Dell Data Protection | Access 홈

Dell Data Protection | Access 홈 페이지는 이 응용 프로그램의 기능에 액세스할 수 있는 시작점입니다. 이 창에서 다음에 액세스할 수 있습니다.

System Access Wizard
액세스 옵션
Self-Encrypting Drive
고급 옵션

창의 맨 아래 오른쪽에 클릭하면 고급 옵션에 액세스할 수 있는 **고급** 링크가 있습니다.

고급 옵션에서 창의 맨 아래 오른쪽의 **홈** 링크를 클릭하면 홈 페이지로 돌아올 수 있습니다.

System Access Wizard

System Access Wizard는 처음 **Dell Data Protection | Access** 응용 프로그램이 실행되면 자동으로 실행됩니다. 이 마법사는 시스템에 로그인하는 방법(예: 암호만 또는 지문과 암호) 및 시기(Windows, pre-Windows 또는 둘 다)를 포함해 시스템에서 보안의 모든 측면을 설정할 수 있도록 안내합니다. 또한, 시스템에 Self-Encrypting Drive가 있는 경우 이 마법사를 통해 구성할 수 있습니다.

관리자 기능

시스템에서 Windows 관리자 권한을 통해 설정된 사용자는 **Dell Data Access | Protection** 에서 다음 기능을 수행할 권리를 가집니다. 단 표준 사용자는 할 수 없습니다.

- 시스템(Pre-Windows) 암호 설정/변경
- 하드 드라이브 암호 설정/변경
- 관리자 암호 설정/변경
- TPM 소유자 암호 설정/변경
- ControlVault 관리자 암호 설정/변경
- 시스템 재설정
- 자격 증명 보관 및 복원
- smartcard 관리자 PIN 설정/변경
- smartcard 지우기/재설정
- Windows에 Dell 보안 로그인 사용/사용 안 함
- Windows 로그인 정책 설정
- 다음을 포함한 Self-Encrypting Drive 관리
    - Self-Encrypting Drive 잠금 사용/사용 안 함
    - Windows 암호 동기화(WPS) 사용/사용 안 함
    - Single Sign On (SSO) 사용/사용 안 함
    - 암호화 정보 삭제 수행

원격 관리

귀하의 조직은 여러 플랫폼에 있는 **Dell Data Protection | Access** 응용 프로그램의 보안 기능이 중앙에서 관리(예: 원격 관리)되는 환경을 설정할 수 있습니다. 이러한 경우 Active Directory 와 같은 Windows 보안 인프라는 **Dell Data Protection | Access** 의 특정 기능을 안전하게 관리하는 데 사용할 수 있습니다.

컴퓨터가 원격에서 관리(예: 원격 관리자가 "소유")되는 경우 **Dell Data Protection | Access** 기능의 로컬 관리가 비활성화되어 응용 프로그램의 관리 창은 로컬에서 액세스할 수 없게 됩니다. 다음 기능에 대한 관리는 원격으로 수행할 수 없습니다.

- TPM(Trusted Platform Module)
- ControlVault
- Pre-Windows 로그인
- 시스템 재설정
- BIOS 암호
- Windows 로그인 정책
- Self-Encrypting Drive
- 지문 및 Smartcard 등록

원격 관리를 위해 Wave Systems의 EMBASSY® Remote Administration Server (ERAS) 사용에 대한 자세한 정보를 요청하려면 dell.com 으로 이동하십시오.

액세스 옵션

액세스 옵션 창에서 시스템에 액세스하는 방법을 설정할 수 있습니다.

Dell Data Protection | Access 옵션을 설정한 경우 사용 가능한 옵션(예: Pre-Windows 로그인을 위한 암호 변경)과 함께 홈 페이지에 표시됩니다. 사용 가능한 옵션은 바로 가기로서, 클릭하면 특정 작업(예: 사전 Windows 암호 변경 또는 다른 지문 등록)을 수행할 수 있는 해당 창으로 이동합니다.

일반

먼저, 로그인 시기(Windows, pre-Windows 또는 둘 다) 및 로그인 방법(예: 지문 및 암호)을 지정할 수 있습니다. 로그인 방법에는 지문, smartcard 및 암호 조합을 포함해 1 또는 2개의 옵션을 선택할 수 있습니다. 목록의 옵션은 사용자의 환경에서 적용되는 로그인 정책과 플랫폼에서 지원되는 로그인 방법에 따른 것입니다.

