의 엔터프라이즈에서 더 높은 수준의 보안을 요구합니다. Data Guardian은 암호화된 파일로 스윕을 수행합니다. • **Windows** 및 **Mac** - 다른 정책에 의해 문서 폴더의 루트에 **보호되지 않은 문서** 폴더가 추가될 수 있습니다. 보호된 Office 문서 또는 기본 파일 보호 유형을 이 폴더에 배치하여 해독합니다. • **Mac** - **/Users**에 있는 파일을 보호합니다. 이러한 플랫폼은 다음 모드에 기반하지 않습니다. • 모바일 • 웹 포털	**Office 문서 - Windows, Mac, 모바일 및 웹 포털** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf - Data Guardian에 의해 보호되는 경우 네트워크에서가 아니라 Adobe Acrobat Reader DC 또는 Microsoft Word를 사용해 엽니다.

Office 문서 - Windows

관리자는 Data Guardian 정책을 추가하여 이러한 옵션의 데이터를 제어하거나 손실되지 않도록 설정할 수 있습니다. 암호화 동작은 모드에 따라 다를 수 있습니다.

Windows에서 보호된 Office 문서에 대한 옵션	설명
• 저장 - Office 문서가 보호된 경우 새로운 컨텐츠를 저장할 수 있습니다. (**다른 이름으로 저장**이 회색으로 표시됩니다.) • 보호된 다른 이름으로 저장 • Office 문서가 이미 보호된 경우 **다음 이름으로 저장**이 회색으로 표시됩니다.	Windows에 대한 기타 정보: • **보호되지 않은** Office 문서 - **저장**, **다른 이름으로 저장** 혹은 **보호된 다른 이름으로 저장** 중 선택할 수 있습니다. • 보호된 Office 문서 및 보호된 이메일에 빨간색 테두리가 표시됩니다.
복사/붙여넣기 및 클립보드	보호된 Office 문서에서 또 다른 보호된 Office 문서로 복사하여 붙여 넣을 수 있습니다. 보호된 문서는 보호되지 않는 문서로 붙여 넣을 수 없습니다.
인쇄	정책에 따라 보호된 Office 문서는 인쇄가 허용되거나 워터마크가 부착되거나 비활성화될 수 있습니다.

Windows에서 보호된 Office 문서에 대한 옵션	설명
내보내기 (Windows 및 Office 2013 이상, 모바일)	정책에 따라 허용되거나 워터마크가 부착되거나 비활성화될 수 있습니다. **노트:** 워터마크가 설정된 경우 Office 문서를 내보낼 수 있습니다. PDF는 내보낼 수 없습니다.
인쇄 화면	정책에 따라 허용되거나 차단될 수 있습니다.
프로세스 차단 예: 캡처 도구	엔터프라이즈가 설정한 정책에 따라 보호된 Office 문서가 열려 있는 경우 일부 프로세스가 차단될 수 있습니다.
온스크린 워터마크	보호된 Office 문서가 열려 있는 경우 화면에는 컴퓨터 이름 및 사용자 이름이 표시된 워터마크가 나타납니다.
TITUS 분류 (옵트인 모드가 있는 Windows)	정책이 활성화되어 있는 경우 Office 문서를 마우스 오른쪽 단추로 클릭하여 TITUS 분류를 선택합니다. 이는 Office 문서를 보호할 다른 방식을 제공합니다.
데이터 분류 (옵트인 모드가 있는 Windows)	주민등록번호나 신용카드번호 같이 민감함 정보를 보호하도록 정책이 활성화 및 구성되어 있는 경우에는 이러한 정보가 포함된 Office 문서가 암호화됩니다.

Office 문서 - Mac, 모바일 및 웹 포털

암호화 동작은 플랫폼 및 모드에 따라 다를 수 있습니다. 관리자가 엔터프라이즈에 적용되는 사항을 알려줄 것입니다.

암호화 옵션	설명
Mac - Dell Data Guardian 인터페이스	**Mac** - 암호화할 보호된 문서를 업로드합니다. 해독할 보호된 문서를 다운로드합니다. 보호된 문서를 편집한 후에는 변경 사항이 클라우드 또는 로컬의 원본 파일에 저장됩니다.
모바일 - Data Guardian 애플리케이션 내부 • 인쇄 • 온스크린 워터마크 • 숨겨진 워터마크 • 내보내기	**모바일** - 기반 정책: • Data Guardian 애플리케이션 내의 Office 문서는 보호됩니다. • 보호된 Office 문서는 인쇄가 허용되거나 워터마크가 부착되거나 비활성화될 수 있습니다. • 보호된 Office 문서가 열려 있는 경우 화면에는 컴퓨터 이름 및 사용자 이름이 표시된 워터마크가 나타납니다.
웹 포털 • 온스크린 워터마크	**웹 포털** - 보호되거나 보호되지 않은 문서를 업로드할 수 있지만 업로드한 모든 파일은 다운로드를 클릭하면 보호됩니다. 보호된 Office 문서가 열려 있는 경우 화면에는 컴퓨터 이름 및 사용자 이름이 표시된 워터마크가 나타납니다.

추가 옵션

암호화 동작은 플랫폼 및 모드에 따라 다를 수 있습니다. 관리자가 엔터프라이즈에 적용되는 사항을 알려줄 것입니다.

옵션	설명(옵트인 및 강제 보호 모드)
기본 파일 보호 - 추가 애플리케이션 및 파일 형식을 보호할 수 있습니다. (Windows, Mac, 모바일, 웹 포털) • 예: .txt 또는 .png **노트:** 현재 이러한 파일 형식은 보호되는 경우에도 빨간색 테두리가 표시되지 않습니다.	관리자가 애플리케이션을 지정하고 파일 형식을 암호화할 정책을 구성할 수 있습니다. **Windows, Mac 및 Mobile** - 삭제되고 암호화된 파일입니다. • **Mac** - 관리자가 설정한 파일 확장자의 경우 */Users* 폴더에서 해당 파일 형식을 암호화합니다. **웹 포털** - 정책에 따라 이러한 파일은 읽기 전용이거나 사용자가 편집할 수 있습니다.
외부 사용자와 보호된 Office 문서 공유 (Windows, Mac, 모바일, 웹 포털) 표지 페이지에는 등록 링크 및 Data Guardian 설치 정보가 나열됩니다.	• 외부 사용자와 **Windows** - 보호된 Office 문서 및 PDF에 **날짜 제한(엠바고)을** 추가할 수도 있습니다. • **웹 포털** - 웹 포털에 공유된 파일을 업로드할 수 있습니다. 웹 포털 내에서는 파일을 공유할 수 없지만 다운로드 후에 공유 가능합니다.
조작된 파일 또는 표지 페이지 (Windows, Mac, 모바일, 웹)	Office 파일의 경우 Data Guardian은 보호된 Office 문서를 스캔하여 일부 조작 형태를 감지할 수 있습니다.
액세스 그룹(사내 환경) (Windows, Mac, 모바일, 웹 포털)	관리자가 활성화한 경우 액세스 그룹에 있는 사람만 암호화된 파일을 볼 수 있습니다. 내부 및 외부 사용자에게 개별 파일에 대한 액세스 권한을 부여할 수 있으며 이들이 액세스 권한을 요청할 수도 있습니다. 추가 정책에 따라 [보호됨]으로 표시된 Outlook 이메일을 마우스 오른쪽 단추로 클릭하고 개별 사용자의 액세스를 제거할 수 있습니다.
지오펜스(모바일)	지정된 영역에 있는 사용자만 휴대 전화에서 해당 파일에 액세스할 수 있습니다.
Outlook 이메일 암호화(Windows)	정책에 따라 *보호* 단추를 사용해 이메일 및 첨부 파일의 내용을 암호화할 수 있습니다. 외부 사용자에게 전송되는 표지 페이지에는 등록 링크 및 Data Guardian 설치 정보가 표시됩니다.

호스팅된 또는 사내 환경

Data Guardian을 직접 설치해야 하는 경우, 관리자가 엔터프라이즈에 적용되는 옵션을 확인할 것입니다.

노트:
모바일 애플리케이션의 경우 Workspace ONE이 설치되어 있으면 SSO(Single Sign-On)를 사용하여 Data Guardian을 인증할 수 있습니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션. 엔터프라이즈가 멀티 테넌트인 경우, 관리자가 설치 ID를 제공합니다. 보호된 문서에 액세스할 수 없는 사용자에 대한 표지 페이지가 표시되면 설치 ID에 대한 정보가 커버 페이지에 포함됩니다. 모든 플랫폼 - 테넌트가 지정된 시간 동안 지불하지 않으면 해당 테넌트를 일시 중지할 수 있습니다.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버. 관리자가 Dell Server URL의 이름을 제공합니다.

클라우드 암호화

암호화 동작은 플랫폼 및 모드에 따라 다를 수 있습니다. 관리자가 엔터프라이즈에 적용되는 사항을 알려줄 것입니다.

플랫폼	설명
모바일	모바일에서 클라우드 보호 사용하기를 참조하십시오.
Mac	온라인 도움말을 참조하십시오.
웹 포털	온라인 도움말을 참조하십시오.
Windows	현재 Data Guardian의 클라우드 암호화 보호 기능은 클라우드 서비스 공급업체의 새로운 기능에 대한 호환성 문제 방지 목적으로 인해 Windows에서 사용할 수 없습니다. 이미 클라우드 암호화로 보호된 .xen 파일을 보려면 Data Guardian의 모바일 앱 또는 웹 포털을 사용하거나 Mac에서 Data Guardian을 사용하십시오.

정책 설정

일부 플랫폼에는 장치에 대한 정책 설정의 일부 목록이 포함되어 있습니다.

플랫폼	정책 설정의 위치
Mac	*기본 설정* 창
모바일	**설정** 아이콘 > **정보**
웹 포털	**설정** 아이콘 > **정보**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

추가 지원

이 문서에 없는 내용과 관련하여 지원이 필요할 경우 관리자에게 문의하십시오.

Identifier	GUID-1DE0401E-4073-46BA-95E3-
Status	Translation Validated

2 요구 사항

이 장에는 클라이언트 하드웨어와 소프트웨어 요구 사항이 나와 있습니다.

Identifier	GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF
Status	Translation Validated

Dell Server

Windows, Mac 및 모바일용 Data Guardian을 사용하려면 Security Management Server 또는 Security Management Server Virtual v9.6 이상이 필요합니다. Data Guardian 웹 클라이언트를 사용하려면 Security Management Server 또는 Security Management Server Virtual v9.8 이상이 필요합니다. 이 문서의 목적에 알맞게 특정 버전을 언급해야 할 경우(예: Security Management Server Virtual 사용 시 다른 절차 적용)를 제외하고 양쪽 서버가 모두 Dell Server로 지칭됩니다.

Identifier	GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21
Status	In Translation

Windows용 Data Guardian

- 배포 시에는 IT 모범 사례를 따라야 합니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.
- 설치/업그레이드/설치 제거를 수행하는 사용자 계정은 로컬 또는 도메인 관리자여야 하며, 관리자 권한은 Microsoft SMS 또는 Dell KACE 등의 배포 도구를 사용하여 임시로 할당할 수 있습니다. 관리자 이외의 사용자는 상승된 권한을 가진 경우에도 지원되지 않습니다.
- 설치/설치 제거를 시작하기 전에 중요한 데이터를 모두 백업하십시오.
- 설치가 진행되는 동안에는 외부(USB) 드라이브 삽입 또는 제거를 비롯하여 컴퓨터를 변경하지 마십시오.
- Data Guardian은 Microsoft Office 2016 및 Microsoft Office 365 Business 및 Business Premium의 특정 버전에서 지원됩니다. Office 365 Business Essentials에서는 지원되지 않습니다.
- Windows용 Data Guardian은 Workspace ONE과 호환됩니다. Workspace ONE 및 MSI 설치를 위한 Data Guardian 설치 관리자의 확장명은 .msi입니다.
- Windows에 설치된 Data Guardian v2.4 이상은 Air Gap 환경에서 지원되지만 몇 가지 제한 사항이 적용됩니다. 현재 감사 이벤트의 지리적 위치 데이터 및 엠바고 파일은 지원되지 않습니다. 웹 비콘을 사용하려면 일부 구성이 필요합니다.
- 대상 장치가 https://yoursecurityservername.domain.com:8443/cloudweb/register 및 https://yoursecurityservername.domain.com:8443/cloudweb에 연결되어 있는지 확인하십시오.
- Data Guardian을 배포하기 전에 대상 장치에 클라우드 스토리지 계정이 아직 설정되지 않은 상태가 가장 좋습니다. 사용자가 기존 계정을 유지하기로 결정할 경우 Data Guardian을 설치하기 전에 *암호화되지 않은* 상태로 유지하려는 파일을 동기화 클라이언트 외부로 이동해야 합니다.
- 클라이언트가 설치된 후 사용자는 컴퓨터를 다시 시작할 준비를 해야 합니다.
- Data Guardian은 동기화 클라이언트의 동작을 방해하지 않습니다. 그러므로 관리자와 최종 사용자는 Data Guardian을 배포하기 전에 이러한 애플리케이션의 작동 방식을 잘 알아야 합니다. 자세한 내용은 Box 지원의 경우 https://support.box.com/home, Dropbox 지원의 경우 https://www.dropbox.com/help, OneDrive 지원의 경우 http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other를 참조하십시오.
- 보호된 Office 문서는 Data Guardian의 도우미 솔루션인 Mozy는 물론 기타 클라우드, 이메일 및 NFS 스토리지 제품에서도 지원됩니다.

- Dell 암호화가 필요하지는 않지만 사용되는 경우 Encryption 클라이언트는 v8.12 이상이어야 합니다.
- Data Guardian은 Windows 시스템 복원 도구 또는 Windows Insider Preview를 지원하지 않습니다.
- Microsoft의 폴더 재지정은 Data Guardian에서 지원되지 않습니다.
- 최신 문서 자료와 기술 권고사항에 대해서는 www.dell.com/support를 정기적으로 확인하시기 바랍니다.

사전 요구 사항

.exe 필수 구성 요소

아직 설치되지 않은 경우 설치 프로그램에서 Microsoft Visual C++ 2017 재배포 가능 패키지(x86 및 x64)를 설치합니다.

노트:
Windows 7 및 Windows 8.1의 경우 Windows Updates를 사용하여 컴퓨터를 최신 상태로 유지해야 합니다. 자세한 내용은 https://support.microsoft.com/en-us/help/2919355 및 https://support.microsoft.com/en-us/help/2999226을 참조하십시오.

.msi 필수 구성 요소

Microsoft Visual Studio C++ 2017 재배포 가능 패키지(x86 및 x64)를 설치해야 합니다.

노트:
또한 MSI를 실행하는 경우 Visual Studio 2010 Tools for Office Runtime(x86 및 x64)도 설치해야 합니다.

일반 사전 요구 사항

Data Guardian에는 Microsoft .Net 4.5.2 이상이 필요합니다. Dell에서 배송된 모든 컴퓨터에는 .Net 4.5.2가 미리 설치되어 있습니다. 하지만 Dell 하드웨어를 설치하지 않거나 이전 Dell 하드웨어에서 Data Guardian을 업그레이드하는 경우에는 Data Guardian을 설치하기 전에 어떤 버전의 .Net이 설치되어 있는지 확인한 후, 필요에 따라 버전을 업데이트해야만 설치 및 업그레이드에 따른 문제를 방지할 수 있습니다. 설치되어 있는 .Net의 버전을 확인하려면 설치하고자 하는 컴퓨터에서 다음 지침을 따르십시오. http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx Microsoft .Net Framework 4.5.2를 설치하려면 https://www.microsoft.com/en-us/download/details.aspx?id=42643로 이동하십시오.

하드웨어

최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다. 다음 표에 Windows 클라이언트를 사용할 수 있도록 지원되는 하드웨어가 나와 있습니다.

Windows 하드웨어

- 200MB의 사용 가능한 디스크 공간(운영 체제에 따라 다름)
- 10/100/1000 또는 Wi-Fi 네트워크 인터페이스 카드
- 설치 및 등록된 TCP/IP

운영 체제

다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32비트 및 64비트)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro 버전 1703(Creators Update/Redstone 2) - 버전 1809(2018년 10월 업데이트/Redstone 5)

노트:
클라이언트가 이러한 운영 체제 중 하나가 아니면 차단됩니다. 필요한 경우 레지스트리 키를 설정하면 관리자가 차단을 재정의할 수 있습니다.

Redstone 4 지원의 경우 운영 체제를 업그레이드하기 전에 에이전트를 업그레이드해야 합니다. https://www.dell.com/support/article/us/en/04/sln307922을 참조하십시오.

노트:
Data Guardian은 Redstone 3 이상 버전의 Microsoft WDEG(Windows Defender Exploit Guard) 또는 Redstone 2 이하 버전의 EMET(Enhanced Mitigation Experience Toolkit)와 호환되지 않습니다.

Windows 7은 Data Guardian 감사 이벤트에 대한 지리 위치 정책과 함께 지원되지 않습니다.

Data Guardian은 한 대의 컴퓨터에 여러 버전의 Office를 지원하지 않습니다.

Microsoft Office

Data Guardian은 다음과 같은 버전의 Office를 지원합니다. 그러나 Office 중 하나의 버전만 설치되어 있어야 합니다.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: 버전 1705, 1708 및 1803(Semi-Annual Channel)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**In Translation**

Mac용 Data Guardian

다음 목록에는 Mac 클라이언트를 사용할 수 있도록 지원되는 하드웨어가 나와 있습니다.

MAC 하드웨어

- Intel Core 2 Duo, Core i3, Core i5, Core i7 또는 Xeon 프로세서
- 2GB RAM
- 10GB의 사용 가능한 디스크 공간

운영 체제

다음 목록에 지원되는 운영 체제가 나와 있습니다.

Mac 운영 체제

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.5

클라우드 스토리지 제공업체

정책 설정에 따라 Mac 인터페이스용 Data Guardian에 다음이 표시될 수 있습니다. 사용자가 클라우드 동기화 클라이언트를 다운로드하거나 설치할 필요가 없습니다.

클라우드 스토리지 제공업체

- Dropbox
- Box
- Google Drive

  노트:
  *Google 백업 및 동기화*가 지원되지 않습니다.

- OneDrive
- OneDrive for Business

Microsoft Office

Mac용 Data Guardian은 다음 버전의 Office를 지원합니다.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6
Status	In Translation

모바일 애플리케이션용 Data Guardian

다음은 모바일용 Data Guardian에서 지원되는 운영 체제 목록입니다.

Android 운영 체제

- 5.0—5.1.1 Lollipop
- 6.0—6.0.1 Marshmallow
- 7.0—7.1.2 Nougat
- 8.0—8.1 Oreo
- 9.0 Pie

iOS 운영 체제

- iOS 10.x—10.3
- iOS 11.x—11.4.1
- iOS 12.x—12.1.4

Chromebook 운영 체제

Chrome OS에서 Android 애플리케이션을 실행하려면 Chrome OS 버전 M53 이상이 필요합니다. 이러한 장치는 Chrome OS에서 Android 앱을 실행할 수 있도록 검증되었지만 영업 담당자와 옵션을 확인하십시오.

- https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

모바일 애플리케이션용 Data Guardian은 다음 버전의 Office로 만든 파일을 열 수 있습니다.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A
Status	In Translation

웹용 Data Guardian

Data Guardian 웹 클라이언트를 활성화하기 위해 관리자는 웹 클라이언트를 호스팅하고 Dell Server v9.8 이상과 통신하는 가상 컴퓨터를 설정합니다 .

다음 가상화된 환경을 사용하여 Data Guardian 웹 클라이언트를 배포할 수 있습니다.

가상 환경

- **VMware ESXi 6.7**
  - 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.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-67/index.jsp를 참조하십시오.

- **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.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-55/index.jsp를 참조하십시오.

- **Microsoft Hyper-V**
  - SLAT(Second Level Address Translation)가 있는 64비트 프로세서
  - 8GB 이상의 RAM 권장
  - 하드웨어가 최소 Hyper-V 요구 사항을 충족해야 함
  - 자세한 내용은 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements를 참조하십시오.

노트:
이러한 최소 구성은 단일 웹 포털에 대한 동시 연결 수가 25개 이하라는 것을 나타냅니다.

클라우드 스토리지 제공업체

정책 설정에 따라 Data Guardian의 웹 포털에서 이러한 클라우드 스토리지 제공업체에 액세스할 수 있습니다.

클라우드 스토리지 제공업체

- OneDrive for Business

Microsoft Office

웹용 Data Guardian은 다음 버전의 Office로 생성된 파일을 열 수 있습니다.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

기타 요구 사항

현재 Amazon Cognito의 다단계 인증(MFA)은 Data Guardian 플랫폼에서 지원되지 않습니다.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

웹 브라우저

Internet Explorer, Mozilla Firefox, Google Chrome 및 Microsoft Edge에서 Data Guardian을 사용할 수 있습니다.

Mac의 경우 Safari도 지원됩니다.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

Windows 및 Mac의 경우 보호된 .pdf 파일을 Adobe Acrobat Reader DC로 열 수 있습니다.

노트:
Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC 및 Adobe Acrobat DC는 지원되지 않습니다.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	In Translation

Windows에서 Data Guardian 설치 또는 제거

Data Guardian을 설치하려면 해당 컴퓨터의 로컬 관리자여야 합니다.

Data Guardian이 설치된 후에 컴퓨터를 다시 시작하기 위해 준비합니다.

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	In Translation

Windows용 설치 작업의 개요

이 개요에서는 Data Guardian의 설치에 대한 순서를 요약합니다.

Data Guardian 설치

작업	설명	자세한 내용
Data Guardian 설치	다음 사항 파악: 사용자가 Data Guardian을 설치해야 합니다. 관리자가 Data Guardian을 이미 설치하였습니다 - 다음 단계를 진행합니다.	사용자 설치: Windows에 Data Guardian 대화형 설치를 참조하십시오. 재부팅을 하고 다음 단계를 계속 진행하십시오.
활성화 상태 확인	알림 영역에서 Data Guardian 아이콘에 녹색 확인 표시()가 있는지 확인하십시오.	아이콘에 주황색 느낌표가 있는 경우에는 활성화에서 발생할 수 있는 문제 - 클라우드 및 보호된 Office를 참조하십시오. **노트:** Office 문서를 열었을 때 설치 또는 활성화 정보가 있는 표지 페이지가 표시되는 경우에는 관리자가 Office 문서를 보호하기 위한 정책을 설정해 놓은 것일 수 있습니다. Data Guardian이 설치되고 활성화되어 있는지 확인하십시오.

Windows용 옵션

작업	설명	자세한 내용
알림 영역 메뉴 보기	파일, 폴더, 문제 해결에 대한 유용한 정보를 제공합니다.	Data Guardian 알림 영역 메뉴 항목 이해

Identifier	GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962
Status	In Translation

암호화되지 않은 파일이 담겨 있는 기존 폴더

Data Guardian을 배포하기 전에 대상 장치에 클라우드 저장소 공급자 계정이 아직 설정되지 않은 상태가 가장 좋습니다.

Data Guardian 설치 전에 로컬 컴퓨터와 동기화된 폴더를 사용하여 클라우드 저장소 공급자 계정이 설정된 경우:

- 클라우드로 동기화되는 기존의 파일 및 폴더는 일반 텍스트를 유지합니다.
- 이러한 기존 폴더에 추가하는 파일도 일반 텍스트를 유지합니다.
- 클라우드로부터 동기화되는 파일은 암호화됩니다.

Identifier	GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8
Status	In Translation

Windows에서의 Data Guardian 대화형 설치

Data Guardian을 설치하려면 로컬 관리자여야 합니다. 사용자가 제품을 설치할 경우에는 사용자에게 설치 미디어의 위치를 알려주십시오.

시작하기 전에

환경 및 Data Guardian 제품에 따라 다음 중에서 필요한 사항을 결정합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 환경이 멀티 테넌트인 경우 설치 ID가 필요합니다.	반드시 Dell Server의 이름을 알고 있어야 합니다.

Data Guardian 설치

Data Guardian이 설치된 후에 컴퓨터를 다시 시작하기 위해 준비합니다.