지문

시스템에 지문 판독기가 포함된 경우 시스템에 로그인하는 데 사용할 지문을 등록하거나 업데이트할 수 있습니다. 지문을 등록한 후에는 시스템의 지문 판독기에 등록된 지문을 문지르면 Windows, pre-Windows 또는 둘 다(일반 액세스 옵션에서 지정한 항목에 따라)로 시스템에 액세스할 수 있습니다. 자세한 내용은 사용자 지문 등록을 참조하십시오.

Pre-Windows 로그인

사용자가 pre-Windows에 로그인해야 하는 것으로 지정한 경우 pre-Windows 액세스를 위한 시스템 암호(pre-Windows 암호라고도 함)를 설정해야 합니다. 이 암호가 설정되면 관리자는 언제라도 암호를 변경할 수 있습니다.

또한, 이 화면에서 pre-Windows를 비활성화할 수도 있습니다. 현재 시스템 암호를 입력하고 암호가 정확한지 확인한 다음 **Disable** (비활성화) 단추를 클릭해야 합니다.

Smartcard

사용자가 로그인하려면 smartcard를 사용해야 하는 것으로 지정한 경우 하나 이상의 기존(접촉식) 또는 contactless smartcard를 등록해야 합니다. smartcard 등록 마법사를 실행하려면 **Enroll another smartcard** (다른 smartcard 등록) 링크를 클릭하십시오. 등록이란 로그인에 사용할 수 있도록 smartcard를 설정하는 것을 의미합니다.

smartcard를 등록한 후에는 **Change or setup my smartcard PIN** (내 smartcard PIN 변경 또는 설정) 링크를 사용해 해당 카드의 PIN을 변경하거나 설정할 수 있습니다.

Pre-Windows 로그인

pre-Windows 로그인이 설정되어 있는 경우 Windows가 로딩되기 전에 시스템이 켜지면 인증(암호, 지문 또는 smartcard)을 제공해야 합니다. pre-Windows 로그인 기능은 시스템에 추가 보안을 제공하여 권한이 없는 사용자가 Windows에 침입하여 컴퓨터에 액세스하지 못하게 합니다(컴퓨터가 도난 당한 경우 등).

Pre-Windows 로그인 창에서 관리자는 pre-Windows 로그인을 설정하거나 pre-Windows(시스템) 암호를 생성하거나 변경할 수 있습니다. 이 암호가 이미 설정되어 있는 경우 이 창에서 pre-Windows 로그인을 비활성화할 수 있습니다. pre-Windows 로그인을 설정하면 다음을 수행하는 마법사가 실행됩니다.

- 시스템 암호: pre-Windows 액세스를 위한 시스템 암호(또는 pre-Windows 암호)를 설정합니다. 이 암호는 사용자가 추가 인증 요소(예: 지문 센서에 문제가 있는 경우 시스템에 액세스하기 위한)를 가지고 있는 경우 백업으로 사용되기도 합니다.
- 지문 또는 Smartcard: pre-Windows 로그인에 사용할 수 있는 지문 또는 smartcard를 설정하며 이 인증 요소가 pre-Windows 암호 대신 또는 함께 사용할 수 있는지 지정합니다.
- Single Sign On: 기본적으로 pre-Windows 인증(암호, 지문 또는 smartcard)은 Windows에 자동으로 로그인하기 위해서도 사용됩니다. 이 기능을 비활성화하려면 "I want to login again at Windows"(Windows에 다시 로그인하고 싶습니다.) 확인란을 선택합니다.
- BIOS 하드 드라이브 암호가 pre-Windows 암호와 함께 설정된 경우 하드 드라이브 암호를 변경하거나 비활성화할 수 있는 옵션도 있습니다.

참고: pre-Windows 인증에 모든 지문 판독기를 사용할 수 있는 것은 아닙니다. 판독기가 호환되지 않는 경우 Windows 로그인에만 지문을 등록할 수 있게 됩니다. 특정 지문 판독기가 호환 가능한지 알아 보려면 시스템 관리자에게 문의하거나 support.dell.com 에서 지원되는 지문 판독기 목록을 참조하십시오.

Pre-Windows 로그인
또한, 이 창에서 pre-Windows를 비활성화할 수도 있습니다. 현재 pre-Windows(시스템) 암호를 입력하고 암호가 정확한지 확인한 다음 **Disable** (비활성화) 단추를 클릭해야 합니다. pre-Windows 로그인을 비활성화하면 등록된 모든 지문 또는 smartcard는 등록된 상태로 유지됩니다.