1. Data Guardian 설치 프로그램을 다운로드하려면 관리자가 지정한 위치로 이동하십시오.
2. 운영 체제에 따라 32비트 또는 64비트 설치 프로그램을 선택하고 로컬 컴퓨터에 복사합니다. 다음은 샘플 설치 프로그램 이름입니다.
   - 호스팅된 Dell 보안 센터 - 설치 프로그램 이름의 확장명은 .exe입니다.
   - 사내 환경 - 설치 프로그램 이름의 확장명은
     - .exe입니다.
     - Workspace ONE용 .msi 확장명 및 MSI 설치
3. 파일을 더블 클릭하여 설치 관리자를 시작합니다.
4. 보안 경고가 표시되면 **실행**을 클릭합니다.
5. 언어를 선택하고 **확인**을 클릭합니다.
6. Microsoft Visual C++ 2015 재배포 가능 패키지 또는 Microsoft .NET Framework 4.5.2 Client Profile을 설치할 것인지 묻는 메시지가 표시되면 **확인**을 클릭합니다.
7. 시작 화면에서 **다음**을 클릭합니다.
8. 라이센스 계약서를 읽고 조건을 수락한 후 **다음**을 클릭합니다.
9. 대상 폴더 화면에서 **다음**을 클릭하여 C:\Program Files\Dell\Data Guardian\의 기본 위치에 설치를 합니다.

C:\Users 또는 C:\Windows 폴더나 어떤 드라이브든 루트 폴더에 Data Guardian을 설치하면 안 됩니다.

10 다음 중 하나를 선택합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버.
a **호스팅된 Dell 보안 센터**를 선택합니다. b 선택 사항으로 엔터프라이즈가 멀티 테넌트인 경우 설치 ID를 입력합니다. **노트:** 엔터프라이즈가 멀티 테넌트이고 설치 ID를 입력하지 않은 경우 관리자가 나중에 레지스트리에 추가할 수 있습니다. c **계속**을 클릭합니다. d 11단계를 계속 진행합니다.	a **사내 Dell Management Server**를 선택합니다. b *Dell Management Server 이름:* 필드에서 컴퓨터가 통신하는 Dell Server 이름(예: server.domain.com)을 입력합니다. www 또는 http(s)를 입력할 필요는 없습니다. 이 정보는 관리자가 제공합니다. **노트:** 관리자가 지시하는 경우를 제외하고 *SSL 신뢰 확인 활성화* 확인란을 선택 해제하지 마십시오. c **다음**을 클릭합니다. d Dell Management Server 정보 확인 화면에서 Dell Server URL 주소가 올바른지 확인합니다. 설치 프로그램이 www 또는 http(s)와 포트를 추가합니다. **다음**을 클릭합니다. e 11단계를 계속 진행합니다.

11 관리 유형 창에서 이 옵션을 선택합니다.

- 내부 사용 - 회사 도메인 내부에 이메일 주소를 갖고 있는 사용자.

12 **설치**를 클릭하여 설치를 시작합니다.
상태 창에 설치 진행률이 표시됩니다.

13 설치 완료 화면이 표시되면 **마침**을 클릭합니다.

14 다시 시작하려면 **예**를 클릭합니다.
Data Guardian 설치가 완료되었습니다.

15 사용자가 활성화를 확인해야 합니다. Data Guardian 알림 영역 아이콘에 녹색 체크 표시  가 표시됩니다.

노트:

엔터프라이즈 내에 Data Guardian이 배포된 방식에 따라 즉각 활성화되지 않을 수도 있습니다. 그러나 활성화가 발생하지 않으면 사용자가 수동으로 활성화해야 합니다.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

활성화에서 발생할 수 있는 문제 - 클라우드 및 보호된 Office

Data Guardian을 설치하였지만 알림 영역의 Data Guardian 아이콘에 녹색 확인 표시()가 없는 경우에는 클라우드 암호화, 보호된 Office 또는 양쪽 모두가 있는지 여부에 따라 다음과 같은 사항을 고려하십시오.

Data Guardian 옵션	발생할 수 있는 문제
보호된 Office	• Data Guardian을 사용하면 기존의 Office 문서를 활성화하기 전에 보호 모드로 변환할 수 있습니다. 이렇게 하면 Office 문서를 열 때 활성화 방법에 관한 정보가 있는 표지 페이지가 표시됩니다.
클라우드 암호화	• 클라우드 동기화 웹 사이트에 대한 액세스가 차단됩니다. • 클라우드 동기화 응용 프로그램이 웹 서비스에 연결할 수 없습니다.

Data Guardian 옵션	발생할 수 있는 문제
	• 로컬 동기화된 폴더는 업데이트되지 않습니다.

다음 중 하나를 수행합니다.

- 재부팅을 하고 user_name@domain.com과 같은 UPN 접미사를 사용하여 다시 로그인합니다.
- Data Guardian을 설치하였을 때 *SSL 신뢰 확인 활성화* 확인란을 선택해야 하는지 여부를 관리자와 확인합니다.
- 컴퓨터를 수동으로 활성화하도록 구성하였는지에 관해서는 시스템 관리자에게 문의하십시오. Data Guardian 활성화를 참조하십시오.

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**In Translation**

Data Guardian 활성화

일반적으로 Data Guardian은 설치 및 리부팅 후에 자동으로 활성화됩니다. 관리자가 수동 활성화를 지시하는 경우에는 다음과 같은 단계를 따릅니다.

1 다음과 같이 Windows에 로그인합니다.
알림 영역에 주황색 느낌표가 있는 방패 아이콘이 표시됩니다.
2 알림 영역에서 **Data Guardian** 아이콘을 클릭하고 **사용자 활성화**를 선택합니다.
3 도메인 이메일 주소와 도메인 암호를 입력하고 **활성화**를 클릭합니다.
내부 사용자(도메인 이메일 주소 사용)일 경우 "등록" 단추를 무시합니다. 외부 사용자만 등록합니다.

활성화가 완료되면 Data Guardian 알림 영역 아이콘()에 녹색 체크 표시가 나타납니다.
4 사용자 모드 상태를 확인합니다. 알림 영역 아이콘을 클릭하고 **세부 정보**를 선택합니다.
5 상단에서 다음과 같은 사용자 모드를 확인합니다.
내부: 회사 도메인 내부에 이메일 주소를 갖고 있는 사용자.

외부: 도메인 이메일 주소 이외의 이메일 주소를 갖고 있는 사용자. 자세한 내용은 외부 사용자로 Data Guardian 사용을 참조하십시오.

> **노트:**
> 사용자 모드에 **미등록**이 뜨면 Data Guardian이 활성화되지 않습니다.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

호스팅된 Dell 보안 센터 및 일시 중지된 테넌트

호스팅된 Dell 보안 센터에서 테넌트가 지정된 기간 동안 지불하지 않는 경우 해당 테넌트를 일시 중지할 수 있습니다. (Windows, Mac, 모바일, 웹 포털에 적용됨)

Data Guardian 내부 및 외부 사용자는 다음을 경험할 수 있습니다.

- 모든 플랫폼 - Data Guardian을 설치하거나, 활성화하거나, 로그인하려고 하면 테넌트가 일시 중지되었다는 대화 상자가 표시됩니다.
- Mac - Data Guardian이 열려 있는 동안 테넌트가 일시 중지된 경우 탐색기 및 모든 파일을 닫은 후 보호된 파일을 열면 일시 중단된 테넌트 대화 상자가 표시됩니다.
- 웹 포털:

- 이미 로그인한 상태에서 암호화된 파일을 업로드하면 업로드 실패 메시지가 표시됩니다.
- 암호화되거나 암호화되지 않은 파일을 업로드한 후 테넌트가 일시 중지된 경우 다운로드 실패 메시지가 표시됩니다.
- 로그아웃한 후 다시 로그인하려고 하면 테넌트가 일시 중지되었음을 나타내는 대화 상자가 표시됩니다.

관리자에게 문의하십시오.

Identifier	GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65
Status	In Translation

Data Guardian 알림 영역 메뉴 항목 이해

세부 정보 화면

Data Guardian 세부 정보 화면에는 다음과 같은 유용한 정보가 제공됩니다.

- 기술 지원을 위해, 사용자가 상태 또는 버전 정보를 제공할 수 있습니다.
- 파일 이름을 검색하려면 오른쪽 하단에서 복사를 선택하고 컨텐츠를 Word 파일에 붙여 넣습니다.
- 누가 폴더를 소유하고 있는지 확인하려면, 폴더를 선택하고 폴더 소유권 열로 스크롤합니다.

세부사항 화면에 액세스하려면,

Data Guardian 알림 영역 아이콘을 오른쪽 마우스로 클릭한 다음에 **세부 정보**를 클릭합니다.

세부 정보 화면의 왼쪽 상단에 다음 정보가 표시됩니다.

서비스 상태: Data Guardian Windows Service의 상태. 중지됨, 보류 시작, 보류 중지, 실행 중, 보류 계속, 보류 일시 중지, 일시 중지됨 값이 있습니다.

실행 상태: 장치 활성화 상태. 활성화, 재활성화 중, 일시 중지됨, 일시 중지 값이 있습니다.

사용자 모드:

- **내부 사용자** - 이 도메인 주소 내의 사용자
- **외부 사용자** - 이 도메인 주소 밖의 사용자
- **미등록** - Data Guardian이 활성화되지 않은 내부 또는 외부 사용자입니다.

등록 이메일: 내부 사용자의 경우 도메인 이메일 주소입니다. 외부 사용자의 경우, 사용자가 등록되어 있는 이메일입니다.

서버 URL: 이 클라이언트와 통신하는 Dell Server.

마지막 정책 수정일: 정책이 마지막으로 수정되고 클라이언트에서 사용한 날짜와 시간.

정책 버전: Dell Server에서 생성한 정책 버전.

세부 정보 화면의 **파일** 영역에는 다음과 같은 정보가 표시됩니다.

이름: 파일의 이름

클라우드: 이 기능은 비활성화되었으므로 더 이상 데이터가 없습니다.

파일 상태: 이 값은 폴더 소유자를 표시합니다. 값은 키 ID로 결정됩니다.

처리 상태: 파일이 키가 필요한지 *완료* 상태인지를 표시합니다.

엔터프라이즈: 기본 서버를 목록에 표시합니다. 이 열에 *오류: 서버의 키가 아닙니다*라는 메시지가 표시되면 키가 해당 엔터프라이즈의 서버에 속한 것이 아닙니다. 암호화된 파일을 위한 키는 반드시 귀하의 엔터프라이즈 서버에 속해야 합니다.

키: 폴더에 할당된 키 ID(새 파일이 이 키를 사용하여 암호화됨)

폴더: 폴더의 모든 경로명.

마지막 수정일: 파일이 수정된 날짜.

지속성 상태: 이것은 파일이 디스크에 있는지 여부를 표시합니다.

XEN 파일 읽기: 이 기능은 비활성화되었습니다.

브라우저 생성: *참* 또는 *거짓*.

로그 파일을 보려면 세부 정보 화면의 우측 하단에서 **로그 보기**를 클릭합니다.

노트:
로그 파일은 C:\ProgramData\Dell\Data Guardian에도 있습니다.

이전에는 Data Guardian의 클라우드 암호화에 세부 정보 화면의 **폴더** 영역이 있었습니다. 현재는 클라우드 암호화가 비활성화되었습니다.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

정책 업데이트 확인

관리자가 정책을 수정하고 정책 업데이트를 사용자에게 통보하는 경우에는 Windows 알림 영역으로 이동하여 **Dell Data Guardian** 아이콘을 클릭하고 **정책 업데이트 확인**을 선택합니다.

관리자가 Microsoft Word에서 생성된 파일을 보호하기 위한 정책을 수정하는 경우에는 해당 업데이트가 적용되도록 Word를 닫아야 합니다.

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

로그 파일 찾기

문제 해결을 위해 관리자가 로그 파일을 요청할 수 있습니다.

로그 파일을 찾으려면 다음을 수행합니다.

1 이동
2 **Xendow.Service.log**를 선택합니다.

노트:
Xendow.Service.log 파일 크기가 3MB에 도달하면 Xendow.Service1.log로 저장된 다음 Xendow.Service2.log로 저장됩니다.

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

Data Guardian 업그레이드

먼저 이전 버전을 설치 제거한 후에 최신 버전을 설치하는 것이 좋습니다. Data Guardian 설치 제거를 참조하십시오.

Identifier	GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6
Status	In Translation

Windows에서 Data Guardian 제거

관리자가 Data Guardian을 설치하였다면 관리자만 이 제품의 설치를 제거해야 합니다. 폴더를 공유하도록 초대를 받았고 외부 컴퓨터에 대한 관리자 권한이 있는 외부 사용자도 해당 외부 컴퓨터에서 Data Guardian의 설치를 제거할 수 있습니다.

Identifier	GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6
Status	In Translation

Data Guardian 제거

컴퓨터의 로컬 관리자만이 Data Guardian의 설치를 제거할 수 있습니다.

로컬 드라이브에 파일 복사

컴퓨터나 장치에서 Data Guardian의 설치를 제거할 경우, 동기화 클라이언트 웹 사이트의 파일은 계속 보안 설정되어 있어야 암호화를 유지할 수 있습니다.

1 설치 제거하기 전에 액세스해야 할 파일이 있는지 확인합니다.
2 파일을 로컬 드라이브에 복사합니다.

동기화 클라이언트 웹 사이트의 폴더 및 파일은 사용자가 다운로드해도 암호화됩니다. 해당 폴더 및 파일을 보려면 Data Guardian을 재설치해야 합니다. 또는 파일을 Data Guardian 웹 포털에서 볼 수 있습니다.

Data Guardian 제거

1 프로그램을 제거하려면 Windows의 제어판을 사용하십시오.
2 **Dell Data Guardian**을 선택하고 상단 메뉴에서 **변경**을 클릭합니다.
3 시작 화면이 표시되면 **다음**을 클릭합니다.
4 **제거**를 선택하고 **다음**을 클릭합니다.
5 Dell Data Guardian 설치 제거를 확인하는 경고가 표시됩니다. 그러면 **다음**을 클릭합니다.
6 프로그램 제거 화면에서 **제거**를 클릭합니다.
상태 창에 진행 과정이 표시됩니다.
7 동기화 클라이언트에서 오류 대화상자가 나타나면 **계속**을 클릭합니다.
8 대화 상자에 Office 문서가 열렸다고 표시되는 경우 **확인**을 클릭하고 Office 문서를 닫고 다시 설치 제거를 시작합니다.
9 완료 화면이 표시되면 **마침**을 클릭합니다.
10 다시 시작하려면 **예**를 클릭합니다.

Data Guardian 설치 제거가 완료되었습니다.

Identifier	GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D
Status	Translation Validated

Dell에 피드백 제공

관리자가 피드백을 사용하도록 설정한 경우에는 사용자가 이 제품에 대한 의견을 Dell에 보낼 수 있습니다. 평가 등급(10은 최고 만족도)을 포함하여 만족도에 대한 2개의 질문과 의견란이 있는 간단한 양식이 제공됩니다.

액세스하려면 알림 영역에서 Data Guardian 아이콘을 클릭하고 **피드백 보내기**를 선택합니다.

정책을 통해 이 기능이 사용되도록 설정되지 않으면 옵션이 표시되지 않습니다.

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	In Translation

Windows에서 Data Guardian 사용하기

관리자가 이미 문서 보호를 위한 정책을 구성했으며 엔터프라이즈에 적용되는 옵션은 어떤 것들이 있는지 알려줄 것입니다.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	In Translation

옵션의 개요

이 개요에는 관리자가 설정한 정책을 기반으로 Data Guardian에서 사용 가능한 옵션이 요약되어 있습니다. 해당 문서를 다른 사용자와 공유하거나 이동식 미디어에 저장하면 안전할 것입니다.

옵션	설명	자세한 내용
Office 및 매크로가 활성화된 문서	여기에는 .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm, .pdf가 포함됩니다.	Office 문서에 대한 보안 수준을 결정하기 위한 파일 메뉴 옵션 관찰을 참조하십시오. 다음 모드 중 하나가 시행됩니다. • 옵트인 • 강제 보호
기본 파일 보호	엔터프라이즈에서 암호화하고 관리자가 구성하고자 하는 추가 애플리케이션 및 파일 형식입니다.	기본 파일 보호를 통한 추가 애플리케이션 및 파일 형식 보호를 참조하십시오.
추가 옵션	이는 Office 문서나 기본 파일 또는 양쪽 모두에 적용될 수 있습니다.	Data Guardian을 위한 추가 옵션을 참조하십시오.
외부 사용자와 파일 공유	비 도메인 이메일 주소의 사용자입니다(다른 엔터프라이즈의 사용자 또는 비 도메인 이메일 주소에서 보호된 파일에 액세스를 희망하는 내부 사용자).	외부 사용자로 Data Guardian 사용을 참조하십시오.

보호된 Office 문서를 사용하여 온라인으로 작업하기

보호된 문서를 만들 때는 해당 문서에 대한 키가 생성되기 때문에 온라인으로 작업하는 것이 가장 좋습니다. 컴퓨터에 이미지가 재설치되고 보호된 문서를 오프라인으로 만들었다면 관리자에게 알려야 합니다.

파일 속성 > Dell Data Guardian 탭

보호된 Office 문서에서 마우스 오른쪽 단추를 클릭하여 **속성**을 선택할 수 있습니다. **Dell Data Guardian** 탭에는 파일의 키 ID, 액세스 및 엠바고 데이터와 같은 정보가 표시됩니다.

Windows의 오버레이 아이콘

Data Guardian 2.2 이상의 경우, 파일 탐색기의 보호된 파일에 오버레이 아이콘이 표시됩니다. 보호된 파일을 마우스 오른쪽 단추로 클릭하면 Dell Data Guardian 탭에 추가 정보가 표시됩니다.

숨겨진 워터마크

관리자가 설정한 정책에 따라 보호된 Office 문서에 사용자를 식별하는 숨겨진 워터마크가 있을 수 있습니다. 문서를 인쇄 또는 공유하는 경우, 워터마크가 유지됩니다.

노트:
Office 문서를 열었을 때 설치 또는 활성화 정보가 있는 표지 페이지가 표시되는 경우에는 관리자가 Office 문서를 보호하기 위한 정책을 설정해 놓은 것일 수 있습니다. Data Guardian이 설치되고 활성화되어 있는지 확인하십시오. 활성화에서 발생할 수 있는 문제 - 클라우드 및 보호된 Office를 참조하십시오.

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

Data Guardian의 보호 모드로 Office 문서 사용

엔터프라이즈 보안을 향상시키기 위해 관리자가 다음과 같은 Office 애플리케이션에 대한 파일을 보호하기 위한 정책을 활성화할 수 있습니다.

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm
- .pdf

승인 받지 않은 사람이 보호된 파일에 액세스할 경우에 파일은 암호화를 유지합니다. 예를 들면 다음과 같은 경우가 있습니다.

- 이메일에 첨부
- 브라우저에서 이동 - 일부 클라우드 동기화 클라이언트에서는 파일 이름을 마우스 오른쪽 단추로 클릭하고 **이동**을 선택합니다.
- 네트워크에서 공유
- 클라우드 스토리지 서비스로 업로드
- 이동식 미디어에 저장

Office 문서의 경우에는 Data Guardian의 설치 또는 활성화에 대한 지침이 있는 표지 페이지가 표시될 수 있습니다. 예를 들면 다음과 같습니다.

- Data Guardian을 설치해야 합니다.
- Data Guardian을 활성화해야 합니다.
- 클라우드에서 보호된 Office 문서를 열었습니다.
- 사용자가 Office 파일을 Data Guardian이 있는 자신의 컴퓨터에서 없는 개인 장치로 다운로드하였습니다.
- 권한이 없는 사용자가 Office 파일 중의 하나에 액세스합니다 - 엔터프라이즈에 특정한 메시지가 있는 표지 페이지가 표시되지만 권한이 없는 사용자는 파일의 컨텐츠를 볼 수 없습니다.

Office 문서에 대한 보안 수준을 결정하기 위한 파일 메뉴 옵션 관찰

관리자가 Data Guardian 정책을 활성화하였는지를 결정하려면 Office 문서를 열고 **파일**을 선택합니다. 왼쪽 창에 *보호된 다른 이름으로 저장*이 표시되면 Office 문서에 대한 추가 보호가 있는 것입니다.

보안 수준을 결정하려면 다음과 같이 활성화되어 있거나 비활성화되어 있는 옵션을 관찰하십시오.

- **옵트인 모드** - 보호할 Office 문서를 결정할 때 옵션이 일부 있습니다.
  - *다른 이름으로 저장*과 *보호된 다른 이름으로 저장*이 활성화되어 있습니다 - Office 문서를 보호하기로 선택하였다면 **보호된 다른 이름으로 저장**을 선택합니다.

  - *인쇄* 및 *내보내기*는 정책에 따라 활성화 또는 비활성화되어 있을 수 있습니다.
  - *공유*가 활성화되었습니다.
  - **문서 > 보안 문서** 폴더 - 옵트인 모드(강제 보호 모드는 제외)를 사용할 경우에 보안 문서 폴더가 문서 폴더의 루트에 추가됩니다. 이 폴더의 Office 문서는 암호화됩니다. 보호된 Office 문서를 이 폴더에서 제거해도 암호화 상태를 유지합니다. 폴더의 이름을 변경해도 이름이 변경된 폴더의 컨텐츠는 암호화 상태를 유지합니다. 폴더를 삭제하면 다시 생성됩니다.
- **강제 보호 모드** - 사용자의 엔터프라이즈에서 더 높은 수준의 보안을 요구합니다.
  - *다른 이름으로 저장*이 비활성화되어 있고 *보호된 다른 이름으로 저장*이 활성화되어 있습니다 - 모든 Office 문서를 보호 모드로 저장해야 합니다.
  - *인쇄* 및 *내보내기*는 정책에 따라 활성화 또는 비활성화될 수 있습니다.
  - *공유*가 비활성화되었습니다.

    노트:
    강제 보호 모드에서는 정책이 특정 시간을 활성화하여 컴퓨터를 스윕하여 보호되지 않은 Office 파일을 찾아 보호 모드로 변경하도록 하기도 합니다. Data Guardian이 보호되지 않은 Office 파일을 스윕하려면 로그인되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
  - **문서 > 보호되지 않은** 폴더 - 강제 보호 모드에서 정책에 의해 활성화되어 있지만(옵트인 모드는 제외) 보호되지 않은 폴더는 문서 폴더의 루트에 추가됩니다. 이 폴더의 Office 문서는 해독됩니다. 폴더를 삭제하면 다시 생성됩니다.

- **보호된 다른 이름으로 저장**을 선택하는 경우 *다른 이름으로 저장 유형* 필드에서 유일한 옵션은 *Office 보호*입니다.

- **파일 > 정보**는 예를 들면 다음과 같이 다양하게 나타날 수 있습니다.
  - 옵트인 및 강제 보호 모드 양쪽 모두의 경우: 관리자가 해당 정책을 활성화하였을 경우 *날짜 제한 추가*가 표시됩니다. 날짜 제한을 추가하여 보안을 향상을 참조하십시오.
  - 옵트인 및 강제 보호 모드 양쪽 모두에 해당: 작성자 및 날짜와 같은 이 Office 문서에 관한 속성 정보가 보안 향상을 위해 숨겨집니다.
  - 읽기 전용 상태: 자세한 내용은 아래를 참조하십시오.

    노트:
    파일 > 정보의 *문서 보호* 옵션은 Data Guardian의 보호 모드가 아닌 Microsoft Office와 관련이 있습니다.

Office 문서를 열었을 때 읽기 전용 모드로 나타나면 다음과 같은 사항을 확인하십시오.

- *보호된 다른 이름으로 저장*이 왼쪽 창에 표시되지 않으면 읽기 전용은 Data Guardian 정책과 관련이 없는 것입니다.
- 관리자가 정책을 더 높은 보안 수준인 강제 보호 모드로 설정하였다면 보호되지 않은 Office 문서는 읽기 전용 모드로 열립니다.

  노트:
  OneDrive의 경우에 **파일 > 열기 > OneDrive**를 통하여 보호되지 않는 Office 문서를 열었는데 해당 문서가 읽기 전용인 경우에는 OneDrive 동기화 클라이언트를 설치하고 설정하였는지 확인하십시오.

Identifier	**GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF**
Status	**In Translation**

Office 문서 보호를 위한 옵트인 모드 사용

사용자의 엔터프라이즈에서 Data Guardian의 보호 모드를 사용하는 경우에 다음을 참조하십시오.

- 옵트인 모드에서 파일 메뉴 옵션 작업하기
- Data Guardian을 위한 추가 옵션

옵트인 모드에서 파일 메뉴 옵션 작업하기

이 표에는 Office 문서에 대한 파일 메뉴 옵션이 나와 있습니다. 보안 수준에 따라 일부 옵션은 회색으로 표시됩니다.

노트:
현재 내장형 Office 문서는 보호된 Office 모드로 지원하지 않습니다.

파일 메뉴	옵트인 모드 및 보호된 Office 문서
열기	파일은 일반적으로 열립니다.
저장	• 옵션: 이미 보호되는 문서 - 보호된 상태로 저장됩니다. 비보호 - 비보호 상태로 저장됩니다. 보호하려면 **보호된 다른 이름으로 저장**을 클릭합니다. • 읽기 전용 문서 - 보호되지 않은 문서를 저장할 수 없다는 대화 상자가 표시됩니다. *다른 이름으로 저장* 창이 열리면 해당 파일을 다른 파일 이름으로 저장해야 합니다.
다른 이름으로 저장	표준 옵션이 있습니다(보호 모드는 제외).
보호된 다른 이름으로 저장	다른 이름으로 저장 유형 필드에서 유일한 옵션은 Office 보호입니다.
인쇄	**사용** 보호된 Office 문서의 경우 관리자가 정책을 통해 인쇄를 비활성화한 경우에는 인쇄를 선택할 수 있으나 보호된 문서를 인쇄할 수 없다는 토스트 메시지가 표시됩니다. 관리자가 인쇄를 허용한 경우에도 다른 정책을 통해 인쇄할 때 각각의 페이지마다 사용자 이름, 도메인 이름 및 컴퓨터 ID를 포함하는 워터마크가 표시될 수 있습니다.
공유	보호된 Office 문서에서 **사용**. 보호되지 않은 문서에서 **사용 안 함**.
내보내기 (Office 2013 이상)	관리자가 정한 정책에 따라 활성화되거나 회색으로 표시될 수 있습니다.
보호된 내보내기 (Office 2013 이상)	내보내기 메뉴 옵션이 회색으로 표시되고 보호되는 내보내기가 활성화되어 있으면 문서는 페이지마다 사용자 이름, 도메인 이름 및 컴퓨터 ID를 포함하는 워터마크를 표시하면서 내보내기가 됩니다. 보호 모드 문서를 외부 사용자에게 내보내는 경우, 외부 사용자는 해당 문서를 열어 볼 수는 있지만 내보내기를 하거나 인쇄를 할 수는 없습니다.

매크로가 활성화된 보호된 문서를 이용하여 온라인으로 작업하기

매크로가 활성화된 보호된 문서에서는 매크로가 존재하지만 차단됩니다. 하지만 현재 Data Guardian에서는 새로 보호되는 문서(.docm, .pptm, .xlsm)를 닫고 다시 연 후에만 매크로가 활성화된 문서를 제어할 수 있습니다. 또한 매크로가 보호되지 않은 보호된 문서를 저장하는 경우에는 해당 문서를 닫고 다시 열어야 매크로를 실행할 수 있습니다.

TITUS 분류 및 옵트인 모드

정책이 활성화되어 있는 경우 관리자는 TITUS 분류를 구성하여 해당 분류로 문서를 암호화합니다. 보호되지 않은 Office 문서를 마우스 오른쪽 단추로 클릭하고 TITUS 분류를 선택할 수 있습니다. 이는 Office 문서를 보호할 다른 방식을 제공합니다.

데이터 분류 및 옵트인 모드

이 정책이 활성화되어 있는 경우, 관리자는 주민등록번호, 신용카드번호 또는 민감한 정보의 특정 내용에 대해 분류를 설정할 수 있습니다. 관리자가 어떤 정보가 분류되었는지 알려줄 것입니다. 이러한 분류 규칙에 따라 정보가 포함되어 있는 문서를 저장할 때 문서가 암호화됩니다.를

정책의 파일 태그 메타데이터에서 사용되는 데이터 분류를 트리거하기 위해 Office 문서에 태그를 사용하는 경우, Office 문서에서 사용하는 태그는 대/소문자가 구분되며 정책에 따라 관리자가 사용하는 대/소문자와 일치합니다.

노트:
이 정책을 활성화하면 스윕이 분류 규칙을 충족하는 파일을 암호화하도록 만듭니다. 그러나 파일을 만들 때 마우스 오른쪽 단추로 클릭하고 **파일 보호**를 선택할 수 있습니다.

Data Guardian으로 Outlook 이메일 암호화도 참조하십시오.

옵트인 모드에 대한 문제 해결

Data Guardian 정책에 따라 보호된 Office 문서에 대한 인쇄가 비활성화된 경우에도 **파일 > 정보**에서 인쇄를 선택하거나 Windows 탐색기에서 보호된 Office 문서를 마우스 오른쪽 단추로 클릭하여 인쇄를 선택할 수 있습니다. 하지만 인쇄를 선택하면 다음과 같은 일이 발생합니다.

- Word - Word가 작동을 멈추었다는 대화 상자가 표시됩니다.
- Excel - 인쇄가 정책에 의해 비활성화되었다는 대화 상자가 표시됩니다.
- PowerPoint - 인쇄가 정책에 의해 비활성화되었다는 대화 상자가 표시됩니다. 확인을 클릭하면 문서가 보호되어 있다는 표지 페이지가 인쇄됩니다.

어떤 옵트인 모드 문서가 보호되는지를 결정하기

옵트인 모드를 사용하고 있는데 어떤 문서의 보호 여부를 알고 싶으면 해당 문서를 열어보십시오. 제목 표시줄에 보호 여부가 나타날 것입니다.

노트:
강제 보호 모드를 사용하면 모든 Office 문서가 보호됩니다.

Identifier	**GUID-5E368002-F3BB-48A7-9A30-B4591019B21F**
Status	**In Translation**

강제 보호 모드를 사용하여 Office 문서 보호

사용자의 엔터프라이즈에서 Data Guardian의 보호 모드를 사용하는 경우에 다음을 참조하십시오.

- 강제 보호 모드를 위한 파일 메뉴 옵션 작업하기
- Data Guardian을 위한 추가 옵션

강제 보호 모드를 위한 파일 메뉴 옵션 작업하기

이 표에는 Office 문서에 대한 파일 메뉴 옵션이 나와 있습니다. 보안 수준에 따라 일부 옵션은 회색으로 표시됩니다.

노트:
현재 내장형 Office 문서는 보호된 Office 모드로 지원하지 않습니다.

파일 메뉴	보호 및 비보호에 대한 강제 보호 모드
열기	보호되지 않는 문서는 읽기 전용 모드로 열립니다.
저장	• 문서가 보호됩니다. • 읽기 전용 문서 - 편집은 할 수 있지만 원래 문서를 저장할 수 없습니다. 저장을 클릭하여 보호 문서로 저장 창이 열리면 새 이름을 사용하여 보호 모드로 저장해야 합니다. • 원격 문서 - 원격 위치에서 문서를 열고 이 문서가 보호되어 있지 않은 경우에는 로컬 드라이브에 저장해야 수정과 저장이 가능합니다. 원격 위치에는 저장할 수 없습니다. **노트:** 저장을 클릭하면 다른 이름으로 저장 창이 열리고 다른 이름으로 저장 유형 필드에서 유일한 옵션은 Office 보호입니다(문서, 프레젠테이션 또는 통합 문서).
다른 이름으로 저장	**사용 안 함**
보호된 다른 이름으로 저장	다른 이름으로 저장 유형 필드에서 유일한 옵션은 Office 보호입니다.
인쇄	**사용** 보호된 Office 문서의 경우 관리자가 정책을 통해 인쇄를 비활성화한 경우에는 인쇄를 선택할 수 있으나 보호된 문서를 인쇄할 수 없다는 토스트 메시지가 표시됩니다. 관리자가 인쇄를 허용한 경우에도 다른 정책을 통해 인쇄할 때 각각의 페이지마다 사용자 이름, 도메인 이름 및 컴퓨터 ID를 포함하는 워터마크가 표시될 수 있습니다.
공유	**사용 안 함**
내보내기 (Office 2013 이상)	관리자가 정한 정책에 따라 활성화되거나 회색으로 표시될 수 있습니다.
보호된 내보내기 (Office 2013 이상)	내보내기 메뉴 옵션이 회색으로 표시되고 보호되는 내보내기가 활성화되어 있으면 문서는 페이지마다 사용자 이름, 도메인 이름 및 컴퓨터 ID를 포함하는 워터마크를 표시하면서 내보내기가 됩니다. **노트:** 보호 모드 문서를 외부 사용자에게 내보내는 경우, 외부 사용자는 해당 문서를 열어 볼 수는 있지만 내보내기를 하거나 인쇄를 할 수는 없습니다.

매크로가 활성화된 보호된 문서를 이용하여 온라인으로 작업하기

매크로가 활성화된 보호된 문서에서는 매크로가 존재하지만 차단됩니다. 하지만 현재 Data Guardian에서는 새로 보호되는 문서(.docm, .pptm, .xlsm)를 닫고 다시 연 후에만 매크로가 활성화된 문서를 제어할 수 있습니다. 또한 매크로가 보호되지 않은 보호된 문서를 저장하는 경우에는 해당 문서를 닫고 다시 열어야 매크로를 실행할 수 있습니다.

Identifier	GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC
Status	In Translation

Data Guardian을 위한 추가 옵션

보호된 Office 문서에 대한 추가 메뉴 옵션

Office 문서의 유형(보호 또는 비보호)이 다음과 같은 사항에 영향을 줄 수 있습니다.

마우스 오른쪽 단추로 클릭 > 보호

Office 문서를 마우스 오른쪽 단추로 클릭하고 **보호**를 선택할 수 있습니다. 표시를 하려면 메뉴 옵션에 컨텐츠를 추가해야 합니다. 빈 문서는 보호할 수 없습니다.

붙여넣기

관리자가 Office 문서를 보호하기 위한 정책을 설정한다면 다음과 같습니다.

- 보호 여부와 관계없이 데이터를 복사하여 기존의 보호된 문서 또는 보호된 PDF에 붙여 넣을 수 있습니다. 보호되지 않은 PDF는 Adobe Acrobat Reader DC에서 열 수 없습니다.
- 보호된 문서에서 보호되지 않는 문서로 복사를 하거나 붙여넣기를 할 수는 없습니다. 클립보드에 아무것도 표시되지 않고 보호되지 않거나 관리되지 않는 문서에는 붙여넣기를 할 수 없다는 엔터프라이즈별 텍스트 메시지가 표시됩니다.

> **노트:**
> 보호된 문서에서 텍스트를 잘라내고 보호되지 않은 문서에서 메시지가 나타나면 보호되는 문서에서 **실행 취소**를 클릭하여 텍스트를 검색합니다.

보호 모드에서 끌어 놓기

보호된 Word 문서에 컨텐츠를 끌어 놓을 수 있습니다. 현재 보호되는 Power Point 및 Excel 파일에서는 끌어 놓기가 비활성화되어 있습니다.

Adobe Acrobat Reader DC로 보호된 PDF 열기 및 편집

Acrobat Reader DC를 사용할 때 다음이 적용됩니다.

- 보호된 .pdf 파일에 주석을 추가하거나 양식을 완성할 수 있습니다. 파일을 저장하면 변경 내용이 포함된 새로운 보호된 .pdf 파일이 만들어집니다. 이것은 Acrobat Reader DC 기능입니다.
- 보안을 강화하기 위해, 하나의 보호된 .pdf 파일을 Acrobat Reader DC로 열면 Acrobat Reader DC를 닫을 때까지 인터넷에 액세스할 수 없습니다.
- 보안을 강화하기 위해, 보호된 .pdf가 열려 있으면 사용자가 해당 인스턴스에서 이메일을 보낼 수 없습니다.

> **노트:**
> 보호된 .pdf 파일을 네트워크에서 열 수 없습니다. Word를 사용하여 보호된 .pdf 파일을 네트워크에서 열 수 있습니다.

봉투 및 라벨용 인쇄

보호된 Office 문서를 인쇄할 때 워터마크를 추가하는 정책을 관리자가 설정한 경우에는 다음과 같은 단계를 따라 봉투나 라벨을 인쇄하십시오.

1 Word 문서에서 **우편물** 탭을 선택합니다.
2 **봉투** 또는 **라벨** 옵션을 선택합니다.
3 주소를 입력하거나 반환한 후에 **인쇄**를 클릭합니다.

노트:
사용자가 다른 옵션을 사용하여 인쇄를 하고 관리자가 인쇄된 Office 문서에 워터마크를 추가하는 정책을 설정하였다면 봉투나 라벨에 워터마크가 표시될 것입니다.

추가 옵션

프로세스 차단

관리자가 설정한 정책에 따라 일부 프로세스(예: 캡처 도구)는 차단될 수 있습니다. 관리자가 해당 프로세스에 대해 알려줄 수 있습니다. 또한, 대화 상자로 프로세스가 차단되었다는 알림이 표시됩니다.

- **강제 보호 모드** - 관리자가 *PrtScr* 단추를 차단하는 정책을 설정한 경우 터치스크린 또는 태블릿에서 화면 인쇄 기능이 차단될 수도 있습니다.
- RS5가 설치된 Windows에는 화면 스케치 앱(이전의 캡처 도구)이 있습니다. 관리자는 Data Guardian을 사용하여 이 앱을 차단하는 정책을 설정하여 보안을 강화할 수 있습니다.

보호된 문서를 Outlook 이메일에 첨부하기

Outlook 이메일에 보호된 문서를 첨부하는 경우에는 *텍스트로 삽입* 대신에 **삽입**을 선택합니다. *텍스트로 삽입*에서는 문서의 컨텐츠를 직접 이메일의 본문에 붙여 넣고 컨텐츠는 더 이상 보호되지 않습니다.

보호된 Office 문서, 정책에 따라 보호된 추가 파일 형식 또는 .xen 파일을 첨부할 수 있습니다.

Data Guardian을 사용하는 Windows의 경우 보호된 문서를 첨부하면 Data Guardian이 해당 이메일 내에 암호화된 파일에 액세스하기 위한 정보를 추가합니다.

- 내부 사용자 - 클라이언트 다운로드 링크가 포함된 정보가 표시됩니다.
- 외부 사용자 - 클라이언트 등록 및 다운로드 링크가 포함된 정보가 표시됩니다.

노트:
추가된 정보를 표시하려면 웹 기반 버전의 Outlook이 아니라 Microsoft Office Outlook에서 이메일을 보내야 합니다.

Data Guardian으로 Outlook 이메일 암호화

Data Guardian v2.0.1 이상의 정책을 기반으로, 내부 사용자는 Outlook의 왼쪽 상단에 있는 *보호* 옵션을 사용하여 이메일과 첨부 파일을 모두 암호화할 수 있습니다. 발신자와 수신자 모두에서 Data Guardian이 설치 및 활성화되어 있어야 합니다.

Data Guardian의 Outlook 이메일 암호화는 Office 2013 이상에서 지원되며 웹 메일에는 지원되지 않습니다.

사용 방법은 다음과 같습니다.

1 왼쪽 상단에 있는 **보호**를 클릭합니다.
2 외부 이메일 주소의 경우 키 공유를 수락하면 **예**를, 메일을 전송하지 않기로 결정한 경우에는 **아니오**를 클릭합니다.

가장 좋은 방법은 한 번에 하나의 이메일을 여는 것입니다. 두 개 이상의 이메일을 연 경우, 보호 단추를 클릭하기 전에 이메일을 클릭하여 포커스를 맞추십시오. 보호 단추는 마우스를 올려놓지 않으면 회색으로 표시되어야 합니다.

사용 중인 데이터는 안전합니다. 이 미리보기 릴리스에서는 저장된 데이터에 대한 DLP(데이터 손실 방지)가 부분적으로 지원됩니다. 보안은 향후 릴리스를 통해 계속 개선될 예정입니다.

DLP를 최소화하기 위해 암호화된 이메일이 열려 있을 때는 일부 작업이 비활성화되거나 차단됩니다.

- Outlook의 *빠른 단계*
- *이동*, *폴더로 이동* 및 추가 폴더 작업

- *다음* 및 *이전* 화살표
- *전달*
- 일부 마우스 오른쪽 클릭 옵션

DLP를 최소화하기 위해 암호화된 이메일이 열려 있을 때는 다음의 작업이 제어됩니다.

- *복사/붙여넣기*
- 데이터 *인쇄* 및 *내보내기*
- 일부 마우스 오른쪽 클릭 옵션
- 임시 보관함 및 *자동 저장*

Outlook 이메일의 받는 사람

암호화된 Outlook 이메일을 열면 문서가 보호되고 있다는 경고가 표시되며, 사용자는 더블 클릭으로만 이 파일을 열 수 있습니다. 이메일 내용은 커버 페이지에만 표시되고 미리 보기에 표시되지 않습니다. 호스팅된 Dell 보안 센터가 멀티 테넌트인 경우, 표지 페이지에는 사내 환경의 Dell Server 이름 또는 특정 테넌트의 설치 ID가 나열됩니다. 표지 페이지에는 Data Guardian 클라이언트 다운로드 링크도 포함되어 있습니다.

이메일 분류

데이터 분류를 통해 암호화된 보호 Office 문서에 대한 로컬 보고서(옵트인 모드)

Office 문서 및 PDF에서 민감한 정보를 보호하기 위해 관리자가 스윕 정책을 설정하고 데이터 분류에 따라 파일을 암호화할 수 있습니다. 주민등록번호, 신용카드번호, 주소, 기업 기밀 데이터 등이 이러한 민감한 정보에 해당합니다. 관리자가 파일 암호화가 필요한 민감한 정보에 대해 알려줄 것입니다.

데이터 분류를 통해 암호화된 파일에 대한 로컬 보고서와 암호화 이유를 보려면 다음과 같이 하십시오.

1 **C:\Users\<username>\AppData\Local\Dell\Data Guardian**으로 이동합니다.
2 **Classification Report.log**를 엽니다.

> **노트:**
> 파일이 암호화되고 있는 중이면 암호화가 완료될 때까지 해당 항목에 여러 개의 라인이 나타날 수 있습니다.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

기본 파일 보호를 통한 추가 애플리케이션 및 파일 형식 보호

정책이 추가 애플리케이션 및 파일 형식의 암호화를 허용하는 경우 관리자가 알려줍니다. 누군가가 기본 파일 보호를 사용하여 암호화된 파일을 열었지만 Data Guardian이 설치되어 있지 않은 경우 컨텐츠를 읽을 수 없습니다.

기본 파일 보호의 개요

애플리케이션

다음은 관리자가 암호화를 원할 수 있는 애플리케이션의 예입니다.

- 메모장

- 워드패드
- Visio
- MS paint

노트:
일부 애플리케이션은 부분적으로만 Data Guardian에서 지원되며 이는 관리자가 알려줍니다.

파일 유형

다음은 구성할 수 있는 추가 파일 형식의 예입니다: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac 및 모바일

기본 파일 보호 정책이 구성되어 있는 경우 Data Guardian은 사용자의 컴퓨터를 스윕하고 해당 확장자의 모든 로컬 파일을 암호화합니다. 기본 파일 보호를 사용하여 암호화된 파일은 파일 확장자와 관련된 애플리케이션만을 사용하여 편집하고 볼 수 있습니다.

노트:
AppData와 같이 특정 시스템 폴더에 있는 파일은 암호화되지 않습니다. Secure Documents 폴더와 같이 보호된 Office 문서와 관련된 폴더 또한 해당됩니다.

Windows의 오버레이 아이콘

Data Guardian 2.2 이상의 경우, 파일 탐색기의 보호된 파일에 오버레이 아이콘이 표시됩니다. 보호된 파일을 마우스 오른쪽 단추로 클릭하면 Dell Data Guardian 탭에 추가 정보가 표시됩니다.

Windows 또는 Mac의 스윕에서 일부 파일 제외(스윕이 활성화되기 전)

엔터프라이즈에서 .txt와 같은 추가 파일 형식을 암호화하기로 결정한 경우 해당 확장자를 가진 일부 파일을 스윕 및 암호화하고 싶지 않을 수 있습니다.

해당 확장자에 대한 기본 파일 보호를 활성화하기 전에 관리자가 폴더를 로컬 컴퓨터에 추가할 수 있는 다른 정책을 설정할 수 있으며 해당 폴더의 파일은 스윕되지 않습니다. 관리자는 정책을 설정하고, 폴더 이름을 생성하고, 폴더 이름을 제공하고, 해당 폴더를 추가할 수 있는 위치를 제안할 수 있습니다. 이러한 파일은 시스템에 필요한 파일이거나 보호가 필요하지 않은 파일일 수 있습니다.

중요:
관리자가 기본 파일 보호 정책을 활성화하기 전에 폴더를 생성해야 합니다.

1 관리자가 제공한 폴더 이름과 경로를 사용합니다.
   - Mac의 경우 **기본 설정 창 > 기본 파일 보호 제외**로 이동합니다. 생성할 폴더 이름과 경로가 여기에 표시됩니다.
2 .txt와 같이 암호화할 필요가 없는 확장자의 경우 지정된 확장자로 파일을 추가합니다. 필요한 경우, 사용자가 생성한 이름의 하위 폴더를 추가할 수 있습니다.

   노트:
   이전에 암호화된 확장자가 있는 파일이 있는 경우 해당 폴더에 파일을 배치하면 해독되지 않으며 암호화된 상태로 유지됩니다. 관리자가 다른 정책을 통해 생성할 수 있는 **보호되지 않은 문서** 폴더가 있는 경우, 기본 파일 보호 유형을 이 폴더에 배치하여 암호를 해독할 수 있습니다.
3 기본 파일 보호가 활성화된 후 네트워크 또는 외부 드라이브의 해당 확장자에 보호되지 않는 파일이 있는 경우 해당 파일을 제외 폴더로 복사할 수 있으며 이 파일은 암호화되지 않은 상태로 유지됩니다. 그렇지 않으면 파일이 암호화됩니다.

컴퓨터에 한 명 이상의 사용자가 있는 경우 현재 로그인한 사용자만 해당 폴더에 파일을 배치하고 스윕에서 제외할 수 있습니다. 다른 사용자가 해당 폴더에 저장한 모든 파일은 스윕되고 암호화됩니다.

Windows 또는 Mac에서 파일 확장명 제거

관리자가 파일 확장명을 제거하기로 결정할 수 있습니다. 이 경우에는 해당 파일 형식을 해독하기 위해 컴퓨터가 스윕됩니다.

- 암호화된 파일의 *속성* > *Dell Data Guardian* 탭이 더 이상 표시되지 않습니다.
- 파일 오버레이 아이콘(있었던 경우)이 더 이상 표시되지 않습니다.
- 해독을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 해당 확장명이 있는 파일이 계속 암호화되어 있는 경우 스윕 중에 열려 있었거나 파일 서버 또는 다른 위치에 저장되어 있었을 수 있습니다.

관리자에게 문의하여 해독되지 않는 해당 확장명이 있는 파일의 복구를 요청하십시오.

Office 애플리케이션

Office 애플리케이션을 사용하여 기본 파일 보호로 암호화된 파일을 열 수 있지만 컨텐츠는 읽기 전용입니다.

웹 포털

설정 > 정책에서 기본 파일 보호가 참으로 설정된 경우 관리자가 웹 포털에서 다운로드할 때 Data Guardian에서 암호화하는 비 Office 파일 형식을 추가했습니다. 관리자가 파일 형식을 알려줘야 합니다.

노트:
아직 지원되지 않는 파일 유형을 업로드하면 웹 포털에서 콘텐츠를 읽을 수 없습니다.

암호화되든 암호화되지 않은 파일 형식이든 비 Office 파일 형식을 업로드할 수 있습니다. 그러나 비 Office 파일을 다운로드하면 파일 확장명이 달라집니다.

비 Office 파일(예: .txt 또는 .png)	설명 다운로드
업로드하기 전에 암호화됨 예: Windows 또는 Mac에서 이미 암호화된 비 Office 파일.	웹 포털에서 다운로드할 경우 .txt 또는 .png와 같은 파일 확장명을 유지합니다.
암호화되지 않은 파일	웹 포털에서 다운로드할 때 파일 확장명은 관리자가 정책에 확장명을 추가했는지 여부에 따라 달라집니다. 하지만 파일은 암호화됩니다. 웹 포털에서 다운로드한 .txt 파일의 예: • **filename.txt** - 관리자가 .txt 파일 형식을 정책에 추가했습니다. • **filename.txt.xen** - .txt 파일 형식이 정책에 포함되지 않았습니다. 파일이 암호화되지만 .xen 확장명이 추가됩니다.