지문 등록

사용자는 pre-Windows 또는 Windows 로그인에 인증하는 데 사용할 수 있는 지문을 등록하거나 업데이트할 수 있습니다. Fingerprint(지문) 탭에서 손가락을 등록했던 손의 이미지가 표시됩니다. **Enroll another**(다른 지문 등록) 링크를 클릭하면 등록 과정을 안내하는 지문 등록 마법사가 실행됩니다. "등록"은 로그인에 사용할 지문을 저장하는 것을 의미합니다. 지문을 등록하려면 유효한 지문 판독기가 올바르게 설치 및 구성되어 있어야 합니다.

참고: pre-Windows 로그인에 모든 지문 판독기를 사용할 수 있는 것은 아닙니다. 호환되지 않는 판독기로 pre-Windows에 등록하려는 경우 오류 메시지가 나타납니다. 장치가 호환 가능한지 알아보려면 시스템 관리자에게 문의하거나 support.dell.com 에서 지원되는 지문 판독기 목록을 참조하십시오.

지문을 등록하면 사용자의 신원을 확인하기 위해 Windows 암호를 입력하라는 메시지가 나타납니다. 정책에서 요구하는 경우 Pre-Windows(시스템) 암호도 입력해야 합니다. 지문 판독기에 문제가 있는 경우 Pre-Windows 암호는 시스템에 액세스하기 위해 사용할 수 있습니다.

메모:

- 등록 작업 동안 적어도 두 개 이상의 지문을 등록하는 것이 좋습니다.
- 사용자는 지문 인증 기능을 활성화하기 전에 지문을 올바르게 등록해야 합니다.
- 시스템의 지문 판독기를 변경할 경우 새로운 판독기로 지문을 재등록해야 합니다. 두 개의 지문 판독기를 번갈아 사용하는 것은 권장되지 않습니다.
- 지문 등록 시 "센서의 초점이 상실됨" 메시지가 반복해서 나타나면 이 컴퓨터가 지문 판독기를 인식하지 못하고 있다는 것을 의미할 수 있습니다. 지문 판독기가 외장인 경우 지문 판독기를 뽑았다가 다시 연결하면 이 문제가 해결되는 경우도 있습니다.

등록된 지문 지우기

Remove fingerprint(지문 제거) 링크를 클릭하거나 지문 등록 마법사에서 등록된 지문을 클릭(선택 해제)하면 등록된 지문을 제거할 수 있습니다.

pre-Windows 인증에 지문을 등록한 특정 사용자를 제거하려면 관리자는 해당 사용자에 대해 등록된 모든 지문의 선택을 취소할 수 있습니다.

참고: 지문 등록 과정에 오류가 나타날 경우 wave.com/support/Dell에서 자세한 내용을 참조하십시오.

Smartcard 등록

Dell Data Protection | Access 에서는 Windows 계정에 로그인하거나 pre-Windows 에서 인증 시 기존(접촉식) 또는 contactless smartcard를 사용하는 옵션을 제공합니다. Smartcard 탭에서 등록 절차를 안내하는 Smartcard Enrollment 마법사를 실행하려면 **Enroll another smartcard** (다른 스마트 카드 등록) 링크를 클릭하십시오. "등록"이란 로그인에 사용할 수 있도록 smartcard를 설정하는 것을 의미합니다.

등록을 수행하려면 유효한 smartcard 인증 장치가 올바르게 설치 및 구성되어 있어야 합니다.

참고: 특정 장치가 호환 가능한지 알아 보려면 시스템 관리자에게 문의하거나 support.dell.com 에서 지원되는 smartcard 목록을 참조하십시오.

등록
smartcard를 등록하면 사용자의 신원을 확인하기 위해 Windows 암호를 입력하라는 메시지가 나타납니다. 정책에서 요구하는 경우 Pre-Windows(시스템) 암호도 입력해야 합니다. smartcard 판독기에 문제가 있는 경우 Pre-Windows 암호는 시스템에 액세스하기 위해 사용할 수 있습니다.

등록 중에 설정되어 있는 경우 smartcard PIN을 입력하라는 메시지가 나타납니다. 정책에서 PIN을 요청하지만 설정한 것이 없는 경우 하나를 만들라고 요청하는 메시지가 나타납니다.