편집 정책이 웹 포털에 활성화되어 있는 경우 사용자는 비 Office 파일을 편집할 수 있습니다.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

변조 및 보호되는 Office 문서

Data Guardian은 보호된 Office 문서를 스캔하여 어떤 형태의 변조를 감지할 수 있습니다.

내부 사용자가 보호된 Office 문서를 변조할 경우 다음과 같습니다.

- Data Guardian이 일부 변조를 복구하거나 복원할 수 있습니다.
- 변조를 복구할 수 없는 경우에는 파일이 변조되었고 관리자에게 문의해야 한다는 메시지가 있는 대화 상자가 표시될 수 있습니다.

권한이 없는 사용자가 보호된 Office 문서를 열면 표지 페이지만 표시됩니다. 권한이 없는 사용자가 표지 페이지를 수정하는 경우, Data Guardian은 권한이 있는 사용자가 보호 대상으로 다시 저장한 시점으로 표지 페이지를 복원합니다.

Identifier	GUID-A8209D75-E380-4809-A55A-CF89E3FBE29A
Status	In Translation

클라우드에서 클라우드 동기화 폴더 및 파일 보기

컴퓨터에 동기화 클라이언트 폴더가 있고 Data Guardian이 폴더를 암호화한 경우 파일은 클라우드에서 암호화됩니다.

Data Guardian 웹 포털을 사용하여 파일을 암호화하는 경우 해당 파일은 .xen 파일로 암호화될 수 있습니다. Windows에서는 암호화된 .xen 파일을 열 수 없습니다. Data Guardian 또는 웹 포털을 통해 모바일 장치에서 이러한 파일을 볼 수 있습니다.

Identifier	GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508
Status	Translation Validated

외부 사용자와 보호된 Office 문서 공유

Data Guardian을 사용하면 이메일, 이동식 미디어, 네트워크 공유 등을 통해 보호된 Office 문서를 공유하거나 이를 클라우드에 업로드하고 공유할 수 있습니다.

- 모든 내부 Data Guardian 사용자가 해당 문서를 볼 수 있습니다.
- 정책에 따라 외부 사용자가 해당 문서를 볼 수 있습니다.

문서를 첨부하고 *전송*을 클릭할 때 확인 대화 상자가 열려 보호된 문서에 대한 키가 외부 사용자와 공유됨을 알립니다.

날짜 제한을 추가하여 보안을 향상

또한 선택적으로 외부 사용자에 대한 보안 강화를 위해 외부 사용자가 보호된 Office 문서를 볼 수 있는 시간을 제한하기 위한 날짜 제한을 추가할 수도 있습니다.

1 **파일 > 정보 > 날짜 제한**을 선택합니다.

2 드롭다운 메뉴에서 외부 사용자가 문서를 볼 수 있는 시작 및 종료 날짜와 시간을 선택합니다.

> **노트:**
> 문서는 보내지만 대상 날짜 및 시간이 될 때까지 외부 사용자가 문서를 보지 못하게 하려면 시작 날짜 및 시간은 미래가 될 수 있습니다.

3 **확인**을 클릭합니다.
문서가 저장되고, 보호되고, 닫힌 다음에 다시 열릴 것입니다.

> **노트:**
> 보호되지 않는 Office 문서에 대한 날짜를 수정한 다음에 취소를 클릭할 경우 Data Guardian은 계속 해당 파일을 보호합니다.

> **노트:**
> 현재 보호된 Office 문서에 날짜 제한을 추가한 다음에 네트워크 드라이브에 저장하려고 한다면 파일을 로컬에 저장한 다음에 네트워크에 복사해야 합니다.

외부 사용자가 날짜 및 시간 범위 이후에 파일을 열면 파일에 액세스 제한이 있으며 외부 사용자는 파일의 작성자에게 문의할 수 있다는 대화 상자가 표시됩니다. 대화 상자에는 외부 사용자에 대한 날짜는 표시되지 않습니다.

사용자가 *시작 날짜* 필드를 미래의 날짜나 시간으로 설정하고 외부 사용자가 이 시간이 되기 전에 파일을 열려고 하면 액세스 제한 때문에 해당 날짜 및 시간이 될 때까지 파일을 열 수 없다는 메시지가 표시됩니다.

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Mac에 Data Guardian 설치 및 사용

Mac용 Data Guardian에는 다음과 같은 내용을 설명하는 특정 화면에 대한 내장형 도움말이 있습니다.

- Dell Data Guardian 인터페이스로 사용자가 암호화하려는 파일을 업로드할 수 있습니다.
- 클라우드 암호화
- 외부 사용자 및 액세스 제한 사항
- 변조

Mac용 Dell Data Guardian 인터페이스에서 도움말 아이콘을 클릭합니다.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Mac용 클라이언트 설치

관리자가 사용자를 엔터프라이즈의 허용 목록에 추가한 경우 https://yoursecurityservername.domain.com:8443/cloudweb/register에서 등록할 수 있습니다.

등록 후 사용자는 로그인하여 해당 클라이언트를 다운로드하도록 https://yoursecurityservername.domain.com:8443/cloudweb으로 안내하는 이메일을 받습니다.

사용자는 로컬 관리자여야 합니다.

Mac용 Data Guardian 설치:

1 Data Guardian 클라이언트의 경우 **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg**에서 설치 프로그램을 찾습니다.
2 Dell-Data-Guardian-0.x.x.xxxx.dmg 내의 **.pkg** 파일을 사용하여 설치 또는 업그레이드합니다.
3 **Dell-Data-Guardian-x.x.x** 패키지를 두 번 클릭합니다.
4 **계속**을 클릭합니다.
5 소개 창에서 **계속**을 클릭합니다.
6 소프트웨어 라이센스 계약 창에서 **계속**을 클릭합니다.
7 계속하려면 **동의**를 클릭합니다.
8 구성 유형 창에서 다음 중 하나를 선택합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션. a **호스팅된 Dell 보안 센터**를 선택합니다. b **계속**을 클릭합니다. c 9단계를 계속 진행합니다.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버. a **사내 Dell Management Server**를 선택합니다. b *Dell Management Server 이름:* 필드에서 컴퓨터가 통신하는 Dell Server 이름(예: server.domain.com)을 입력합니다. www 또는 http(s)를 입력할 필요는 없습니다. 이 정보는 관리자가 제공합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
	c **계속**을 클릭합니다. d 9단계를 계속 진행합니다.

9 설치 유형 창에서 다음 중 하나를 수행합니다.
- **설치**를 클릭한 다음 10단계로 이동합니다.
- **설치 위치 변경**을 클릭합니다.
  1 대상 선택 창에서 모든 사용자를 선택합니다. 현재는 이 옵션만 선택할 수 있습니다.
  2 **계속**을 클릭합니다.
  3 **설치**를 클릭한 다음 10단계로 이동합니다.

10 대화 상자에서 사용자 이름 및 암호를 입력하고 **소프트웨어 설치**를 클릭합니다.

11 요약 창에 **닫기**를 클릭합니다.

12 메시지가 나타나면 .pkg 파일을 유지하거나 *휴지통*으로 이동합니다.

13 다음 중 하나를 수행합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
설치 후 자격 증명 창이 자동으로 열립니다. 엔터프라이즈가 멀티 테넌트인 경우 설치 ID가 필요합니다. 1 자격 증명 창에 로그인 계정 이메일을 입력하고 **계속**을 클릭합니다. 2 다음 중 하나를 수행합니다. • 엔터프라이즈가 멀티 테넌트인 경우 설치 ID를 입력하고 **계속**을 클릭하고 3단계로 계속합니다. **노트:** 오류가 표시되면 자격 증명을 확인하십시오. 잘못된 이메일 주소 또는 설치 ID가 있는 경우 **초기화 다시 시작**을 클릭하여 자격 증명을 다시 입력하십시오. • 단일 테넌트의 경우 3단계를 계속 진행합니다. 3 Microsoft 창에서 암호를 입력하고 **로그인**을 클릭합니다. 4 Azure 창에서 암호를 입력합니다. 5 **로그인**을 클릭합니다. **노트:** 오류가 표시되면 자격 증명을 확인하십시오. 잘못된 이메일 주소가 있는 경우 **초기화 다시 시작**을 클릭하여 자격 증명을 다시 입력하십시오. 6 Dell Data Guardian 인터페이스가 열립니다. Dell Data Guardian 애플리케이션을 참조하십시오.	1 Finder를 열려면 .dmg 창을 닫습니다. 2 최종 사용자 활성화를 참조하십시오.

노트:
엔터프라이즈가 Cloud Edition에서 Data Guardian으로 업그레이드하는 경우, 사용자는 Data Guardian을 인증하고 클라우드 스토리지 제공업체와 다시 연결해야 합니다. 인증에 대한 자세한 내용은 온라인 Data Guardian 도움말을 참조하십시오.

Identifier	GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC
Status	In Translation

최종 사용자 활성화(사내 환경)

사내 Dell Management Server에 대한 활성화

사내 환경에서 처음 Dell Data Guardian을 연 후에는 활성화를 위해 로그인을 해야 합니다.

1 Finder에서 **응용 프로그램**을 선택하고 **Dell Data Guardian**을 두 번 클릭합니다.
2 자격 증명 창이 열리면 Dell Server 주소(company.server.com)를 입력합니다. 이 정보는 관리자가 제공합니다. 기본 포트 번호는 8443입니다. 엔터프라이즈에서 기본 포트를 사용자 지정 포트 번호로 수정하는 경우, 관리자가 알려줄 것입니다.

> **노트:**
> 관리자가 지시하는 경우는 제외하고 SSL 오류 확인란을 선택하지 마십시오.

3 이메일 주소와 암호를 입력합니다.
4 **로그인**을 클릭하여 Data Guardian을 활성화합니다.
5 아래의 *Dell Data Guardian 애플리케이션*을 참조하십시오.

인증에 대한 자세한 내용은 온라인 Dell Data Guardian 도움말을 참조하십시오.

Dell Data Guardian 애플리케이션

Dell Data Guardian 응용 프로그램이 열리고 활성화되면 희미한 클라우드 저장소 제공업체 이름이 왼쪽 창에 활성화됩니다.

기업에서 모든 사용자가 동일한 클라우드 서비스를 사용하여 협업하기를 원한다면, 관리자는 해당 서비스만 활성화하고 다른 서비스가 표시되는 것을 차단하도록 정책을 설정할 수 있습니다.

Data Guardian에 대한 인증이 취소 또는 만료되면 클라우드 저장소 공급자 이름도 회색으로 표시됩니다.

1 왼쪽 창에서 클라우드 저장소 제공업체를 선택합니다.
2 자격 증명을 입력하라는 창이 열립니다. 자격 증명을 입력합니다.

인증되면 클라우드 저장소 제공업체 이름이 활성화됩니다.

Identifier	GUID-8882A835-A7A8-4C7B-8330-3080F871A121
Status	Translation Validated

호스팅된 Dell 보안 센터 및 일시 중지된 테넌트

호스팅된 Dell 보안 센터에서 테넌트가 지정된 기간 동안 지불하지 않는 경우 해당 테넌트를 일시 중지할 수 있습니다. (Windows, Mac, 모바일, 웹 포털에 적용됨)

Data Guardian 내부 및 외부 사용자는 다음을 경험할 수 있습니다.

- 모든 플랫폼 - Data Guardian을 설치하거나, 활성화하거나, 로그인하려고 하면 테넌트가 일시 중지되었다는 대화 상자가 표시됩니다.
- Mac - Data Guardian이 열려 있는 동안 테넌트가 일시 중지된 경우 탐색기 및 모든 파일을 닫은 후 보호된 파일을 열면 일시 중단된 테넌트 대화 상자가 표시됩니다.

- 웹 포털:
  - 이미 로그인한 상태에서 암호화된 파일을 업로드하면 업로드 실패 메시지가 표시됩니다.
  - 암호화되거나 암호화되지 않은 파일을 업로드한 후 테넌트가 일시 중지된 경우 다운로드 실패 메시지가 표시됩니다.
  - 로그아웃한 후 다시 로그인하려고 하면 테넌트가 일시 중지되었음을 나타내는 대화 상자가 표시됩니다.

관리자에게 문의하십시오.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

기본 파일 보호를 통한 추가 애플리케이션 및 파일 형식 보호

정책이 추가 애플리케이션 및 파일 형식의 암호화를 허용하는 경우 관리자가 알려줍니다. 누군가가 기본 파일 보호를 사용하여 암호화된 파일을 열었지만 Data Guardian이 설치되어 있지 않은 경우 컨텐츠를 읽을 수 없습니다.

기본 파일 보호의 개요

애플리케이션

다음은 관리자가 암호화를 원할 수 있는 애플리케이션의 예입니다.

- 메모장
- 워드패드
- Visio
- MS paint

> **노트:**
> 일부 애플리케이션은 부분적으로만 Data Guardian에서 지원되며 이는 관리자가 알려줍니다.

파일 유형

다음은 구성할 수 있는 추가 파일 형식의 예입니다: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac 및 모바일

기본 파일 보호 정책이 구성되어 있는 경우 Data Guardian은 사용자의 컴퓨터를 스윕하고 해당 확장자의 모든 로컬 파일을 암호화합니다. 기본 파일 보호를 사용하여 암호화된 파일은 파일 확장자와 관련된 애플리케이션만을 사용하여 편집하고 볼 수 있습니다.

> **노트:**
> AppData와 같이 특정 시스템 폴더에 있는 파일은 암호화되지 않습니다. Secure Documents 폴더와 같이 보호된 Office 문서와 관련된 폴더 또한 해당됩니다.

Windows의 오버레이 아이콘

Data Guardian 2.2 이상의 경우, 파일 탐색기의 보호된 파일에 오버레이 아이콘이 표시됩니다. 보호된 파일을 마우스 오른쪽 단추로 클릭하면 Dell Data Guardian 탭에 추가 정보가 표시됩니다.

Windows 또는 Mac의 스윕에서 일부 파일 제외(스윕이 활성화되기 전)

엔터프라이즈에서 .txt와 같은 추가 파일 형식을 암호화하기로 결정한 경우 해당 확장자를 가진 일부 파일을 스윕 및 암호화하고 싶지 않을 수 있습니다.

해당 확장자에 대한 기본 파일 보호를 활성화하기 전에 관리자가 폴더를 로컬 컴퓨터에 추가할 수 있는 다른 정책을 설정할 수 있으며 해당 폴더의 파일은 스윕되지 않습니다. 관리자는 정책을 설정하고, 폴더 이름을 생성하고, 폴더 이름을 제공하고, 해당 폴더를 추가할 수 있는 위치를 제안할 수 있습니다. 이러한 파일은 시스템에 필요한 파일이거나 보호가 필요하지 않은 파일일 수 있습니다.

중요:
관리자가 기본 파일 보호 정책을 활성화하기 전에 폴더를 생성해야 합니다.

1 관리자가 제공한 폴더 이름과 경로를 사용합니다.
   - Mac의 경우 **기본 설정 창 > 기본 파일 보호 제외**로 이동합니다. 생성할 폴더 이름과 경로가 여기에 표시됩니다.
2 .txt와 같이 암호화할 필요가 없는 확장자의 경우 지정된 확장자로 파일을 추가합니다. 필요한 경우, 사용자가 생성한 이름의 하위 폴더를 추가할 수 있습니다.

   노트:
   이전에 암호화된 확장자가 있는 파일이 있는 경우 해당 폴더에 파일을 배치하면 해독되지 않으며 암호화된 상태로 유지됩니다. 관리자가 다른 정책을 통해 생성할 수 있는 **보호되지 않은 문서** 폴더가 있는 경우, 기본 파일 보호 유형을 이 폴더에 배치하여 암호를 해독할 수 있습니다.
3 기본 파일 보호가 활성화된 후 네트워크 또는 외부 드라이브의 해당 확장자에 보호되지 않는 파일이 있는 경우 해당 파일을 제외 폴더로 복사할 수 있으며 이 파일은 암호화되지 않은 상태로 유지됩니다. 그렇지 않으면 파일이 암호화됩니다.

컴퓨터에 한 명 이상의 사용자가 있는 경우 현재 로그인한 사용자만 해당 폴더에 파일을 배치하고 스윕에서 제외할 수 있습니다. 다른 사용자가 해당 폴더에 저장한 모든 파일은 스윕되고 암호화됩니다.

Windows 또는 Mac에서 파일 확장명 제거

관리자가 파일 확장명을 제거하기로 결정할 수 있습니다. 이 경우에는 해당 파일 형식을 해독하기 위해 컴퓨터가 스윕됩니다.

- 암호화된 파일의 *속성 > Dell Data Guardian* 탭이 더 이상 표시되지 않습니다.
- 파일 오버레이 아이콘(있었던 경우)이 더 이상 표시되지 않습니다.
- 해독을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 해당 확장명이 있는 파일이 계속 암호화되어 있는 경우 스윕 중에 열려 있었거나 파일 서버 또는 다른 위치에 저장되어 있었을 수 있습니다.

관리자에게 문의하여 해독되지 않는 해당 확장명이 있는 파일의 복구를 요청하십시오.

Office 애플리케이션

Office 애플리케이션을 사용하여 기본 파일 보호로 암호화된 파일을 열 수 있지만 컨텐츠는 읽기 전용입니다.

웹 포털

설정 > 정책에서 기본 파일 보호가 참으로 설정된 경우 관리자가 웹 포털에서 다운로드할 때 Data Guardian에서 암호화하는 비 Office 파일 형식을 추가했습니다. 관리자가 파일 형식을 알려줘야 합니다.

노트:
아직 지원되지 않는 파일 유형을 업로드하면 웹 포털에서 콘텐츠를 읽을 수 없습니다.

암호화되든 암호화되지 않은 파일 형식이든 비 Office 파일 형식을 업로드할 수 있습니다. 그러나 비 Office 파일을 다운로드하면 파일 확장명이 달라집니다.

비 Office 파일(예: .txt 또는 .png)	설명 다운로드
업로드하기 전에 암호화됨	웹 포털에서 다운로드할 경우 .txt 또는 .png와 같은 파일 확장명을 유지합니다.

비 Office 파일(예: .txt 또는 .png)	설명 다운로드
예: Windows 또는 Mac에서 이미 암호화된 비 Office 파일.	
암호화되지 않은 파일	웹 포털에서 다운로드할 때 파일 확장명은 관리자가 정책에 확장명을 추가했는지 여부에 따라 달라집니다. 하지만 파일은 암호화됩니다. 웹 포털에서 다운로드한 .txt 파일의 예: • **filename.txt** - 관리자가 .txt 파일 형식을 정책에 추가했습니다. • **filename.txt.xen** - .txt 파일 형식이 정책에 포함되지 않았습니다. 파일이 암호화되지만 .xen 확장명이 추가됩니다.

편집 정책이 웹 포털에 활성화되어 있는 경우 사용자는 비 Office 파일을 편집할 수 있습니다.

Identifier	GUID-FC539BCB-1939-4E0A-8A36-
Status	Translation Validated

iOS 또는 Android에서 Data Guardian Mobile 설치 및 사용하기

이 절에서는 iOS 또는 Android 장치에서 Data Guardian Mobile을 사용하는 것에 관한 기본 정보를 설명합니다. 관리자가 Data Guardian을 사용하도록 정책을 설정하면 파일은 암호화되고 안전합니다. 암호화된 파일로 보거나 작업하려면 모바일 디바이스에 Data Guardian 앱이 설치되어 있어야 합니다.

Identifier	GUID-116F412E-15BE-4E29-A886-5A308BA693ED
Status	Translated

사전 요구 사항

Data Guardian 앱을 사용하기 전에 사용자 환경에 맞게 필요한 사항을 결정합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 환경이 멀티 테넌트인 경우 설치 ID가 필요합니다.	반드시 Dell Server의 이름(server.domain.com)을 알고 있어야 합니다. 이 정보는 관리자가 제공합니다.

Identifier	GUID-A802F8F9-1B8F-47DD-8525-518A4C004221
Status	Translation Validated

Data Guardian 모바일 시작하기

이 순서에 따라 Data Guardian 모바일을 사용합니다.

작업	설명	참조 섹션
Data Guardian 설치 - 옵션 결정:	관리자가 이미 설치함	관리자 설치: Data Guardian 앱을 누르고 로그인을 합니다.
	사용자가 설치해야 함	사용자 설치: 다음 섹션 중 하나 참조: • iOS 장치에 설치 • Android 장치에 설치
모바일에 적용될 정책 결정	관리자가 적용되는 정책을 알려줍니다.	다음과 같이 나타날 수 있습니다. • 보호된 Office 문서 • 클라우드 보호 • 추가 옵션

작업	설명	참조 섹션
파일 관리자에서 탐색	Data Guardian 옵션을 참조하십시오.	파일 관리자에서 탐색
클라우드 보호 정책이 활성화되어 있는 경우, 클라우드 스토리지 공급자 계정에 액세스합니다.	해당 장치에서 Data Guardian 앱의 파일 관리자 화면으로 이동하고 클라우드 스토리지 서비스를 누릅니다.	클라우드 스토리지 공급자 계정에 액세스를 참조하십시오.

Data Guardian 정책에 따라 다음과 같이 나타날 수 있습니다.

- 보호된 Office 파일(.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf)은 파일 확장명을 유지합니다.
- .txt와 같은 애플리케이션 및 파일 형식
- 클라우드에서 비 Office 파일의 확장명은 .xen입니다.

Data Guardian이 설치된 모바일 디바이스에서 다음과 같은 작업을 수행할 수 있습니다.

- 폴더 및 파일 생성
- 폴더 및 파일 삭제
- 외부 사용자와 문서 공유(외부 사용자에 대해 정책이 활성화된 경우)

Identifier	GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3
Status	In Translation

App Store를 통해 iOS 장치에서 Data Guardian 설치 또는 제거

iOS 장치에 설치

사전 요구 사항: 장치에서 Touch ID 지문 스캐너를 지원하고 PIN 대신 이를 사용하려는 경우 Data Guardian을 설치하기 전에 Touch ID에 대해 장치를 구성해야 합니다.

1 장치에서 **App Store**를 누르고 **Data Guardian Mobile**을 검색합니다.
2 **Data Guardian** 앱을 선택하고 설치합니다.
3 라이센스 계약에 동의하려면 확인란을 가볍게 누릅니다.
4 다음 옵션 중 하나를 선택합니다.

호스팅된 Dell 보안 센터	사내
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션. a **호스팅된 Dell 보안 센터**를 누릅니다. b 이메일을 입력합니다. c **제출**을 누릅니다. **노트:** 이메일 주소가 두 개 이상의 테넌트에 있는 경우 설치 ID를 입력합니다. d Microsoft Azure 창에서 암호를 입력합니다. e **로그인**을 누릅니다.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버. a **사내**을 누릅니다. b 로그인 화면의 서버 필드에 회사 Dell Server의 이름을 입력합니다(예: server.domain.com). c 사용자 이름과 암호를 입력합니다. d **로그인**을 누릅니다.

5 메시지가 표시되면 지문 센서를 탭하거나 PIN을 생성합니다.

이제 계정이 활성화되었으며 Data Guardian 파일 관리자 화면이 표시됩니다.

Data Guardian 앱 설치 제거

1 iOS Apps 창에서 **Data Guardian** 아이콘을 길게 누릅니다.
2 **x**를 누릅니다.
3 **삭제**를 누릅니다.

Identifier	GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4
Status	In Translation

Workspace ONE으로 iOS 장치에서 Data Guardian 설치 또는 제거

Workspace ONE이 설치되어 있는 경우 SSO(Single Sign-On)를 사용하여 Data Guardian을 인증할 수 있습니다. 다음 단계는 호스팅된 Dell 보안 센터 또는 사내 Dell Management Server에 동일하게 적용됩니다.

관리자가 Data Guardian 앱을 장치로 내보냅니다.

1 **Data Guardian** 앱 설치 여부를 묻는 메시지가 표시되면 **확인**을 누릅니다.
2 **Data Guardian** 앱을 실행합니다.
3 라이센스 계약에서 **허용**을 누릅니다.
4 Workspace ONE 또는 Data Guardian을 선택한 다음 **Workspace ONE**을 눌러 SSO(Single Sign-On)를 사용합니다.
5 암호를 입력합니다.
6 메시지가 표시되면 PIN을 생성합니다.