메모:

- 사용자가 pre-Windows에서 smartcard 사용에 대해 등록된 후에는 제거할 수 없습니다.
- 표준 사용자는 smartcard에서 사용자 PIN을 변경할 수 있으며, 관리자는 관리자 PIN과 사용자 PIN을 모두 변경할 수 있습니다.
- 또한, 관리자는 smartcard를 재설정할 수도 있으며, 재설정된 smartcard는 다시 등록할 때까지 Windows 로그인 시 인증 또는 pre-Windows에 사용할 수 없습니다.

참고: TPM 인증서 인증의 경우 관리자는 Microsoft Windows smartcard 등록 과정을 통해 TPM 인증서를 등록할 수 있습니다. 관리자는 이 응용 프로그램과의 호환성을 위해 Smartcard CSP 대신 Cryptographic Service Provider로 "Wave TCG-Enabled CSP"를 선택해야 합니다. 또한, Dell 보안 로그인은 클라이언트에 적합한 인증 유형 정책으로 활성화되어야 합니다.

참고: Smartcard Service가 실행 중이 아니라는 오류 메시지가 나타날 경우 다음을 수행해 이 서비스를 시작/재시작할 수 있습니다.

- 제어판에서 관리 도구 창으로 이동한 다음 서비스를 선택하고 Smartcard를 오른쪽 버튼으로 클릭한 다음 시작 또는 다시 시작을 선택합니다.
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

Self-Encrypting Drive 개요

Dell Data Protection | Access는 데이터 암호화가 드라이브 하드웨어에 임베드되어 있는 Self-Encrypting Drive의 하드웨어 기반 보안 기능을 관리합니다. 이 기능은 드라이브 잠금이 활성화된 상태에서는 인증된 사용자만이 암호화된 데이터에 액세스할 수 있도록 보장하는 데 사용됩니다.

Self-Encrypting Drive 창은 **Self-Encrypting Drive** 아래 탭을 클릭하면 액세스됩니다. 이 탭은 하나 이상의 Self-Encrypting Drive(SED)가 시스템에 존재하는 경우에만 표시됩니다.

Self-Encrypting Drive 설정 마법사를 시작하려면 **Setup** (설정) 링크를 클릭합니다. 이 마법사에서 드라이브 관리자 암호를 생성하고, 이 암호를 백업하며 드라이브 암호화 설정을 적용합니다. 시스템 관리자만 Self-Encrypting Drive 설정 마법사에 액세스할 수 있습니다.

중요! 드라이브가 설정된 후에는 데이터 보호 및 드라이브 잠금이 "활성화"됩니다. 드라이브가 잠겨지면 다음 동작이 적용됩니다.

- 드라이브는 드라이브의 전원이 꺼질 때마다 *잠금* 모드가 됩니다.
- 드라이브는 사용자가 올바른 사용자 이름과 암호를 Pre-Windows 로그인 화면에 입력하지 않으면 부팅되지 않습니다. 드라이브 잠금이 활성화되기 전에 드라이브에 있는 데이터는 컴퓨터에 있는 모든 사용자가 액세스할 수 있습니다.
- 드라이브는 다른 컴퓨터에 보조 드라이브로 연결되어 있는 경우에도 보호되어 해당 드라이브 데이터에 액세스하려면 인증이 필요합니다.

드라이브가 설정되면 Self-Encrypting Drive 창에는 드라이브와 사용자가 드라이브 암호를 변경할 수 있는 링크가 표시됩니다. 드라이브 관리자인 경우 이 창에서 드라이브 사용자를 추가 또는 제거할 수도 있습니다. 설정된 외장 드라이브가 있는 경우 이 창에 표시되며 잠금을 해제할 수 없습니다.

참고: 보조 외장 드라이브를 잠그려면 드라이브는 컴퓨터와는 별도로 전원을 꺼야 합니다.

드라이브 관리자는 **고급>장치**에서 드라이브 설정을 변경할 수 있습니다. 자세한 내용은 드라이브 관리 - Self-Encrypting 드라이브를 참조하십시오.

드라이브 설정

Self-Encrypting Drive 설정 마법사는 드라이브 설정 단계를 안내합니다. 이 과정을 진행할 때 다음 개념을 기억하는 것이 중요합니다.

드라이브 관리자

드라이브 액세스를 설정(및 드라이브 관리자 암호 설정)한 시스템 관리자 권한을 가진 첫 번째 사용자가 드라이브 관리자가 되며, 드라이브 액세스에 변경 사항을 적용할 수 있는 유일한 사용자입니다. 첫 번째 사용자를 의도적으로 드라이브 관리자로 설정하기 위해서는 "I understand"(동의) 확인란을 선택해 이 단계를 계속해야 합니다.