> **노트:**
> Workspace ONE에 로그인하는 경우 Data Guardian에 대한 PIN만 입력하면 됩니다.

이제 계정이 활성화되었으며 Data Guardian 파일 관리자 화면이 표시됩니다.

Identifier	GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046
Status	In Translation

Google Play를 통해 Android 장치에서 Data Guardian 설치 또는 제거

Android 장치에 설치

1 자신의 장치에서 Google Play에 액세스한 다음에 Data Guardian **Mobile**을 검색합니다.
2 **Data Guardian** 앱을 선택하고 설치합니다.
3 라이센스 계약에 동의하려면 확인란을 가볍게 누릅니다.
4 다음 옵션 중 하나를 선택합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션. a **호스팅된**을 누릅니다. b 이메일을 입력합니다. c **제출**을 누릅니다.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버. a **사내**을 누릅니다. b 로그인 화면의 서버 필드에 회사 Dell Server의 이름을 입력합니다(예: server.domain.com). c 사용자 이름과 암호를 입력합니다. d **로그인**을 누릅니다.

노트:
이메일 주소가 두 개 이상의 테넌트에 있는 경우 설치 ID를 입력합니다.

d Microsoft Azure 창에서 암호를 입력합니다.
e **로그인**을 누릅니다.

5 메시지가 표시되면 PIN을 생성합니다.

이제 계정이 활성화되었으며 Data Guardian 파일 관리자 화면이 표시됩니다.

Data Guardian 앱 설치 제거

1 Android Apps 창에서 **설정**을 누릅니다.
2 **설정**에서 **앱**을 누릅니다.
3 **Data Guardian** 아이콘을 길게 누릅니다.
4 아이콘을 설치 제거 옵션으로 끌어 놓습니다.
5 **확인**을 누릅니다.

Identifier	GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814
Status	In Translation

Workspace ONE으로 Android 장치에서 Data Guardian 설치 또는 제거

Workspace ONE이 설치되어 있는 경우 SSO(Single Sign-On)를 사용하여 Data Guardian을 인증할 수 있습니다. 다음 단계는 호스팅된 Dell 보안 센터 또는 사내 Dell Management Server에 동일하게 적용됩니다.

1 장치에서 **허브**를 누릅니다.
2 **앱 카탈로그**를 누릅니다.
3 Dell Data Guardian에서 **설치**를 누릅니다.
4 *설치 확인*에서 **설치**를 누릅니다.
5 *Google Play Protect*에서 **허용**을 누릅니다.
6 앱 설치 완료 메시지에서 **완료**를 누릅니다.
7 **열기**를 눌러 Data Guardian 앱을 실행합니다.
8 Workspace ONE 또는 Data Guardian을 인증한 다음 **Workspace ONE**을 눌러 SSO(Single Sign-On)를 사용합니다.
9 라이센스 계약에서 확인란을 누릅니다.
10 **SSO(Single Sign On)**를 누릅니다.
11 메시지가 표시되면 PIN을 생성합니다.

노트:
Workspace ONE에 로그인하는 경우 Data Guardian에 대한 PIN만 입력하면 됩니다.

이제 계정이 활성화되었으며 Data Guardian 파일 관리자 화면이 표시됩니다.

Data Guardian 앱 설치 제거

1 Android Apps 창에서 **설정**을 누릅니다.
2 **설정**에서 **앱**을 누릅니다.
3 **Data Guardian** 아이콘을 길게 누릅니다.
4 아이콘을 설치 제거 옵션으로 끌어 놓습니다.

5 **확인**을 누릅니다.

Identifier	GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8
Status	In Translation

파일 관리자 탐색

Data Guardian의 파일 관리자에서 로컬 스토리지 또는 클라우드를 사용할 수 있습니다. Data Guardian을 열면 파일 관리자가 열립니다.

파일 관리자 화면

파일 관리자 화면의 기본 폴더는 다음을 포함합니다.

- 문서
- 다운로드
- 사진

새로 생성 화면

추가(+) 아이콘을 누르면 *새로 생성* 화면에서 다음과 같은 옵션이 표시됩니다.

- 설명서
- 스프레드시트
- 프레젠테이션(PowerPoint)
- 사진
- 폴더
- 클라우드 서비스

탐색 창 옵션

탐색 창 아이콘을 누릅니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **브라우저**
- **파일 관리자**
- **설정** 아이콘:
  - **PIN 변경** 단추(정책으로 활성화된 경우)
  - **브라우저**
  - **파일 관리자(설정)** - 다음 옵션 사용
    - **새로 고침 간격** - Data Guardian이 클라우드 서비스를 동기화하는 빈도입니다. Dell은 *수동* 또는 *매일*을 선택할 것을 권장합니다. 기타 옵션으로는 *1시간* 또는 *주* 단위를 선택할 수 있습니다.
    - **10MB 다운로드 경고** - 활성화하거나 비활성화하십시오. Wi-Fi에 연결되어 있지 않고 다운로드 크기가 10MB를 초과하면 이 옵션을 사용하십시오.
    - **캐시 지우기** - 임시 파일을 지웁니다.
  - (iOS) - iOS 버전에 따라, 지문이나 얼굴 인식을 사전 구성한 경우 **Touch ID** 또는 **Face ID**를 사용합니다. Data Guardian을 사용할 때 탭하여 활성화하거나 비활성화합니다.
  - **정보** - Data Guardian 정책 및 버전 보기
  - **Data Guardian 종료** 단추

  - **클라우드 계정** - 연결 여부를 나타냅니다.
- **브라우저**
- **파일 관리자** - 파일 관리자 화면으로 돌아갑니다.
- **Data Guardian 잠금**

추가 옵션

- 즐겨찾기에 파일 추가
  - iOS의 경우 탐색 창을 참조하십시오.
  - Android의 경우 파일 이름을 길게 누르십시오.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Data Guardian Mobile을 위한 정책 결정

관리자가 엔터프라이즈에 설정된 정책에 대해 알려줄 것입니다.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Data Guardian 정책 및 버전 보기

일부 Data Guardian 정책은 **정보**에 나와 있습니다. 이러한 정책 또는 Data Guardian 버전을 보려면

1 Data Guardian 탐색 창에서 **설정 > 정보**를 누릅니다.
2 **정책**을 누릅니다.
관리자가 설정한 정책에 따라 다음과 같은 항목이 목록에 표시됩니다.
  - 암호 길이
  - 비활성 시간 초과
  - 로그인 실패
  - 복사 및 붙여넣기 - 보호된 문서를 보호된 문서로 복사할 수 있습니다.

  버전
3 추가 정책 옵션을 결정합니다.
이러한 항목은 다음과 같습니다.
  - 보호된 Office 문서
  - 클라우드 보호
  - 추가 정책

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

모바일에서 보호된 Office 문서 사용하기

관리자가 엔터프라이즈에 활성화된 옵션을 알려줄 것입니다. Data Guardian이 설치된 상태에서 보호된 Office 문서를 열면 문서의 암호 해독 중이라는 메시지가 표시됩니다.

Office 문서를 위한 Data Guardian 옵션

다음과 같은 Data Guardian 옵션이 표시됩니다.

- **생성** - 정책 설정에 따라 문서 생성시 보호됩니다. 이 파일의 헤더에는 *보호된 문서*가 표시됩니다.
- **복사/붙여넣기** - 보호된 Office 문서는 다른 보호된 Office 문서로만 복사할 수 있습니다.
- **인쇄** - 추가 정책 설정에 따라 인쇄할 때 워터마크가 표시될 수 있습니다.
- **내보내기** - 추가 정책 설정에 따라 내보내기할 때 워터마크가 표시될 수 있습니다.

Office 문서가 열려 있는 경우 좌측 상단의 아이콘을 눌러 다음의 옵션을 표시합니다.

- **저장**
- **다른 이름으로 저장**
- **내보내기**
- **관리되는 파일이 열린 상태에서**

정책에 따른 추가 Office 옵션은 다음과 같습니다.

- **편집** - .docx 및 .ppt Office 파일을 편집할 수 있습니다.

  노트:
  현재 .csv 및 .csv.xen 파일은 모바일 장치에서 편집할 수 없습니다.

- **숨겨진 워터마크** - 정책에 따라 보호된 Office 문서에 사용자를 식별하는 숨겨진 워터마크가 표시될 수 있습니다. 문서를 인쇄 또는 공유하는 경우, 워터마크가 유지됩니다.
- **온스크린 워터마크** - 보호된 보호된 Office 문서를 여는 경우 클라이언트 화면에 워터마크가 표시됩니다.

Office 문서를 위한 추가 정보

오프라인일 때의 보호된 Office 문서

보호된 Office 문서 또는 매크로가 활성화된 보호된 문서를 만들었는데 오프라인인 경우에는 해당 문서에 대한 키가 생성됩니다. 장치가 온라인이 되면 키가 Dell Server로 업로드됩니다. 장치의 오프라인 상태가 3일 동안 계속되면 Data Guardian이 Dell Server에 접속할 수 없었다는 알림이 나타납니다. 이 알림은 사용자가 네트워크에 연결할 때까지 매일 표시됩니다. 암호화된 파일을 보려면 모바일 장치가 온라인이어야 합니다.

보호된 Office 문서 문제 해결

iOS 장치에서 25MB보다 큰 보호된 Office 문서를 열고 메모리 부족 대화 상자가 표시되면 Data Guardian이 아니라 Polaris Office에서 경고가 표시됩니다. 장치의 메모리가 충분하면 파일을 닫고 다시 여십시오.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

기본 파일 보호를 통한 추가 애플리케이션 및 파일 형식 보호

정책이 추가 애플리케이션 및 파일 형식의 암호화를 허용하는 경우 관리자가 알려줍니다. 누군가가 기본 파일 보호를 사용하여 암호화된 파일을 열었지만 Data Guardian이 설치되어 있지 않은 경우 컨텐츠를 읽을 수 없습니다.

기본 파일 보호의 개요

애플리케이션

다음은 관리자가 암호화를 원할 수 있는 애플리케이션의 예입니다.

- 메모장
- 워드패드
- Visio
- MS paint

> **노트:**
> 일부 애플리케이션은 부분적으로만 Data Guardian에서 지원되며 이는 관리자가 알려줍니다.

파일 유형

다음은 구성할 수 있는 추가 파일 형식의 예입니다: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac 및 모바일

기본 파일 보호 정책이 구성되어 있는 경우 Data Guardian은 사용자의 컴퓨터를 스윕하고 해당 확장자의 모든 로컬 파일을 암호화합니다. 기본 파일 보호를 사용하여 암호화된 파일은 파일 확장자와 관련된 애플리케이션만을 사용하여 편집하고 볼 수 있습니다.

> **노트:**
> AppData와 같이 특정 시스템 폴더에 있는 파일은 암호화되지 않습니다. Secure Documents 폴더와 같이 보호된 Office 문서와 관련된 폴더 또한 해당됩니다.

Windows의 오버레이 아이콘

Data Guardian 2.2 이상의 경우, 파일 탐색기의 보호된 파일에 오버레이 아이콘이 표시됩니다. 보호된 파일을 마우스 오른쪽 단추로 클릭하면 Dell Data Guardian 탭에 추가 정보가 표시됩니다.

Windows 또는 Mac의 스윕에서 일부 파일 제외(스윕이 활성화되기 전)

엔터프라이즈에서 .txt와 같은 추가 파일 형식을 암호화하기로 결정한 경우 해당 확장자를 가진 일부 파일을 스윕 및 암호화하고 싶지 않을 수 있습니다.

해당 확장자에 대한 기본 파일 보호를 활성화하기 전에 관리자가 폴더를 로컬 컴퓨터에 추가할 수 있는 다른 정책을 설정할 수 있으며 해당 폴더의 파일은 스윕되지 않습니다. 관리자는 정책을 설정하고, 폴더 이름을 생성하고, 폴더 이름을 제공하고, 해당 폴더를 추가할 수 있는 위치를 제안할 수 있습니다. 이러한 파일은 시스템에 필요한 파일이거나 보호가 필요하지 않은 파일일 수 있습니다.

> **중요:**
> 관리자가 기본 파일 보호 정책을 활성화하기 전에 폴더를 생성해야 합니다.

1 관리자가 제공한 폴더 이름과 경로를 사용합니다.
   - Mac의 경우 **기본 설정 창 > 기본 파일 보호 제외**로 이동합니다. 생성할 폴더 이름과 경로가 여기에 표시됩니다.
2 .txt와 같이 암호화할 필요가 없는 확장자의 경우 지정된 확장자로 파일을 추가합니다. 필요한 경우, 사용자가 생성한 이름의 하위 폴더를 추가할 수 있습니다.

노트:
이전에 암호화된 확장자가 있는 파일이 있는 경우 해당 폴더에 파일을 배치하면 해독되지 않으며 암호화된 상태로 유지됩니다. 관리자가 다른 정책을 통해 생성할 수 있는 **보호되지 않은 문서** 폴더가 있는 경우, 기본 파일 보호 유형을 이 폴더에 배치하여 암호를 해독할 수 있습니다.

3 기본 파일 보호가 활성화된 후 네트워크 또는 외부 드라이브의 해당 확장자에 보호되지 않는 파일이 있는 경우 해당 파일을 제외 폴더로 복사할 수 있으며 이 파일은 암호화되지 않은 상태로 유지됩니다. 그렇지 않으면 파일이 암호화됩니다.

컴퓨터에 한 명 이상의 사용자가 있는 경우 현재 로그인한 사용자만 해당 폴더에 파일을 배치하고 스윕에서 제외할 수 있습니다. 다른 사용자가 해당 폴더에 저장한 모든 파일은 스윕되고 암호화됩니다.

Windows 또는 Mac에서 파일 확장명 제거

관리자가 파일 확장명을 제거하기로 결정할 수 있습니다. 이 경우에는 해당 파일 형식을 해독하기 위해 컴퓨터가 스윕됩니다.

- 암호화된 파일의 *속성* > *Dell Data Guardian* 탭이 더 이상 표시되지 않습니다.
- 파일 오버레이 아이콘(있었던 경우)이 더 이상 표시되지 않습니다.
- 해독을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 해당 확장명이 있는 파일이 계속 암호화되어 있는 경우 스윕 중에 열려 있었거나 파일 서버 또는 다른 위치에 저장되어 있었을 수 있습니다.

관리자에게 문의하여 해독되지 않는 해당 확장명이 있는 파일의 복구를 요청하십시오.

Office 애플리케이션

Office 애플리케이션을 사용하여 기본 파일 보호로 암호화된 파일을 열 수 있지만 컨텐츠는 읽기 전용입니다.

웹 포털

설정 > 정책에서 기본 파일 보호가 참으로 설정된 경우 관리자가 웹 포털에서 다운로드할 때 Data Guardian에서 암호화하는 비 Office 파일 형식을 추가했습니다. 관리자가 파일 형식을 알려줘야 합니다.

노트:
아직 지원되지 않는 파일 유형을 업로드하면 웹 포털에서 콘텐츠를 읽을 수 없습니다.

암호화되든 암호화되지 않은 파일 형식이든 비 Office 파일 형식을 업로드할 수 있습니다. 그러나 비 Office 파일을 다운로드하면 파일 확장명이 달라집니다.

비 Office 파일(예: .txt 또는 .png)	설명 다운로드
업로드하기 전에 암호화됨 예: Windows 또는 Mac에서 이미 암호화된 비 Office 파일.	웹 포털에서 다운로드할 경우 .txt 또는 .png와 같은 파일 확장명을 유지합니다.
암호화되지 않은 파일	웹 포털에서 다운로드할 때 파일 확장명은 관리자가 정책에 확장명을 추가했는지 여부에 따라 달라집니다. 하지만 파일은 암호화됩니다. 웹 포털에서 다운로드한 .txt 파일의 예: • **filename.txt** - 관리자가 .txt 파일 형식을 정책에 추가했습니다. • **filename.txt.xen** - .txt 파일 형식이 정책에 포함되지 않았습니다. 파일이 암호화되지만 .xen 확장명이 추가됩니다.

편집 정책이 웹 포털에 활성화되어 있는 경우 사용자는 비 Office 파일을 편집할 수 있습니다.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

모바일에서 클라우드 보호 사용하기

관리자가 클라우드 보호를 사용하는 경우 2개의 앱이 필요합니다.

- 클라우드 동기화 클라이언트 앱 - 클라우드 동기화 클라이언트에 해당하는 온라인 도움말을 참조하십시오.
- Data Guardian 모바일 앱에 귀사에서 사용되는 클라우드 동기화 클라이언트가 나열되며 다운로드를 할 수도 있습니다.

승인 받지 않은 사람이 다른 사용자의 클라우드 스토리지 계정에 액세스하여 Data Guardian이 설치되어 있지 **않은** 모바일 장치에 파일을 다운로드해도 파일을 열거나 볼 수 없습니다. 보호된 Office 문서를 열면 Data Guardian 없이는 문서를 볼 수 없다는 것을 나타내는 표지 페이지만 표시됩니다. 따라서 데이터의 보안이 강화됩니다.

클라우드 스토리지 공급자 계정에 액세스

클라우드 스토리지 공급자 계정에 액세스하려면

1 파일 관리자 화면에서 추가(**+**) 아이콘을 누릅니다.

2 **클라우드 서비스**를 누릅니다.

Data Guardian 정책에 따라 클라우드 스토리지 서비스에 표시되는 항목이 결정됩니다. 관리자가 회사 내에서 사용되는 특정 클라우드 스토리지 서비스를 하나 이상 지정하고 다른 항목은 차단할 수 있습니다.

3 온라인 화면 지침에 따라 다음 중 하나를 수행합니다.

- 클라우드 스토리지 서비스를 사용하여 계정을 만듭니다.
- 기존 클라우드 스토리지 서비스 계정에 로그인합니다.

> **노트:**
> 자세한 내용은 클라우드 스토리지 서비스 도움말을 참조하십시오.

> **노트:**
> 클라우드 동기화 클라이언트 앱을 장치에 다운로드하면 Data Guardian은 해당 앱에서 직접 업로드하는 폴더나 파일을 암호화하지 않습니다. 파일을 암호화하고 보호하려면 Data Guardian 앱을 사용하여 업로드해야 합니다.

클라우드 보호 사용

Data Guardian이 설치된 모바일 디바이스에서 다음과 같은 작업을 수행할 수 있습니다.

- 폴더 생성
- 파일 업로드 및 다운로드

> **노트:**
> Data Guardian을 이용하여 해당 장치에서 업로드와 다운로드를 시작해야 합니다. 클라우드에 업로드할 때 암호화하는 파일은 클라우드 동기화 클라이언트 앱이 아닌 Data Guardian 홈 화면에서 업로드해야 합니다. 파일을 누르면 Data Guardian이 자동으로 파일의 암호를 해독하고 앱 내에서 일반 텍스트로 표시합니다. 하지만 클라우드에서는 .xen 파일로 표시되어 보호됩니다.

- 폴더 및 파일 삭제
- 내부 사용자로부터 공유 폴더 수락

노트:
Data Guardian을 통해 내부 사용자와 폴더를 공유하는 경우에는 클라우드 스토리지 웹사이트로 가서 해당 폴더를 루트 폴더로 이동시키거나 공유된 폴더를 다운로드해야 장치에서 볼 수 있습니다.

- **파일 > 복사** - 관리자가 설정한 정책에 따라 클라우드 서비스의 파일을 다른 클라우드 서비스로 복사할 수 있습니다.
- OneDrive 또는 Dropbox를 사용하는 Android의 경우에 애플리케이션에서 파일을 공유할 수 없고 해당 파일이 Data Guardian 앱과 링크를 공유한다면 장치의 파일 브라우저 앱에서 파일을 공유합니다.

클라우드 스토리지 서비스 연결 해제

동일한 클라우드 스토리지 서비스에 여러 개의 계정을 사용하는 경우 서비스와 계정에서 동시에 로그인 상태를 유지할 수 없습니다. 연결을 해제할 확인란을 선택 해제하고 현재 계정에서 로그아웃한 후에 다른 자격 증명을 사용하여 로그인해야 합니다.

1 Data Guardian 탐색 창을 열고 **설정 > 파일 관리자 > 클라우드 서비스**를 누릅니다. 클라우드 스토리지 서비스에 대한 액세스를 허용하면 확인란에 체크 표시가 나타납니다.

2 다음 중 하나를 수행합니다.

Android

a **연결됨**을 누릅니다.

b **예**를 누릅니다.

iOS

a **연결 해제됨**을 누릅니다.

이렇게 하면 Data Guardian 액세스 및 파일이 제거됩니다. 그러나 클라우드의 파일은 제거되지 않습니다.

클라우드 보호 문제 해결

Dropbox for Business에서 한 파일을 오프라인으로 사용 가능으로 표시한 다음에 Dropbox 웹 사이트에서 파일의 이름을 변경할 경우, 해당 파일은 Data Guardian 앱을 사용하는 iOS 장치에서 열리지 않습니다.

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

모바일에서 추가 정책 사용하기

엔터프라이즈에 대해 어떤 정책이 설정되었는지 관리자가 알려줄 것입니다.

PIN 사용

관리자는 PIN과 길이 설정을 요구하는 정책을 설정할 수 있습니다.

변조

Data Guardian은 보호된 Office 문서를 스캔하여 어떤 형태의 변조를 감지할 수 있습니다.

지오펜스를 통한 추가 보호

관리자가 정한 정책을 기준으로 모바일 장치에서 해당 보호된 Office 문서에 대한 추가 보호를 하게 만들고 .xen 파일을 특정 지역 외부에서 열 수 없게 만들 수 있습니다. 보호된 파일을 열려면 승인된 지역에 있어야 합니다. 현재 해당되는 지역은 미국과 캐나다입니다. 지오펜스가 작동하게 하려면 장치에서 지오펜스를 활성화시켜야 합니다. 관리자가 지오펜스 기능을 활성화하였지만 위치 서비스가 해제(Off)로 설정되어 있는 경우에는 파일 액세스가 거부됩니다.

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

Data Guardian 및 동기화 클라이언트에 관한 보안 고려 사항

Data Guardian은 데이터를 안전하게 만들기 위해 폴더와 파일을 암호화합니다. Data Guardian은 동기화 클라이언트와 함께 작동하기 때문에 이러한 고려 사항을 알아야 합니다.

Google Drive

Google Drive에는 사용자가 실시간으로 문서를 공동 작업할 수 있는 Google Docs 앱이 포함되어 있습니다. 하지만 공동 작업은 Dell Server가 아닌 Google 서버에서 수행됩니다. 따라서 파일이 암호화되지 않습니다. Data Guardian을 사용하는 Android 및 iOS 장치에서는 이러한 Google Docs에 대한 액세스가 차단됩니다. 이는 플랫폼에 따라 약간 다릅니다.

- Android
- iOS - 메시지가 표시됩니다.

노트:
*Google 백업 및 동기화*가 지원되지 않습니다.

OneDrive 및 OneDrive for Business

OneDrive for Business를 사용하는 경우, 여러 개의 파일이 다운로드되고 동안 다운로드 작업을 취소하면 OneDrive for Business는 다운로드되지 않은 파일을 취소하지만 다운로드가 진행되고 있는 파일은 계속 다운로드합니다. 이는 Microsoft 관련 문제입니다. 따라서 취소하기 전에 파일 다운로드가 완전히 완료될 때까지 기다리십시오.

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

로그

보안 상의 이유로, 모바일 장치에서 로그 파일을 사용할 수 없습니다.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

호스팅된 Dell 보안 센터 및 일시 중지된 테넌트

호스팅된 Dell 보안 센터에서 테넌트가 지정된 기간 동안 지불하지 않는 경우 해당 테넌트를 일시 중지할 수 있습니다. (Windows, Mac, 모바일, 웹 포털에 적용됨)

Data Guardian 내부 및 외부 사용자는 다음을 경험할 수 있습니다.

- 모든 플랫폼 - Data Guardian을 설치하거나, 활성화하거나, 로그인하려고 하면 테넌트가 일시 중지되었다는 대화 상자가 표시됩니다.
- Mac - Data Guardian이 열려 있는 동안 테넌트가 일시 중지된 경우 탐색기 및 모든 파일을 닫은 후 보호된 파일을 열면 일시 중단된 테넌트 대화 상자가 표시됩니다.
- 웹 포털:
  - 이미 로그인한 상태에서 암호화된 파일을 업로드하면 업로드 실패 메시지가 표시됩니다.

- 암호화되거나 암호화되지 않은 파일을 업로드한 후 테넌트가 일시 중지된 경우 다운로드 실패 메시지가 표시됩니다.
- 로그아웃한 후 다시 로그인하려고 하면 테넌트가 일시 중지되었음을 나타내는 대화 상자가 표시됩니다.

관리자에게 문의하십시오.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

Dell에 피드백 보내기

관리자가 피드백 정책을 사용하도록 설정한 경우에는 사용자가 이 제품에 대한 의견을 Dell에 보낼 수 있습니다. 정책을 통해 이 기능이 사용되도록 설정되지 않으면 옵션이 표시되지 않습니다.

피드백을 보내려면 다음을 수행합니다.

1 Data Guardian 탐색 창에서 **피드백**을 누릅니다.
2 간단한 질문에 응답하여 만족도(10은 최고 만족도)를 평가하고 의견을 입력합니다.

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	In Translation

웹 클라이언트에서 보호된 파일 보기 또는 편집하기

관리자가 Data Guardian 웹 포털을 설정한 경우 해당 웹 클라이언트에 대한 URL에 연결하여 Data Guardian 클라이언트를 설치하지 않고 암호화된 파일을 볼 수 있습니다. 정책에 따라 파일을 편집할 수도 있습니다.

관리자에 의해 설정된 정책에 따라 다음을 볼 수 있습니다.

- 보호된 Office 문서: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf
- .xen 파일 - 클라우드에 업로드할 때 Data Guardian이 암호화한 Office 또는 비 Office 파일입니다.
- 메모장과 같은 추가 파일 형식

관리자가 설정한 정책에 따라 클라우드 스토리지 제공업체에 액세스할 수 있습니다.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Data Guardian용 웹 포털에 액세스

사용하는 브라우저에 따라 단계가 조금 달라질 수 있습니다.

1 관리자로부터 웹 포털에 액세스하기 위한 URL을 가져옵니다.
2 URL을 클릭합니다.
경고가 뜨는 경우 **계속** 또는 **진행**을 클릭합니다.
3 사용권 계약 화면에서 **동의**를 클릭합니다.
경고가 뜨는 경우 **계속** 또는 **진행**을 클릭합니다.
4 도메인 자격 증명을 입력합니다.
5 **로그인**을 클릭합니다.
6 위치 추적을 허용하는지 묻는 메시지가 나타나면 옵션을 선택합니다.
7 파일을 보거나 편집하려면 Data Guardian 웹 포털에서 사용 가능한 온라인 도움말을 참조하십시오.

노트:
Mac의 경우 Safari에서 팝업을 허용하도록 구성해야 합니다.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

기본 파일 보호를 통한 추가 애플리케이션 및 파일 형식 보호

정책이 추가 애플리케이션 및 파일 형식의 암호화를 허용하는 경우 관리자가 알려줍니다. 누군가가 기본 파일 보호를 사용하여 암호화된 파일을 열었지만 Data Guardian이 설치되어 있지 않은 경우 컨텐츠를 읽을 수 없습니다.

기본 파일 보호의 개요

애플리케이션

다음은 관리자가 암호화를 원할 수 있는 애플리케이션의 예입니다.

- 메모장
- 워드패드
- Visio
- MS paint

> **노트:**
> 일부 애플리케이션은 부분적으로만 Data Guardian에서 지원되며 이는 관리자가 알려줍니다.

파일 유형

다음은 구성할 수 있는 추가 파일 형식의 예입니다: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac 및 모바일

기본 파일 보호 정책이 구성되어 있는 경우 Data Guardian은 사용자의 컴퓨터를 스윕하고 해당 확장자의 모든 로컬 파일을 암호화합니다. 기본 파일 보호를 사용하여 암호화된 파일은 파일 확장자와 관련된 애플리케이션만을 사용하여 편집하고 볼 수 있습니다.

> **노트:**
> AppData와 같이 특정 시스템 폴더에 있는 파일은 암호화되지 않습니다. Secure Documents 폴더와 같이 보호된 Office 문서와 관련된 폴더 또한 해당됩니다.

Windows의 오버레이 아이콘

Data Guardian 2.2 이상의 경우, 파일 탐색기의 보호된 파일에 오버레이 아이콘이 표시됩니다. 보호된 파일을 마우스 오른쪽 단추로 클릭하면 Dell Data Guardian 탭에 추가 정보가 표시됩니다.

Windows 또는 Mac의 스윕에서 일부 파일 제외(스윕이 활성화되기 전)

엔터프라이즈에서 .txt와 같은 추가 파일 형식을 암호화하기로 결정한 경우 해당 확장자를 가진 일부 파일을 스윕 및 암호화하고 싶지 않을 수 있습니다.

해당 확장자에 대한 기본 파일 보호를 활성화하기 전에 관리자가 폴더를 로컬 컴퓨터에 추가할 수 있는 다른 정책을 설정할 수 있으며 해당 폴더의 파일은 스윕되지 않습니다. 관리자는 정책을 설정하고, 폴더 이름을 생성하고, 폴더 이름을 제공하고, 해당 폴더를 추가할 수 있는 위치를 제안할 수 있습니다. 이러한 파일은 시스템에 필요한 파일이거나 보호가 필요하지 않은 파일일 수 있습니다.

> **중요:**
> 관리자가 기본 파일 보호 정책을 활성화하기 전에 폴더를 생성해야 합니다.

1 관리자가 제공한 폴더 이름과 경로를 사용합니다.
   - Mac의 경우 **기본 설정 창 > 기본 파일 보호 제외**로 이동합니다. 생성할 폴더 이름과 경로가 여기에 표시됩니다.
2 .txt와 같이 암호화할 필요가 없는 확장자의 경우 지정된 확장자로 파일을 추가합니다. 필요한 경우, 사용자가 생성한 이름의 하위 폴더를 추가할 수 있습니다.

노트:
이전에 암호화된 확장자가 있는 파일이 있는 경우 해당 폴더에 파일을 배치하면 해독되지 않으며 암호화된 상태로 유지됩니다. 관리자가 다른 정책을 통해 생성할 수 있는 **보호되지 않은 문서** 폴더가 있는 경우, 기본 파일 보호 유형을 이 폴더에 배치하여 암호를 해독할 수 있습니다.

3 기본 파일 보호가 활성화된 후 네트워크 또는 외부 드라이브의 해당 확장자에 보호되지 않는 파일이 있는 경우 해당 파일을 제외 폴더로 복사할 수 있으며 이 파일은 암호화되지 않은 상태로 유지됩니다. 그렇지 않으면 파일이 암호화됩니다.

컴퓨터에 한 명 이상의 사용자가 있는 경우 현재 로그인한 사용자만 해당 폴더에 파일을 배치하고 스윕에서 제외할 수 있습니다. 다른 사용자가 해당 폴더에 저장한 모든 파일은 스윕되고 암호화됩니다.

Windows 또는 Mac에서 파일 확장명 제거

관리자가 파일 확장명을 제거하기로 결정할 수 있습니다. 이 경우에는 해당 파일 형식을 해독하기 위해 컴퓨터가 스윕됩니다.

- 암호화된 파일의 *속성* > *Dell Data Guardian* 탭이 더 이상 표시되지 않습니다.
- 파일 오버레이 아이콘(있었던 경우)이 더 이상 표시되지 않습니다.
- 해독을 완료하는 데 몇 분 정도 걸릴 수 있습니다. 해당 확장명이 있는 파일이 계속 암호화되어 있는 경우 스윕 중에 열려 있었거나 파일 서버 또는 다른 위치에 저장되어 있었을 수 있습니다.

관리자에게 문의하여 해독되지 않는 해당 확장명이 있는 파일의 복구를 요청하십시오.

Office 애플리케이션

Office 애플리케이션을 사용하여 기본 파일 보호로 암호화된 파일을 열 수 있지만 컨텐츠는 읽기 전용입니다.

웹 포털

설정 > 정책에서 기본 파일 보호가 참으로 설정된 경우 관리자가 웹 포털에서 다운로드할 때 Data Guardian에서 암호화하는 비 Office 파일 형식을 추가했습니다. 관리자가 파일 형식을 알려줘야 합니다.

노트:
아직 지원되지 않는 파일 유형을 업로드하면 웹 포털에서 콘텐츠를 읽을 수 없습니다.

암호화되든 암호화되지 않은 파일 형식이든 비 Office 파일 형식을 업로드할 수 있습니다. 그러나 비 Office 파일을 다운로드하면 파일 확장명이 달라집니다.

비 Office 파일(예: .txt 또는 .png)	설명 다운로드
업로드하기 전에 암호화됨 예: Windows 또는 Mac에서 이미 암호화된 비 Office 파일.	웹 포털에서 다운로드할 경우 .txt 또는 .png와 같은 파일 확장명을 유지합니다.
암호화되지 않은 파일	웹 포털에서 다운로드할 때 파일 확장명은 관리자가 정책에 확장명을 추가했는지 여부에 따라 달라집니다. 하지만 파일은 암호화됩니다. 웹 포털에서 다운로드한 .txt 파일의 예: • **filename.txt** - 관리자가 .txt 파일 형식을 정책에 추가했습니다. • **filename.txt.xen** - .txt 파일 형식이 정책에 포함되지 않았습니다. 파일이 암호화되지만 .xen 확장명이 추가됩니다.

편집 정책이 웹 포털에 활성화되어 있는 경우 사용자는 비 Office 파일을 편집할 수 있습니다.

Identifier	GUID-932E973E-B2CD-4305-B50F-F85231243FA4
Status	In Translation

클라우드 스토리지 제공업체 사용

정책에 따라 웹 포털은 클라우드 스토리지 제공업체에 액세스할 수 있습니다. 자세한 내용은 웹 포털 온라인 도움말을 참조하십시오.

Identifier	GUID-8882A835-A7A8-4C7B-8330-3080F871A121
Status	Translation Validated

호스팅된 Dell 보안 센터 및 일시 중지된 테넌트

호스팅된 Dell 보안 센터에서 테넌트가 지정된 기간 동안 지불하지 않는 경우 해당 테넌트를 일시 중지할 수 있습니다. (Windows, Mac, 모바일, 웹 포털에 적용됨)

Data Guardian 내부 및 외부 사용자는 다음을 경험할 수 있습니다.

- 모든 플랫폼 - Data Guardian을 설치하거나, 활성화하거나, 로그인하려고 하면 테넌트가 일시 중지되었다는 대화 상자가 표시됩니다.
- Mac - Data Guardian이 열려 있는 동안 테넌트가 일시 중지된 경우 탐색기 및 모든 파일을 닫은 후 보호된 파일을 열면 일시 중단된 테넌트 대화 상자가 표시됩니다.
- 웹 포털:
  - 이미 로그인한 상태에서 암호화된 파일을 업로드하면 업로드 실패 메시지가 표시됩니다.
  - 암호화되거나 암호화되지 않은 파일을 업로드한 후 테넌트가 일시 중지된 경우 다운로드 실패 메시지가 표시됩니다.
  - 로그아웃한 후 다시 로그인하려고 하면 테넌트가 일시 중지되었음을 나타내는 대화 상자가 표시됩니다.

관리자에게 문의하십시오.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

외부 사용자로 Data Guardian 사용

도메인이 아닌 이메일 주소를 사용하는 외부 사용자도 Data Guardian을 사용할 수 있습니다. 다음은 몇 가지 예입니다.

- 엔터프라이즈의 일부로 Data Guardian을 설치하고 활성화하였지만 보호되는 파일을 회사 외부의 사용자와 공유하거나 공동 작업해야 하는 경우.
- 사용자 회사의 이메일 주소는 엔터프라이즈 도메인 내에 있지만, 도메인이 아닌 개인용 이메일 주소를 사용하여 컴퓨터나 모바일 장치에 Data Guardian을 설치하고 활성화하려는 경우. 이렇게 하면 엔터프라이즈 도메인이 아닌 이메일 주소에서 보낸 보호되는 파일과 상호 작용할 수 있습니다.

외부 사용자는 서버 요구 사항을 충족해야 합니다. 또한 도메인이나 사용자가 엔터프라이즈의 블랙리스트에 없어야 합니다.

호스팅된 환경의 경우, 외부 사용자는 하나의 테넌트에 대해서만 활성화할 수 있습니다.

외부 사용자를 위한 옵션은 다음과 같습니다.

- **Windows** - Data Guardian 클라이언트를 다운로드하고 설치합니다. Windows의 내부 사용자 작업 및 외부 사용자 작업을 참조하십시오.
- **Mac** - 외부 사용자 및 Mac을 참조하십시오.
- **모바일**
- **웹 포털** - Data Guardian 클라이언트를 다운로드하는 대신 Data Guardian 웹 포털을 사용합니다. 외부 사용자는 보호된 Office 문서 .pdf 또는 .xen 파일을 볼 수 있습니다. 정책에 따라 외부 사용자가 파일을 편집할 수 있습니다. 외부 사용자 및 웹 포털을 참조하십시오.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	In Translation

Windows의 내부 사용자 작업

다음을 수행하여 보호된 파일을 외부 사용자와 공유할 수 있습니다.

- 보호된 Office 문서에 *보호된 파일에 대한 액세스 권한* 옵션 사용
- 외부 사용자가 액세스를 요청할 때 액세스를 승인하거나 거부
- Outlook 이메일을 통해 보호된 Office 문서를 전송합니다.

하나 이상의 보호된 Office 파일에 액세스 권한 부여

외부 사용자와 공유하는 모든 파일에 액세스 권한을 부여해야 합니다.

1 보호된 파일을 마우스 오른쪽 단추로 클릭하고 **보호된 파일에 대한 액세스 권한**을 선택합니다. 파일을 하나만 선택할 수도 있고 최대 50개까지 여러 개를 선택할 수도 있습니다. 보호된 문서 액세스 공유 창이 열립니다. 파일은 다음 위치에 있을 수 있습니다.
   - 로컬 폴더 또는 네트워크 드라이브
   - 이메일

- 이동식 미디어
- 네트워크 공유

2 *공유할 이메일 주소* 필드의 오른쪽 최상단에 비 도메인 사용자의 이메일 주소를 입력하고 **추가**를 클릭합니다.

3 이 단계를 반복하여 최대 10개의 이메일 주소를 추가할 수 있습니다.

4 **확인**을 클릭합니다.
공유에 성공했거나 이메일 주소에 보호된 파일을 수신할 권한이 없다는 것을 나타내는 대화 상자가 표시됩니다.

5 아직 등록하지 않은 외부 사용자에게 Dell Server에 등록하고, Data Guardian을 다운로드 및 활성화하며, 공유된 보호된 파일을 보는 데 사용할 지침이 있는 이메일을 받게 될 것이라고 알리는 것이 좋습니다.

외부 사용자가 액세스를 요청할 때 액세스를 승인하거나 거부

Data Guardian을 설치한 외부 사용자는 보호된 문서에 대한 키가 없을 경우에 해당 문서에 대한 액세스를 요청할 수 있습니다.

1 외부 사용자로부터 보호된 문서에 대한 액세스를 요청하는 이메일을 받을 경우, 담당자가 외부 사용자의 이름과 요청한 파일을 볼 수 있습니다.

2 **승인** 또는 **거부**를 선택합니다.
외부 사용자에게 이메일이 전달됩니다. 승인을 하는 경우, 보호된 문서에 대한 키가 공유됩니다.

담당자가 없는 경우에는 담당자의 관리자가 액세스를 승인하거나 거부할 수 있습니다.

Outlook 이메일을 통해 보호된 파일 보내기

보호된 파일을 첨부하고 *보내기*를 클릭하면 보호되는 파일에 대한 키가 공유될 것이라는 확인 프롬프트가 표시됩니다.

노트:
외부 사용자가 보호된 파일을 이메일로 보내는 경우에는 키가 공유되지 않습니다.

Identifier	GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438
Status	In Translation

Windows에서의 외부 사용자 작업

보호된 파일에 대한 액세스 권한은 내부 사용자가 부여할 수 있습니다. 다음이 전송될 수 있습니다.

- 등록 지침이 포함된 이메일
- 올바른 이메일 주소 등록을 위한 링크를 포함하는 표지 페이지가 있는 보호된 파일

노트:
호스팅된 Dell 보안 센터가 멀티 테넌트인 경우, 표지 페이지에는 사내 환경의 Dell Server 이름 또는 특정 테넌트의 설치 ID가 나열됩니다. 표지 페이지에는 Data Guardian 클라이언트 다운로드 링크도 포함되어 있습니다.

외부 사용자가 Data Guardian 문서를 열어 보려면 다음을 수행해야 합니다.

- Data Guardian에 등록합니다.
- Data Guardian 다운로드 및 설치 - 외부 사용자는 자신의 컴퓨터에 대한 관리자 권한이 있어야 합니다.

Data Guardian 등록

내부 사용자가 처음으로 파일을 공유할 때 외부 사용자가 등록을 해야 합니다.

Data Guardian에 등록하려면 다음을 수행합니다.

1 다음 중 하나를 수행합니다.
- 이메일 - **수락**을 클릭합니다.
- 표지 페이지 경고를 표시하는 보호된 문서 - 제공된 링크를 클릭하여 올바른 이메일 주소를 등록합니다.

2 엔터프라이즈 환경에 따라 다음 일련의 단계 중 하나를 따릅니다.

호스팅된 Dell 보안 센터

호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션.

a Dell Data Guardian 웹 포털이 열리면 이메일 주소를 입력합니다.

b 아래로 스크롤하여 **동의**를 클릭합니다.

c Dell Security Center 창에서 *계정이 없으신가요?*까지 아래로 스크롤하여 **가입**을 클릭합니다.

d 새 계정 페이지에서 이메일, 이름, 성 및 암호를 입력합니다. 암호는 8자 이상으로 구성되어 소문자, 대문자, 특수 문자 및 숫자를 포함해야 합니다.

e **가입**을 클릭합니다.

f 등록에 사용한 이메일로 이동하고 검증 코드를 검색하여 입력합니다.

> **노트:** 이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

g **계정 확인**을 클릭합니다. 검증이 완료되면 웹 포털이 열립니다.

h 보호된 파일을 웹 포털로 끌어온 다음 **지금 업로드**를 클릭합니다.

i 등록 후 환영 이메일을 받게 됩니다. 이 이메일에는 Windows 클라이언트 다운로드를 위한 링크가 포함되어 있습니다.

> **노트:** 호스팅된 Dell 보안 센터가 멀티 테넌트인 경우 이 이메일에는 필요한 설치 ID도 나열됩니다.

사내 Dell Management Server

Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버.

> **노트:** 사내 환경인 경우 등록 전에 Data Guardian을 설치할 수 있습니다. 활성화할 때 **등록** 링크를 클릭하십시오.

a Dell Data Guardian 창이 열리면 이메일 주소를 입력합니다.

b **등록**을 클릭합니다.

c 등록 페이지에서 암호를 입력하고 확인한 다음 **로그인**을 클릭합니다.
등록 확인 대화상자가 표시되고 내부 사용자가 입력한 주소로 이메일이 전송됩니다. 이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

d Dell Server에서 보낸 계정 확인 이메일에서 하이퍼링크를 클릭합니다.

> **노트:** 이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

e 웹 페이지로 이어집니다.

f 확인 페이지에서 **로그인하려면 계속 하십시오**를 클릭합니다.

g 로그인 페이지에서 **암호 분실**을 클릭합니다.

> **노트:** Dell Server에서 임의의 암호를 할당하였습니다. 사용자는 이 암호를 재설정해야 합니다.

h 암호 재설정 페이지에서 암호를 입력하고 확인한 다음에 **등록**을 클릭합니다.
등록 확인 대화상자가 표시되고 내부 사용자가 입력한 주소로 이메일이 전송됩니다.

i 계정 활성화 이메일을 열고 링크를 클릭합니다.
이 이메일에는 Data Guardian을 설치할 때 사용할 Dell Server 이름도 포함되어 있습니다.

j 로그인 페이지에서, 등록할 때 사용한 이메일 주소와 암호를 입력합니다.

k **로그인**을 클릭합니다.
Data Guardian 다운로드 페이지가 열립니다.

Windows에 Data Guardian 다운로드 및 설치

등록 후 링크를 클릭하여 Windows 클라이언트를 다운로드할 수 있습니다. 처음에 제공되는 내부 사용자에 따라 다음 링크를 사용할 수 있습니다.

- Security Management Server의 경우, Windows 클라이언트용 옵션이 있는 다운로드 페이지가 열립니다.
- Security Management Server Virtual의 경우, Windows를 클릭하면 dell.com/support 사이트로 이동합니다.
- 보호된 파일을 받은 경우, 표지 페이지에 클라이언트 다운로드 링크가 포함되어 있습니다.
- 클라이언트 다운로드 링크가 포함된 환영 이메일을 받을 수 있습니다.

이러한 단계에서는 Windows에 대한 Data Guardian 설치를 설명합니다.

1 Windows에서 컴퓨터의 운영 체제에 따라 **다운로드(32비트)** 또는 **다운로드(64비트)**를 클릭합니다.
2 설치 파일을 컴퓨터의 디렉터리에 다운로드합니다.
3 설치 파일을 두 번 클릭하여 설치 프로그램을 실행합니다.
4 언어를 선택하고 **확인**을 클릭합니다.
5 Microsoft Visual C++ 2010 재배포 가능 패키지를 설치할 것인지를 묻는 메시지가 나타나면 **확인**을 클릭합니다.
6 시작 화면에서 **다음**을 클릭합니다.
7 라이센스 계약서를 읽고 조건을 수락한 후 **다음**을 클릭합니다.
8 대상 폴더 화면에서 **다음**을 클릭하여 C:\Program Files\Dell\Dell Data Guardian\의 기본 위치에 설치를 합니다.
9 구성 유형 화면에서 다음 중 하나를 선택합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
a 호스팅된 Dell 보안 센터를 선택합니다. b 엔터프라이즈가 멀티 테넌트인 경우, 표지 페이지 또는 환영 이메일에서 찾을 수 있는 설치 ID를 입력합니다. c **다음**을 클릭합니다. d 10단계를 계속 진행합니다.	a 사내 Dell Management Server를 선택합니다. b *서버 이름:* 필드에 이 컴퓨터가 통신할 Dell Server 이름을 입력합니다. 이 이름은 수신한 활성화 이메일 또는 다운로드 페이지 상단에서 볼 수 있습니다. c **다음**을 클릭합니다. d 활성화 서버 확인 화면에서 Dell Server URL 주소가 올바른지 확인하십시오. 설치 프로그램이 www 또는 http(s)와 포트를 추가합니다. **다음**을 클릭합니다. e 10단계를 계속 진행합니다.

10 관리 유형 창에서 이 옵션을 선택합니다.
- 외부 사용: 엔터프라이즈 도메인 이메일 주소 이외의 이메일 주소를 갖고 있는 사용자.

11 **설치**를 클릭하여 설치를 시작합니다.
상태 창에 설치 진행률이 표시됩니다.
12 설치 완료 화면이 표시되면 **마침**을 클릭합니다.
13 다시 시작하려면 **예**를 클릭합니다.
Data Guardian 설치가 완료되었습니다.
14 Data Guardian 활성화를 참조하십시오.

노트:
Windows에서 Data Guardian 사용하기에 나와 있는 참고 및 예외를 반드시 참조하십시오. 예를 들어 네트워크에서 보호되는 .pdf 파일은 열 수 없습니다. Word를 사용하여 보호된 .pdf 파일을 네트워크에서 열 수 있습니다.

Identifier	**GUID-92B941BF-52D2-4302-AFA1-3D348E260E03**
Status	**In Translation**

Data Guardian 활성화

Data Guardian이 설치되고 컴퓨터가 재부팅되면 다음 단계에 따라 활성화를 하십시오.

1 다음과 같이 Windows에 로그인합니다.
알림 영역에 주황색 느낌표가 있는 구름 아이콘이 표시됩니다.
2 알림 영역에 대화상자가 표시되면 **활성화를 하려면 여기를 클릭하십시오**를 클릭합니다.
대화 상자가 표시되지 않으면 알림 영역에서 **Data Guardian** 아이콘을 클릭하고 **사용자 활성화**를 선택합니다.

노트:
호스팅된 환경의 경우, 외부 사용자는 한 번에 하나의 테넌트에 대해서만 활성화할 수 있습니다. 한 테넌트에 대해 이미 활성화한 경우, Data Guardian을 제거하고 다른 설치 ID로 다시 설치해야 합니다. 필요한 경우, 웹 포털을 사용하여 보호된 문서를 업로드하고 볼 수 있습니다.