드라이브 관리자 암호

마법사는 드라이브 관리자 암호를 만들고 확인으로 암호를 다시 입력하라는 메시지가 나타납니다. 드라이브 관리자 암호를 생성하려면 신원을 입증하기 위해 사용자의 Windows 암호를 입력해야 합니다. 현재 Winodws 사용자는 이 암호를 생성할 수 있는 관리자 권한입니다.

드라이브 자격 증명 백업
위치에 입력하거나 **찾아보기** 단추를 클릭해 위치를 선택하고 드라이브 관리자 자격 증명의 백업 사본을 저장합니다.

중요**!**

- 이러한 자격 증명을 백업할 때 기본 하드 드라이브가 아닌 드라이브(예: 이동식 미디어)에 백업하는 것이 좋습니다. 그렇지 않으면, 드라이브에 대한 액세스를 잃으면 백업에 액세스할 수 없게 됩니다.
- 드라이브 설정을 완료한 후에는 다음에 시스템 전원이 켜진 후에 시스템에 액세스하려면 사용자는 Windows가 로딩되기 전에 정확한 사용자 이름과 암호(또는 지문)를 입력해야 합니다.

드라이브 사용자 추가
드라이브 관리자는 유효한 Windows 사용자인 경우 다른 사용자를 드라이브에 추가할 수 있습니다. 드라이브에 사용자를 추가하면 관리자는 처음 로그인 시 사용자가 암호를 재설정해야 하는 옵션을 가집니다. 사용자는 pre-Windows 인증 화면에서 암호를 재설정해야 드라이브의 잠금이 해제됩니다.

고급 설정

- *Single Sign On* - 기본적으로 드라이브에 인증하기 위해 pre-Windows에 입력하는 Self-Encrypting Drive 암호는 Windows에 자동으로 로그인하는 데도 사용됩니다(일명 "Single Sign On"). 이 기능을 비활성화하려면 드라이브 설정 구성 시 "I want to login again when Windows starts"(Windows 시작 시 다시 로그인합니다) 확인란을 선택하십시오.
- *지문 로그인* - 지원되는 플랫폼에서 암호 대신 지문을 사용해 Self-Encrypting Drive에 인증하길 원하는지 지정할 수 있습니다.
- *절전/대기(S3) 지원*(플랫폼에서 지원되는 경우) - 활성화된 경우 Self-Encrypting Drive는 안전하게 절전/대기 모드(또는 S3 모드)로 전환되어 절전/대기 모드에서 재개 시 pre-Windows 인증이 필요하게 됩니다.

메모:

- S3 지원이 활성화된 경우 드라이브 암호화 암호는 BIOS 암호 제한(있는 경우)의 적용을 받습니다. 구체적인 BIOS 암호 제한에 대한 자세한 내용은 시스템 하드웨어 제조업체에 문의하십시오.
- 일부 Self-Encrypting Drive에서만 S3 모드를 지원합니다. 드라이브 설정 중에 드라이브가 대기/절전 모드를 지원하는지 여부를 알게 됩니다. 이 모드를 지원하지 않는 드라이브의 경우 최대 절전 모드가 활성화되어 있는 경우 Windows S3 요청은 자동으로 최대 절전 요청으로 전환됩니다(컴퓨터에서 최대 절전을 활성화하는 것이 좋습니다).
- SSO(Single Sign On) 옵션을 설정한 후 처음으로 로그인하면 이 프로세스는 Windows 로그인 프롬프트에서 일시 중지하게 됩니다. 이어서 사용자의 Windows 인증 양식을 입력하라는 화면이 나타나고, 입력된 내용은 이후의 Windows 로그인을 위해 안전하게 저장됩니다. 다음에 시스템이 재부팅되면 SSO를 통해 자동으로 Windows에 로그인하게 됩니다. 사용자의 인증(암호, 지문, Smartcard PIN)이 변경될 경우에도 동일한 과정이 필요합니다. 컴퓨터가 도메인에 있고 해당 도메인이 Windows 로그인을 위해 ctrl+alt+del을 눌러야 하는 정책이 있는 경우 이 정책이 존중됩니다.

주의! **Dell Data Protection | Access** 응용 프로그램을 제거할 경우 먼저 Self-Encrypting Drive 데이터 보호를 비활성화하고 드라이브의 잠금을 해제해야 합니다.