3 등록할 때 사용한 이메일 주소와 암호를 입력하고 **활성화**를 클릭합니다.

노트:
사내 환경의 경우, 등록하기 전에 Data Guardian을 설치한 경우에는 활성화할 때 **등록** 링크를 클릭합니다.

활성화가 완료되면 Data Guardian 알림 영역 아이콘()에 녹색 체크 표시가 나타납니다.

4 사용자 모드 상태를 확인합니다. 나중에 장치가 다른 사용자에게 다시 프로비저닝되도록 하거나 다시 등록되지 않도록 하려면 알림 영역 아이콘을 클릭하고 **세부 정보**를 선택합니다.
상단에 다음과 같은 사용자 모드가 표시됩니다.

외부: 도메인 이메일 주소 이외의 이메일 주소를 갖고 있는 사용자.

Identifier	**GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74**
Status	**Translation Validated**

내부 사용자로부터 액세스 요청

Windows, Mac, 모바일에서 외부 사용자가 Data Guardian을 설치하고 활성화하였다면 내부 사용자로부터 보호된 Office 문서 또는 .pdf에 대한 액세스를 요청할 수 있습니다. 외부 사용자는 각 파일마다 별도의 요청을 해야 합니다.

1 보호된 Office 문서를 열 때 액세스를 요청해야 한다는 메시지가 표시되면 **예** 또는 **아니요**를 클릭합니다.
요청이 성공적으로 전송되었다는 대화 상자가 표시됩니다. 내부 사용자는 액세스를 승인하거나 거부할 수 있고, 외부 사용자는 해당 결과가 있는 이메일을 수신합니다. 내부 사용자가 액세스를 승인하기 전에 외부 사용자가 보호된 파일을 열면 요청이 보류 중이라는 메시지가 표시됩니다.

2 외부 사용자는 48시간 후에 다시 액세스를 요청할 수 있습니다.
외부 사용자는 알림 영역에서 Data Guardian을 마우스 오른쪽 단추로 클릭하고 **세부 정보** 페이지를 선택할 수 있습니다. **보안** 탭을 클릭합니다. 요청에 대한 시간이 *없음*으로 되돌아가면 외부 사용자는 액세스를 다시 요청할 수 있습니다.

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

외부 사용자 및 Mac 작업

Mac용 내부 사용자 작업

다음 중 하나를 수행합니다.

- 보호된 문서 - 이메일, 네트워크 공유 또는 이동식 스토리지를 통해 보호된 파일을 외부 사용자에게 보냅니다.
- Data Guardian의 클라우드 암호화가 활성화된 경우 - Dell Data Guardian 인터페이스에서 보호된 파일을 클라우드 스토리지 공급자 열 옆의 열로 끌어 놓습니다.

Mac용 외부 사용자 작업

Data Guardian 등록

내부 사용자가 처음으로 파일을 공유할 때 외부 사용자가 등록을 해야 합니다.

Data Guardian에 등록하려면 다음을 수행합니다.

1 표지 페이지 경고를 표시하는 보호된 문서를 열면 제공된 링크를 클릭하여 올바른 이메일 주소를 등록합니다.

노트:
호스팅된 Dell 보안 센터가 멀티 테넌트인 경우, 표지 페이지에는 사내 환경의 Dell Server 이름 또는 특정 테넌트의 설치 ID가 나열됩니다. 표지 페이지에는 Data Guardian 클라이언트 다운로드 링크가 포함되어 있습니다.

2 사용자 환경에 따라 다음 중 하나를 수행합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버.
a Dell Data Guardian 웹 포털이 열리면 이메일 주소를 입력합니다. b 아래로 스크롤하여 **동의**를 클릭합니다. c Dell Security Center 창에서 *계정이 없으신가요?*까지 아래로 스크롤하여 **가입**을 클릭합니다. d 새 계정 페이지에서 이메일, 이름, 성 및 암호를 입력합니다. 암호는 8자 이상으로 구성되어 소문자, 대문자, 특수 문자 및 숫자를 포함해야 합니다. e **가입**을 클릭합니다. f 등록에 사용한 이메일로 이동하고 검증 코드를 검색하여 입력합니다. **노트:** 이메일이 표시되지 않는 경우 스팸함을 확인하십시오. g **계정 확인**을 클릭합니다. 검증이 완료되면 웹 포털이 열립니다. h 보호된 파일을 업로드하여 볼 수 있습니다. Mac 클라이언트 다운로드 링크가 포함된 이메일이 전송됩니다. 또는 표지 페이지에서 링크를 클릭할 수도 있습니다. 아래를 참조하십시오.	a Dell Data Guardian 창이 열리면 이메일 주소를 입력합니다. b **등록**을 클릭합니다. c 등록 페이지에서 암호를 입력하고 확인한 다음 **로그인**을 클릭합니다. 등록 확인 대화상자가 표시되고 내부 사용자가 입력한 주소로 이메일이 전송됩니다. 이메일이 표시되지 않는 경우 스팸함을 확인하십시오. d 계정 확인 이메일을 열고 링크를 클릭합니다. 이 이메일에는 Data Guardian을 설치할 때 사용할 Dell Server 이름도 포함되어 있습니다. e 등록 확인 페이지에서 **로그인 화면으로 돌아가기**를 클릭합니다. 표지 페이지에서 링크를 클릭하여 클라이언트를 다운로드하고 설치할 수 있습니다. 아래를 참조하십시오.

Data Guardian 클라이언트 다운로드 및 설치(선택사항)

1 Dell Data Guardian 페이지에서, 등록할 때 사용한 이메일 주소와 암호를 입력합니다.
2 **로그인**을 클릭합니다.
Windows, iOS, Android 및 Mac OS X에 대한 옵션과 함께 Data Guardian 다운로드 페이지가 열립니다.
3 Mac OS X에서 **다운로드**를 클릭합니다.
4 *드라이버 및 다운로드* 페이지에서 **Apple Mac OS**를 선택하고 **다운로드**를 클릭합니다.
5 컴퓨터의 디렉터리로 .dmg를 다운로드하여 .pkg를 실행합니다.
6 다음 중 하나를 수행하여 로그인/활성화합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
a 등록 시 사용한 이메일 주소를 사용하십시오. b 로그인 정보는 .dmg에 로그인하는 데 사용됩니다. c **로그인**을 클릭합니다.	a Data Guardian에 대한 온라인 도움말을 확인하고 계정 확인 이메일에 나열된 Dell Server 이름을 입력합니다. b 또한 이메일 주소와 암호를 입력합니다. 로그인 정보는 등록할 때 사용한 정보입니다. c **로그인**을 클릭합니다.

Identifier	GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A
Status	Translation Validated

외부 사용자 및 모바일

내부 사용자가 클라우드를 통해 보호된 파일에 대한 링크를 공유하는 경우, 파일에서 유효한 이메일 주소를 등록하기 위한 링크가 포함된 표지 페이지를 표시합니다.

노트:
호스팅된 Dell 보안 센터가 멀티 테넌트인 경우, 표지 페이지에는 사내 환경의 Dell Server 이름 또는 특정 테넌트의 설치 ID가 나열됩니다. 표지 페이지에는 Data Guardian 클라이언트 다운로드 링크도 포함되어 있습니다.

외부 사용자가 Data Guardian 문서를 열어 보려면 다음을 수행해야 합니다.

- Data Guardian에 등록합니다.
- Data Guardian 다운로드 및 설치 - 외부 사용자는 자신의 컴퓨터에 대한 관리자 권한이 있어야 합니다.

Data Guardian 등록

내부 사용자가 처음으로 파일을 공유할 때 외부 사용자가 등록을 해야 합니다.

Data Guardian에 등록하려면 다음을 수행합니다.

1 표지 페이지 경고에서 유효한 이메일 주소를 등록하기 위한 링크를 클릭합니다.

2 엔터프라이즈 환경에 따라 다음 일련의 단계 중 하나를 따릅니다.

호스팅된 Dell 보안 센터

호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션.

a Dell Data Guardian 웹 포털이 열리면 이메일 주소를 입력합니다.

b 아래로 스크롤하여 **동의**를 클릭합니다.

c Dell Security Center 창에서 *계정이 없으신가요?*까지 아래로 스크롤하여 **가입**을 클릭합니다.

d 새 계정 페이지에서 이메일, 이름, 성 및 암호를 입력합니다. 암호는 8자 이상으로 구성되어 소문자, 대문자, 특수 문자 및 숫자를 포함해야 합니다.

e **가입**을 클릭합니다.

f 등록에 사용한 이메일로 이동하고 검증 코드를 검색하여 입력합니다.

노트:
이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

g **계정 확인**을 클릭합니다. 검증이 완료되면 웹 포털이 열립니다.

h 보호된 파일을 웹 포털로 끌어온 다음 **지금 업로드**를 클릭합니다.

i 등록 후 환영 이메일을 받게 됩니다. 이 이메일에는 Windows 클라이언트 다운로드를 위한 링크가 포함되어 있습니다.

사내 Dell Management Server

Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버.

노트:
사내 환경인 경우 등록 전에 Data Guardian을 설치할 수 있습니다. 활성화할 때 **등록** 링크를 클릭하십시오.

a Dell Data Guardian 창이 열리면 이메일 주소를 입력합니다.

b **등록**을 클릭합니다.

c 등록 페이지에서 암호를 입력하고 확인한 다음 **로그인**을 클릭합니다.
등록 확인 대화상자가 표시되고 내부 사용자가 입력한 주소로 이메일이 전송됩니다. 이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

d Dell Server에서 보낸 계정 확인 이메일에서 하이퍼링크를 클릭합니다.

노트:
이메일이 표시되지 않는 경우 스팸함을 확인하십시오.

e 웹 페이지로 이어집니다.

f 확인 페이지에서 **로그인하려면 계속 하십시오**를 클릭합니다.

g 로그인 페이지에서 **암호 분실**을 클릭합니다.

노트:
Dell Server에서 임의의 암호를 할당하였습니다. 사용자는 이 암호를 재설정해야 합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
노트: 호스팅된 Dell 보안 센터가 멀티 테넌트인 경우 이 이메일에는 필요한 설치 ID도 나열됩니다.	h 암호 재설정 페이지에서 암호를 입력하고 확인한 다음에 **등록**을 클릭합니다. 등록 확인 대화상자가 표시되고 내부 사용자가 입력한 주소로 이메일이 전송됩니다. i 계정 활성화 이메일을 열고 링크를 클릭합니다. 이 이메일에는 Data Guardian을 설치할 때 사용할 Dell Server 이름도 포함되어 있습니다. j 로그인 페이지에서, 등록할 때 사용한 이메일 주소와 암호를 입력합니다. k **로그인**을 클릭합니다. Data Guardian 다운로드 페이지가 열립니다.

모바일용 Data Guardian 다운로드 및 설치

다음 중 하나를 수행합니다.

- Android 장치에서 Data Guardian 설치 또는 제거
- iOS 장치에서 Data Guardian 설치 또는 제거

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

외부 사용자 및 웹 포털

내부 사용자 작업

내부 사용자는 다음 중 하나를 수행할 수 있습니다.

- 외부 사용자에게 Data Guardian 웹 포털에 액세스하기 위한 기업 URL을 전송합니다.
- 보호되는 파일을 외부 사용자 전송합니다. 사용자가 파일을 열 때 표지 페이지가 표시됩니다.

외부 사용자는 정책에 따라 보호된 Office 문서 .pdf 파일 및 .xen 파일을 보거나 파일을 편집할 수 있습니다. 외부 사용자는 Data Guardian 클라이언트를 다운로드 할 필요가 없습니다.

웹 포털에 대한 외부 사용자 작업

Data Guardian 웹 포털에 등록하려면 다음을 수행합니다.

1 내부 사용자 또는 보호된 파일의 표지 페이지에서 받은 웹 포털 URL을 클릭합니다.
2 라이센스 계약 화면에서 아래로 스크롤하여 **동의**를 클릭합니다.
3 엔터프라이즈가 호스팅된 환경인지 사내인지에 따라 다음 중 하나를 수행합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
호스팅된 Dell Data Security 소프트웨어 관리용 SaaS(Software-as-a-Service) 솔루션.	Dell Data Security 소프트웨어 관리용 엔터프라이즈 네트워크에 위치한 사내 서버.
a 이메일과 암호를 입력합니다. b **로그인**을 클릭합니다. c 이메일, 이름, 성, 암호를 입력합니다. 암호는 8자 이상으로 구성되어 소문자, 대문자, 특수 문자 및 숫자를 포함해야 합니다.	a b **아직 계정이 없습니까?**를 클릭합니다. c 이메일 주소를 입력하고 **등록**을 클릭합니다.

호스팅된 Dell 보안 센터	사내 Dell Management Server
d **가입**을 클릭합니다. e 등록에 사용한 이메일로 이동하고 검증 코드를 검색하여 입력합니다. f 검증 코드를 입력하고 **계정 확인**을 클릭합니다. 웹 포털이 열립니다. 내부 사용자가 키를 공유하지 않는 경우에는 웹 포털에 액세스할 수 있지만 파일을 열 수는 없습니다.	**노트:** 외부 사용자로 등록하고 싶은 외부 사용자의 경우, 도메인이 아닌 이메일 주소를 사용합니다. d 등록 페이지에서 암호를 입력하고 확인한 후 **등록**을 클릭합니다. 제공한 이메일 주소로 확인 이메일이 전송되었다는 메시지가 확인 페이지에 표시됩니다. e 계정 활성화를 완료하려면 제목이 *계정 확인*인 이메일을 열고 링크를 클릭합니다. f 등록 확인 화면에서 **로그인 화면으로 돌아가기**를 클릭합니다. g 등록할 때 사용한 이메일 주소와 암호를 입력합니다.

4 Dell Data Guardian 업로드 페이지가 열립니다.
5 **찾아보기**를 클릭하여 파일을 탐색한 다음 파일을 웹 포털에 끌어서 놓습니다.
6 **?**를 클릭하여 각 페이지에 대한 온라인 도움말을 봅니다.

파일을 편집하려면 관리자가 해당 사용자에 대한 정책을 수정해야 합니다. 등록이 완료된 후 권한이 부여되면 웹 포털에서 로그아웃했다가 다시 로그인해야 합니다.

필요에 따라, Data Guardian 클라이언트를 다운로드할 수 있습니다. 표지 페이지에는 Data Guardian 클라이언트 다운로드 링크가 포함되어 있습니다. 호스팅된 Dell 보안 센터가 멀티 테넌트인 경우, 표지 페이지에는 사내 환경의 Dell Server 이름 또는 특정 테넌트의 설치 ID가 나열됩니다.

내부 사용자로부터 액세스 요청

보호된 Office 문서 또는 .pdf를 업로드하고 *업로드 실패* 대화 상자에 액세스 권한이 없다고 표시되는 경우 파일 작성자로부터 액세스 권한을 요청할 수 있습니다.

1 *업로드 실패* 대화 상자에서 **예**를 클릭합니다.
2 액세스가 허용되었는지 또는 거부되었는지를 나타내는 내부 사용자의 이메일을 기다립니다.

노트:
내부 사용자로부터 이메일을 받지 못한 경우 48시간 후에 액세스를 다시 요청해야 합니다. 내부 사용자가 액세스를 승인하기 전에 보호된 파일을 열면 요청이 보류 중이라는 메시지가 표시됩니다.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

보호된 Office 문서 보기

엔터프라이즈에서 Office 문서를 보호하기 위한 정책을 활성화하고 내부 사용자가 보호된 파일을 외부 사용자에게 보낼 경우, 외부 사용자는 문서를 처음 열 때 Dell Server에 연결되어 있어야 합니다. 그 다음에는 지정된 시간(예: 1주일) 동안 오프라인으로 문서를 열고 볼 수 있습니다. 그 후에 외부 사용자는 Dell Server에 연결하여 보호된 문서를 다시 열어야 합니다.

보안 목적상 외부 사용자는 보호된 Office 문서로 다음과 같은 작업을 할 수 없습니다.

- 인쇄

- 내보내기
- 다른 이름으로 저장
- 공유

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

호스팅된 Dell 보안 센터 및 일시 중지된 테넌트

호스팅된 Dell 보안 센터에서 테넌트가 지정된 기간 동안 지불하지 않는 경우 해당 테넌트를 일시 중지할 수 있습니다. (Windows, Mac, 모바일, 웹 포털에 적용됨)

Data Guardian 내부 및 외부 사용자는 다음을 경험할 수 있습니다.

- 모든 플랫폼 - Data Guardian을 설치하거나, 활성화하거나, 로그인하려고 하면 테넌트가 일시 중지되었다는 대화 상자가 표시됩니다.
- Mac - Data Guardian이 열려 있는 동안 테넌트가 일시 중지된 경우 탐색기 및 모든 파일을 닫은 후 보호된 파일을 열면 일시 중단된 테넌트 대화 상자가 표시됩니다.
- 웹 포털:
  - 이미 로그인한 상태에서 암호화된 파일을 업로드하면 업로드 실패 메시지가 표시됩니다.
  - 암호화되거나 암호화되지 않은 파일을 업로드한 후 테넌트가 일시 중지된 경우 다운로드 실패 메시지가 표시됩니다.
  - 로그아웃한 후 다시 로그인하려고 하면 테넌트가 일시 중지되었음을 나타내는 대화 상자가 표시됩니다.

관리자에게 문의하십시오.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Data Guardian의 액세스 그룹으로 보안 강화(사내 환경)

Data Guardian의 액세스 그룹은 암호화된 데이터에 대해 협업을 수행할 수 있는 사용자 그룹을 만들어 보안을 강화합니다. 파일의 소유자가 액세스 권한을 부여하지 않으면 그룹 밖에 있는 사용자는 데이터에 대한 액세스나 보기를 할 수 없습니다. 액세스 그룹에는 내부 및 외부 사용자가 포함될 수 있습니다. Windows, Mac, 모바일 및 웹 포털에서 액세스 그룹을 사용할 수 있습니다.

엔터프라이즈에 따라 다음 옵션 중 하나를 선택합니다.

- 엔터프라이즈에 옵트인 모드로 Data Guardian이 설치되어 있음
- 엔터프라이즈에 강제 보호 모드로 Data Guardian이 설치되어 있음
- 엔터프라이즈에 아직 Data Guardian 및 옵트인 모드가 없음
- 엔터프라이즈에 아직 Data Guardian 및 강제 보호 모드가 없음

다음 항목도 수행할 수 있습니다.

- 암호화된 파일의 소유자 변경
- 키에 대한 액세스 해지

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

엔터프라이즈에 옵트인 모드로 Data Guardian이 설치되어 있음

엔터프라이즈에서 액세스 그룹을 사용하여 중요 데이터에 대한 보안을 강화하는 경우 액세스 그룹에 누가 있는지 알아야 합니다. 초기에는 원활한 전환을 보장하기 위해 엔터프라이즈에서 기존의 공유된 파일과 암호화된 파일을 처리하기 위한 짧은 기간을 제공할 수도 있습니다. 전환 기간이 완료되면 액세스 그룹에 있는 사람이 사용자가 생성한 모든 공유 및 암호화된 파일을 볼 수 있습니다. 액세스 그룹 외부의 개인에게 액세스 권한을 부여할 수 있습니다.

액세스 그룹에서 해당하는 사람을 확인합니다.

관리자는 특정 파일에 대한 액세스 권한이 필요한 사람에 따라 사용자의 액세스 그룹 중 하나 이상에 있는 사람을 알려 줄 것입니다. 내부 및 외부 사용자가 포함될 수 있습니다. 특정 사용자와 함께 중요 데이터에 대한 작업을 하는 경우에는 관리자에게 해당 콘텐츠에 대한 액세스 그룹을 생성하도록 요청할 수 있습니다.

전환 기간을 사용하여 공유된 파일 및 암호화된 파일 처리

Data Guardian이 이미 설치되어 있고 기존 파일이 암호화되어 있는 경우 암호화된 공유 파일을 위한 짧은 전환 기간을 두는 것이 엔터프라이즈에게 가장 좋은 방법입니다. 원활한 전환을 위해 암호화된 공유 파일의 경우 다음 사항에 유의하십시오.

- 파일의 소유자나 작성자는 내부 또는 외부에서 파일에 계속 액세스할 수 있습니다.
- 액세스 그룹 내부의 내부 또는 외부 사용자는 대부분의 공유 파일에 액세스할 수 있습니다. 일부 파일과 연관된 키 유형에 따라 일부 파일에 대한 액세스 권한을 상실할 수 있습니다.
- 액세스 그룹 외부에 있는 내부 사용자 - 사용자는 전환 기간 동안 모든 공유 파일을 열어야 키에 대한 액세스 권한을 얻을 수 있습니다. 이 짧은 기간 동안 공유된 파일과 암호화된 파일을 열지 않으면 파일에 액세스할 수 없게 됩니다.
- 액세스 그룹에 있지 않은 외부 사용자 - 암호화된 파일에 액세스 권한을 이미 부여한 경우 외부 사용자는 전환 기간과 전환 후에도 계속 액세스할 수 있습니다.

전환 기간 후에 파일에 대한 액세스 권한을 상실하면 소유자에게 액세스를 요청할 수 있습니다.

전환 기간 후 암호화된 공유 파일에 다시 액세스 권한 확보

옵트인 모드의 Windows 및 Mac에서 다음을 수행하여 다시 액세스 권한을 확보할 수 있습니다.

- 보호된 Office 문서 - 내부 및 외부 사용자가 액세스 권한을 요청하는 대화 상자가 표시되고 파일 소유자가 액세스 권한 부여 여부를 결정할 수 있습니다.
- 기본 파일 보호를 통해 암호화된 추가 파일 형식 - 사후 공유 프롬프트가 없습니다. 사용자는 파일 소유자를 확인하고 암호화된 파일을 마우스 오른쪽 단추로 클릭하여 Data Guardian 탭에서 키 ID를 찾아야 합니다. 사용자는 소유자에게 해당 정보를 전송하고 액세스를 요청할 수 있습니다.

변환 기간 후 새롭게 암호화된 파일에 대한 협업

전환 기간 후 생성 및 암호화하는 새 파일의 경우:

- 액세스 그룹 내부의 내부 또는 외부 사용자 - 모든 공유 및 암호화된 파일에 액세스할 수 있습니다.
  - 액세스 그룹에서 제거된 모든 사용자는 액세스 권한을 상실합니다.
  - 파일 소유자가 그룹에서 제거된 경우에도 다른 사용자는 계속 액세스할 수 있습니다.
- 액세스 그룹 외부의 내부 또는 외부 사용자 - 암호화된 파일을 볼 수 없습니다.
  - 액세스 그룹 내부의 내부 사용자는 액세스 권한을 부여할 수 있습니다.
  - 외부 사용자가 암호화된 파일의 소유자인 경우 다른 개인에게 액세스 권한을 부여할 수 있습니다.
  - 그룹 외부의 내부 또는 외부 사용자가 암호화된 Office 문서를 받아 열려고 하면 액세스 권한을 요청하는 대화 상자가 표시됩니다.
  - 그룹 외부의 내부 또는 외부 사용자가 기본 파일 보호로부터 파일 형식을 수신하고 열려고 하는 경우, 사용자는 암호화된 파일을 마우스 오른쪽 단추로 클릭하여 Data Guardian 탭에서 키 ID를 찾은 다음 해당 정보를 소유자에게 보낼 수 있습니다.

Identifier	**GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57**
Status	**In Translation**

엔터프라이즈에 강제 보호 모드로 Data Guardian이 설치되어 있음

엔터프라이즈에서 액세스 그룹을 사용하여 중요 데이터에 대한 보안을 강화하는 경우 액세스 그룹에 누가 있는지 알아야 합니다. 초기에는 원활한 전환을 보장하기 위해 엔터프라이즈에서 기존의 공유된 파일과 암호화된 파일을 처리하기 위한 짧은 기간을 제공할 수도 있습니다. 전환 기간이 완료되면 액세스 그룹에 있는 사람이 사용자가 생성한 모든 공유 및 암호화된 파일을 볼 수 있습니다. 액세스 그룹 외부의 개인에게 액세스 권한을 부여할 수 있습니다.

액세스 그룹에서 해당하는 사람을 확인합니다.

관리자는 특정 파일에 대한 액세스 권한이 필요한 사람에 따라 사용자의 액세스 그룹 중 하나 이상에 있는 사람을 알려 줄 것입니다. 내부 및 외부 사용자가 포함될 수 있습니다. 특정 사용자와 함께 중요 데이터에 대한 작업을 하는 경우에는 관리자에게 해당 콘텐츠에 대한 액세스 그룹을 생성하도록 요청할 수 있습니다.

전환 기간을 사용하여 공유된 파일 및 암호화된 파일 처리

Data Guardian이 이미 설치되어 있고 기존 파일이 암호화되어 있는 경우 암호화된 공유 파일을 위한 짧은 전환 기간을 두는 것이 엔터프라이즈에게 가장 좋은 방법입니다. 원활한 전환을 위해 암호화된 공유 파일의 경우 다음 사항에 유의하십시오.

- 파일의 소유자나 작성자는 내부 또는 외부에서 파일에 계속 액세스할 수 있습니다.
- 액세스 그룹 내부의 내부 또는 외부 사용자는 대부분의 공유 파일에 액세스할 수 있습니다. 일부 파일과 연관된 키 유형에 따라 일부 파일에 대한 액세스 권한을 상실할 수 있습니다.
- 액세스 그룹 외부에 있는 내부 사용자 - 사용자는 전환 기간 동안 모든 공유 파일을 열어야 키에 대한 액세스 권한을 얻을 수 있습니다. 이 짧은 기간 동안 공유된 파일과 암호화된 파일을 열지 않으면 파일에 액세스할 수 없게 됩니다.
- 액세스 그룹에 있지 않은 외부 사용자 - 암호화된 파일에 액세스 권한을 이미 부여한 경우 외부 사용자는 전환 기간 후에도 계속 액세스할 수 있습니다.

전환 기간 후에 파일에 대한 액세스 권한을 상실하면 소유자에게 액세스를 요청할 수 있습니다.

전환 기간 후 암호화된 공유 파일에 다시 액세스 권한 확보

강제 보호 모드의 Windows 및 Mac의 경우 다음을 수행하여 다시 액세스 권한을 확보할 수 있습니다.

- 보호된 Office 문서 - 내부 및 외부 사용자가 액세스 권한을 요청하는 대화 상자가 표시되고 파일 소유자가 액세스 권한 부여 여부를 결정할 수 있습니다.
- 기본 파일 보호를 통해 암호화된 추가 파일 형식 - 사후 공유 프롬프트가 없습니다. 사용자는 파일 소유자를 확인하고 암호화된 파일을 마우스 오른쪽 단추로 클릭하여 Data Guardian 탭에서 키 ID를 찾아야 합니다. 사용자는 소유자에게 해당 정보를 전송하고 액세스를 요청할 수 있습니다.

전환 기간 후 새로 생성된 파일에 대한 협업

전환 기간 후 생성 및 암호화하는 새 파일의 경우:

- 액세스 그룹 내부의 내부 또는 외부 사용자 - 모든 공유 및 암호화된 파일에 액세스할 수 있습니다.
  - 액세스 그룹에서 제거된 모든 사용자는 액세스 권한을 상실합니다.
  - 파일 소유자가 그룹에서 제거된 경우에도 다른 사용자는 계속 액세스할 수 있습니다.
- 액세스 그룹 외부의 내부 또는 외부 사용자 - 암호화된 파일을 볼 수 없습니다.
  - 액세스 그룹 내부의 내부 사용자는 액세스 권한을 부여할 수 있습니다.
  - 외부 사용자가 암호화된 파일의 소유자인 경우 다른 개인에게 액세스 권한을 부여할 수 있습니다.
  - 그룹 외부의 내부 또는 외부 사용자가 암호화된 파일을 받아 열려고 하면 액세스 권한을 요청하는 대화 상자가 표시됩니다.

Identifier	GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4
Status	In Translation

엔터프라이즈에 아직 Data Guardian 및 옵트인 모드가 없음

엔터프라이즈에서 중요 데이터에 대한 보안을 강화하기 위해 액세스 그룹과 함께 Data Guardian을 사용하려는 경우 내부 또는 외부 사용자와 함께 공유하는 파일을 확인하고 관리자가 만들어 준 액세스 그룹에 이러한 사용자가 있을지를 알아보는 것이 가장 좋은 방법입니다. 초기에는 원활한 전환을 보장하기 위해 엔터프라이즈에서 기존의 공유 파일을 처리하기 위한 짧은 기간을 제공할 수도 있습니다. 전환 기간이 완료되면 액세스 그룹에 있는 사람이 사용자가 생성한 모든 공유된 파일과 암호화된 파일을 볼 수 있습니다. 액세스 그룹 외부의 개인에게 액세스 권한을 부여하여 이들과 협업을 하면서 보안을 강화할 수 있습니다.

액세스 그룹에서 해당하는 사람을 확인합니다.

관리자는 특정 파일에 대한 액세스 권한이 필요한 사람에 따라 사용자의 액세스 그룹 중 하나 이상에 있는 사람을 알려 줄 것입니다. 내부 및 외부 사용자가 포함될 수 있습니다. 특정 사용자와 함께 중요 데이터에 대한 작업을 하는 경우에는 관리자에게 해당 콘텐츠에 대한 액세스 그룹을 생성하도록 요청할 수 있습니다.

전환 기간을 사용하여 공유 파일 처리

Data Guardian이 설치되면 Windows 또는 Mac에서 스윕이 발생하며 관리자가 해당 정책을 활성화한 경우 다음 파일이 암호화됩니다.

- 기본 파일 보호를 위해 구성된 추가 파일 형식(예: .txt 또는 .png)
- 데이터 분류 파일(Windows)
- TITUS 분류 파일(Windows)

이미 파일에 대한 협업을 하거나 내부 또는 외부 사용자와 공유하는 경우 해당 사용자는 액세스 그룹에 있을 수도 있고 없을 수도 있습니다. 원활한 전환을 위한 가장 좋은 방법은 다른 사용자와 공유하는 암호화된 파일을 처리하기 위한 짧은 전환 기간을 가지는 것입니다. 이 전환 기간 동안에 컴퓨터에 로그인해야 합니다.

이러한 파일에 대한 공유 또는 협업을 계속하려면 다음 사항에 유의하십시오.

- 위에 나열된 공유 파일의 경우 로그인하고 컴퓨터를 스윕한 첫 번째 사람이 공유 파일의 소유자가 됩니다.
- 다른 사람이 파일의 소유자가 되고 원래 작성자가 액세스 그룹에 없는 경우 원래 소유자가 새 소유자에게 액세스 권한을 요청해야 합니다. 원래 소유자는 관리자에게 소유권 변경을 요청할 수도 있습니다.
- 외부 사용자 컴퓨터는 스윕되지 않기 때문에 보호되지 않은 공유 파일의 사본은 스윕되고 암호화되지 않습니다.
- Data Guardian의 클라우드 암호화가 활성화되고 사용자가 클라우드 스토리지 공급업체의 폴더 또는 파일을 공유하는 경우 이러한 파일도 스윕됩니다.

전환 기간 후 새로 생성된 파일에 대한 협업

전환 기간 후 생성 및 암호화하는 새 파일의 경우:

- 액세스 그룹 내부의 내부 또는 외부 사용자 - 모든 공유 및 암호화된 파일에 액세스할 수 있습니다.
  - 액세스 그룹에서 제거된 모든 사용자는 액세스 권한을 상실합니다.
  - 파일 소유자가 그룹에서 제거된 경우에도 다른 사용자는 계속 액세스할 수 있습니다.
- 액세스 그룹 외부의 내부 또는 외부 사용자 - 암호화된 파일을 볼 수 없습니다.
  - 액세스 그룹 내부의 내부 사용자는 액세스 권한을 부여할 수 있습니다.
  - 외부 사용자가 암호화된 파일의 소유자인 경우 다른 개인에게 액세스 권한을 부여할 수 있습니다.

- 그룹 외부의 내부 또는 외부 사용자가 암호화된 파일을 받아 열려고 하면 액세스 권한을 요청하는 대화 상자가 표시됩니다.

Identifier	GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2
Status	In Translation

엔터프라이즈에 아직 Data Guardian 및 강제 보호 모드가 없음

엔터프라이즈에서 중요 데이터에 대한 보안을 강화하기 위해 액세스 그룹과 함께 Data Guardian을 사용하려는 경우 내부 또는 외부 사용자와 함께 공유하는 파일을 확인하고 관리자가 만들어 준 액세스 그룹에 이러한 사용자가 있을지를 알아보는 것이 가장 좋은 방법입니다. 초기에는 원활한 전환을 보장하기 위해 엔터프라이즈에서 기존의 공유 파일을 처리하기 위한 짧은 기간을 제공할 수도 있습니다. 전환 기간이 완료되면 액세스 그룹에 있는 사람이 사용자가 생성한 모든 공유된 파일과 암호화된 파일을 볼 수 있습니다. 액세스 그룹 외부의 개인에게 액세스 권한을 부여하여 이들과 협업을 하면서 보안을 강화할 수 있습니다.

액세스 그룹에서 해당하는 사람을 확인합니다.

관리자는 특정 파일에 대한 액세스 권한이 필요한 사람에 따라 사용자의 액세스 그룹 중 하나 이상에 있는 사람을 알려 줄 것입니다. 내부 및 외부 사용자가 포함될 수 있습니다. 특정 사용자와 함께 중요 데이터에 대한 작업을 하는 경우에는 관리자에게 해당 콘텐츠에 대한 액세스 그룹을 생성하도록 요청할 수 있습니다.

전환 기간을 사용하여 공유 파일 처리

Data Guardian이 설치되면 Windows 또는 Mac에서 스윕이 발생하며 관리자가 해당 정책을 활성화한 경우 다음 파일이 암호화됩니다.

- Office 문서
- PDF
- 기본 파일 보호를 위해 구성된 추가 파일 형식(예: .txt 또는 .png)

원활한 전환을 위한 가장 좋은 방법은 다른 사용자와 공유하는 암호화된 파일을 처리하기 위한 짧은 전환 기간을 가지는 것입니다. 이 전환 기간 동안에 컴퓨터에 로그인해야 합니다.

이러한 파일에 대한 공유 또는 협업을 계속하려면 다음 사항에 유의하십시오.

- 위에 나열된 공유 파일의 경우 로그인하고 컴퓨터를 스윕한 첫 번째 사람이 공유 파일의 소유자가 됩니다.
- 다른 사람이 파일의 소유자가 되고 원래 작성자가 액세스 그룹에 없는 경우 원래 소유자가 새 소유자에게 액세스 권한을 요청해야 합니다. 원래 소유자는 관리자에게 소유권 변경을 요청할 수도 있습니다.
- 외부 사용자 컴퓨터는 스윕되지 않기 때문에 보호되지 않은 공유 파일의 사본은 스윕되고 암호화되지 않습니다.
- Data Guardian의 클라우드 암호화가 활성화되고 사용자가 클라우드 스토리지 공급업체의 폴더 또는 파일을 공유하는 경우 이러한 파일도 스윕됩니다.

전환 기간 후 새로 생성된 파일에 대한 협업

전환 기간 후 생성 및 암호화하는 새 파일의 경우:

- 액세스 그룹 내부의 내부 또는 외부 사용자 - 모든 공유 및 암호화된 파일에 액세스할 수 있습니다.
  - 액세스 그룹에서 제거된 모든 사용자는 액세스 권한을 상실합니다.
  - 파일 소유자가 그룹에서 제거된 경우에도 다른 사용자는 계속 액세스할 수 있습니다.
- 액세스 그룹 외부의 내부 또는 외부 사용자 - 암호화된 파일을 볼 수 없습니다.
  - 액세스 그룹 내부의 내부 사용자는 액세스 권한을 부여할 수 있습니다.
  - 외부 사용자가 암호화된 파일의 소유자인 경우 다른 개인에게 액세스 권한을 부여할 수 있습니다.
  - 그룹 외부의 내부 또는 외부 사용자가 암호화된 파일을 받아 열려고 하면 액세스 권한을 요청하는 대화 상자가 표시됩니다.

Identifier	GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B
Status	Translated

암호화된 파일의 소유자 변경

액세스 그룹에 대한 전환 기간 중에 사용자가 원래 작성했던 공유 및 암호화된 문서의 소유자로 다른 사용자가 지정되면 원래 사용자는 관리자에게 자신을 소유자로 지정할 것을 요청할 수 있습니다.

Identifier	GUID-0ED28BBC-3A7C-48F3-A1AE-A5039C39C392
Status	In Translation

키에 대한 액세스 해지

외부 사용자에게 암호화된 파일에 대한 액세스 권한을 부여하는 경우 사용자는 해당 파일을 열 수 있는 키를 가지고 있습니다.
필요한 경우, 외부 사용자가 파일에 더 이상 액세스할 수 없게 하려면 관리자에게 키를 해지하도록 요청할 수 있습니다. 이는 외부 사용자에게만 적용됩니다.

Identifier	GUID-8B76A529-19A6-4107-983B-707F5AB1D09C
Status	In Translation

Windows에서 보호된 파일 사전 공유

Data Guardian이 설치되어 있어야 하며 하나 이상의 액세스 그룹에 할당되어야 합니다.
내부 또는 외부 사용자가 액세스 그룹에 없으면 보호된 파일을 미리 공유할 수 있습니다.

1 보호된 파일을 마우스 오른쪽 단추로 클릭하고 **보호된 파일 액세스**를 선택합니다.
보호된 파일 액세스 공유 UI에서 문서 이름이 선택한 파일에 표시됩니다.
2 *공유할 이메일*에서 **추가**를 클릭하고 외부 사용자 또는 액세스 그룹에 없는 내부 사용자의 유효한 이메일 주소를 입력합니다.
한 번에 최대 10개의 개별 주소를 추가할 수 있습니다.
3 이메일 주소를 수정하려면 **수정**을 클릭합니다.
4 이메일 주소를 삭제하려면 항목을 선택하고 **삭제**를 클릭합니다.

> **노트:**
> 파일 소유자 이름이 표시되며 선택하거나 삭제할 수 없습니다.

5 사용 가능한 그룹에 액세스 그룹이 표시됩니다. 하나 이상의 그룹을 선택하고 화살표를 사용하여 *공유 그룹*에 추가합니다.
6 **확인**을 클릭합니다. 확인 메시지가 표시됩니다.

> **노트:**
> 외부 사용자는 보호된 문서를 다른 외부 사용자와 공유할 수 없습니다.

외부 사용자가 Data Guardian 보호 파일을 처음으로 수신하는 경우, 보호된 파일을 보려면 사용자는 Data Guardian을 설치하거나 웹 포털을 사용해야 합니다.

Identifier	GUID-C67795A0-FA20-4E32-9A2B-89654D67DFB2
Status	In Translation

Mac에서 보호된 파일 사전 공유

Data Guardian이 설치되어 있어야 하며 하나 이상의 액세스 그룹에 할당되어야 합니다.

내부 또는 외부 사용자가 액세스 그룹에 없으면 보호된 파일을 미리 공유할 수 있습니다.

1 보호된 파일을 마우스 오른쪽 단추로 클릭하고 **보호된 파일 액세스**를 선택합니다.
보호된 파일 액세스 공유 UI에서 문서 이름이 선택한 파일에 표시됩니다.
2 *공유할 이메일*에서 **추가**를 클릭하고 외부 사용자 또는 액세스 그룹에 없는 내부 사용자의 유효한 이메일 주소를 입력합니다.
한 번에 최대 10개의 개별 주소를 추가할 수 있습니다.
3 이메일 주소를 삭제하려면 항목을 선택하고 **삭제**를 클릭합니다.

> **노트:**
> 파일 소유자 이름이 표시되며 선택하거나 삭제할 수 없습니다.

4 사용 가능한 그룹에 액세스 그룹이 표시됩니다. 하나 이상의 그룹을 선택하고 화살표를 사용하여 *공유 그룹*에 추가합니다.
5 **확인**을 클릭합니다. 확인 메시지가 표시됩니다.

> **노트:**
> 외부 사용자는 보호된 문서를 다른 외부 사용자와 공유할 수 없습니다.

외부 사용자가 Data Guardian 보호 파일을 처음으로 수신하는 경우, 보호된 파일을 보려면 사용자는 Data Guardian을 설치하거나 웹 포털을 사용해야 합니다.

Identifier	GUID-FAF997A4-8E8E-4DCB-BA76-575F951F0799
Status	In Translation

iOS 또는 Android에서 보호된 파일 사전 공유

내부 또는 외부 사용자가 액세스 그룹에 없으면 보호된 파일을 미리 공유할 수 있습니다.

1 보호된 파일을 탭합니다.
2

> **노트:**
> *사용자* 탭에서 파일 소유자 이름이 표시되지만 선택하거나 삭제할 수 없습니다. 내부 또는 외부 사용자와 파일을 이미 공유한 경우 해당 이름이 표시됩니다.

3 *사용자* 탭에서 액세스 그룹에 없는 외부 사용자 또는 내부 사용자의 이메일 주소를 추가하려면 오른쪽 아래에 있는 더하기 아이콘(+)을 클릭합니다.
4 이메일 주소를 삭제하려면 살짝 밀고 **삭제**를 탭합니다.
5 **그룹** 탭을 탭하여 액세스 그룹을 봅니다.
6 보호된 파일을 공유하려면 그룹을 탭합니다.

> **노트:**
> 체크 표시는 보호된 파일을 공유하기로 선택한 그룹을 나타냅니다.

7 오른쪽 상단에서 **공유**를 탭합니다.
확인 메시지가 표시됩니다. 외부 사용자는 보호된 문서를 다른 외부 사용자와 공유할 수 없습니다.

외부 사용자가 Data Guardian 보호 파일을 처음으로 수신하는 경우, 보호된 파일을 보려면 사용자는 Data Guardian을 설치하거나 웹 포털을 사용해야 합니다.

Identifier	GUID-455BE40E-83D4-4C42-890C-18067EE3CFD5
Status	In Translation

웹 포털에서 보호된 파일 사전 공유

내부 또는 외부 사용자가 액세스 그룹에 없으면 보호된 파일을 미리 공유할 수 있습니다.

1 웹 포털에서 보호된 문서를 업로드합니다.
관리자가 하나 이상의 액세스 그룹을 배치한 경우 *보호된 파일 액세스* 아이콘이 다운로드 아이콘 옆에 표시됩니다.
2 **보호된 파일 액세스** 아이콘을 클릭합니다.
보호된 파일 액세스 공유 UI에서 문서 이름이 선택한 파일에 표시됩니다.
3 *공유할 이메일 주소*에서 **새로 추가**를 클릭합니다.
4 액세스 그룹에 없는 외부 사용자 또는 내부 사용자의 유효한 이메일 주소를 입력하고 체크 표시를 클릭하여 저장합니다. 한 번에 최대 10개의 개별 주소를 추가할 수 있습니다.

> **노트:**
> 이메일 주소를 삭제하려면 **X**를 클릭합니다. 문서를 공유하는 사용자의 이름은 강조 표시되며 선택하거나 삭제할 수 없습니다.

5 사용 가능한 그룹에 액세스 그룹이 표시됩니다. **모두 선택**을 클릭하거나 옵션 옆에 있는 화살표 아이콘을 클릭하여 *공유 그룹*에 추가하거나 제거합니다.
6 **확인**을 클릭합니다.

> **노트:**
> 외부 사용자는 보호된 문서를 다른 외부 사용자와 공유할 수 없습니다.

외부 사용자가 Data Guardian 보호 파일을 처음으로 수신하는 경우 사용자는 웹 포털을 설치해야 합니다.

Identifier	GUID-5BE95524-98D7-476C-9790-CA2298568418
Status	In Translation

보호된 파일을 외부 사용자로 사전 공유

Data Guardian이 설치되어 있어야 하며 하나 이상의 액세스 그룹에 할당되어야 합니다.
보호된 파일의 작성자 또는 소유자인 경우 내부 사용자와 파일을 미리 공유할 수 있습니다. 보호된 문서는 다른 외부 사용자와 공유할 수 없습니다. 파일을 소유하고 있지 않으면 공유할 수 없습니다.

- *공유할 이메일*은 보호된 문서가 공유된 다른 사용자의 이름을 나열하지 않습니다.
- 사용 가능한 그룹에 그룹이 표시되지 않습니다. 개별 사용자에게만 공유할 수 있습니다.

1 보호된 파일을 마우스 오른쪽 단추로 클릭하고 **보호된 파일 액세스**를 선택합니다.
보호된 파일 액세스 공유 UI에서 문서 이름이 선택한 파일에 표시됩니다.
2 *공유할 이메일*에서 **추가**를 클릭하고 외부 사용자 또는 액세스 그룹에 없는 내부 사용자의 유효한 이메일 주소를 입력합니다.
한 번에 최대 10개의 개별 주소를 추가할 수 있습니다.
3 이메일 주소를 수정하려면 **수정**을 클릭합니다.
4 이메일 주소를 삭제하려면 항목을 선택하고 **삭제**를 클릭합니다.

> **노트:**
> 파일 소유자로서 이름을 선택하거나 삭제할 수 없습니다.

5 **확인**을 클릭합니다. 확인 메시지가 표시됩니다.

사용자가 Data Guardian 보호 파일을 처음으로 수신하는 경우, 보호된 파일을 보려면 사용자는 Data Guardian을 설치하거나 웹 포털을 사용해야 합니다.

Identifier	**GUID-F97CE528-0A49-4763-80D0-0F5937EAE934**
Status	**In Translation**

보호된 이메일에 액세스할 수 있는 사람 수정

관리자가 설정한 정책에 따라, 사용자가 보호한 이메일을 마우스 오른쪽 단추로 클릭하고 액세스 그룹의 사용자에게 보낼 수 있습니다. 해당 이메일에 액세스할 수 있는 사람을 수정할 수 있습니다.

1 Outlook에서 [보호됨]으로 표시된 이메일을 마우스 오른쪽 단추로 클릭합니다.
2 하단에서 **보호된 이메일 액세스**를 선택합니다.
공유된 액세스 권한이 있는 사용자의 목록이 표시됩니다.
3 보호된 이메일에 더 이상 액세스하지 못하도록 하려면 개별 사용자를 제거합니다.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

자주 묻는 질문

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

기타 FAQ

질문

질문

컴퓨터의 이름을 변경했습니다. 그랬더니 정책 업데이트도 받지 못하고 암호화를 통한 클라우드 액세스도 불가능합니다.

답변

일반적으로, Dell Server는 사용자가 원래 등록된 끝점만 인식합니다. 이 끝점의 이름을 변경하면 Dell Server가 정책을 전송할 위치를 인식하지 못하여 Data Guardian이 예상대로 작업을 수행하지 못합니다.

해결 방법

Data Guardian을 제거한 다음에 다시 설치합니다. 삭제를 하려면 관리자 권한이 있어야 합니다.

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

Office 문서 및 보호 모드 FAQ

질문

Office 문서(.docx, .pptx, .xlsx, .docm, .pptm, .xlsm)를 열려고 시도했는데 표지 페이지가 표시되었습니다.

답변

관리자가 Office 문서를 보호하려는 정책을 설정하였다면 사용자나 사용자의 관리자가 Data Guardian을 설치해야 합니다. 알림 영역의 Data Guardian 아이콘에 활성화되어 있다는 것을 나타내는 녹색 확인 표시가 있는지 확인하십시오.

해결 방법

Data Guardian을 설치해야 하는지 활성화해야 하는지를 결정하십시오. Data Guardian 설치 또는 활성화와 관련하여 발생할 수 있는 문제를 참조하십시오.

질문

보호된 Office 문서(Word, PowerPoint 또는 Excel)를 열 수 없습니다.

답변

다음 사항을 확인하십시오.

- 파일 블록 설정 - 관리자가 Office 문서를 보호하기 위한 정책을 설정하는 경우에 **파일 > 옵션**에서 이 설정을 사용하지 마십시오.

해결 방법

파일 블록 설정을 확인하려면 다음을 수행하십시오.

1 Office 문서에서 **파일 > 옵션**을 선택합니다.
2 목록에서 **Trust Center**를 선택합니다.
3 오른쪽에서 **Trust Center 설정**을 클릭합니다.
4 목록에서 **파일 블록 설정**을 선택합니다.
5 *Word/Excel/PowerPoint 2007과 이후의 문서 및 템플릿*에 대하여 *열기* 확인란의 선택이 해제되어 있는지 확인합니다.
6 **확인**을 클릭합니다.