SED 사용자 기능

Self-Encrypting Drive 관리자는 드라이브 보안 및 사용자에 대한 모든 관리를 수행합니다. 드라이브 관리자가 아닌 드라이브 사용자는 다음 작업만을 수행할 수 있습니다.

- 본인의 드라이브 암호 변경
- 드라이브 잠금 해제

이러한 작업은 **Dell Data Protection | Access**의 **Self-Encrypting Drive** 탭에서 액세스 가능합니다.

암호 변경

등록된 사용자가 새 드라이브 인증 암호를 만들 수 있습니다. 드라이브 암호가 새 값으로 설정되기 전에 현재 Self-Encrypting Drive 암호를 입력해야 합니다.

메모:

- 이 응용 프로그램에서는 Windows 암호 길이 및 암호 복잡성 정책이 설정되어 있는 경우 이를 시행합니다. Windows 암호 정책이 설정되어 있지 않은 경우 Self-Encrypting Drive 암호의 최대 길이는 32자입니다. S3(절전/대기)이 활성화되어 있지 않은 경우 최대 길이는 127자입니다.
- 사용자의 Self-Encrypting Drive 암호는 Windows 암호와는 별개의 것입니다. 사용자의 Windows 암호를 변경하거나 재설정해도 Windows 암호 동기화가 활성화되어 있지 않은 경우 사용자의 드라이브 암호에는 영향을 미치지 않습니다. 자세한 내용은 장치: Self-Encrypting Drive 를 참조하십시오.
- 영문이 아닌 키보드의 경우 Self-Encrypting Drive 암호에는 사용할 수 없는 제한 문자 집합이 있습니다. Windows 암호에 제한된 문자가 포함되어 있고 Windows 암호 동기화가 활성화되어 있는 경우 동기화가 실패하고 오류 메시지가 나타납니다.

드라이브 잠금 해제

드라이브 잠금 해제는 등록된 드라이브 사용자가 잠긴 드라이브를 해제할 수 있습니다. 드라이브 잠금이 활성화되면 컴퓨터 전원이 꺼질 때마다 드라이브는 잠금 상태가 됩니다. 시스템에 다시 전원이 공급되면 pre-Windows 인증 화면에서 암호를 입력하여 드라이브에 인증해야 합니다.

메모:

- 컴퓨터에서 여러 사용자 계정이 동시에 활성화되어 있는 경우 절전 모드(예: 절전/대기 또는 최대 절전)로 들어가지 못할 수도 있습니다.
- pre-Windows 인증 화면에서 중국어, 일본어, 한국어 및 러시아어로 자국어 구현이 되어 있는 응용 프로그램 버전에서는 사용자 1, 사용자 2가 해당 드라이브 사용자 이름으로 대체됩니다.

고급 옵션

Dell Data Protection | Access 의 고급 옵션을 통해 관리자 권한을 가진 사용자는 응용 프로그램의 다음 측면을 관리할 수 있습니다.

유지 보수
암호
장치

참고: 관리자 권한을 가진 사용자만 고급 옵션에서 수정을 할 수 있으며, 표준 사용자는 이러한 설정을 볼 수는 있지만 변경 사항을 적용할 수는 없습니다.

유지 보수 개요

유지 보수 창은 관리자가 Windows 로그인 기본 설정을 설정하고 목적에 맞게 준비하도록 시스템을 재설정하거나 시스템의 보안 하드웨어에 저장된 사용자 자격 증명을 보관 또는 복원하기 위해 사용할 수 있습니다. 자세한 내용은 다음 항목을 참조하십시오.

액세스 기본 설정

액세스 기본 설정 창을 통해 관리자는 시스템의 모든 사용자를 위한 Windows 로그인 기본 설정을 지정할 수 있습니다.

Dell 보안 로그인 사용
표준 Windows ctrl-alt-delete 화면을 대체하는 옵션을 통해 Windows에 액세스하기 위해 Windows 암호 대신(또는 함께) 다른 요소의 인증 방법을 사용할 수 있습니다. Windows 로그인 프로세스의 보안을 강화하기 위해 두 번째 인증 요소로 지문을 추가하기로 선택할 수 있습니다. 또한, smartcard 또는 TPM 인증서를 포함해 Windows에 로그인하는 데 부가적인 인증 요소를 추가할 수 있습니다.

메모:

- Dell 보안 로그인을 사용하면 시스템의 모든 사용자에게 적용됩니다.
- 이 옵션은 사용자가 본인의 지문 또는 smartcard를 등록한 후에 사용하는 것이 좋습니다.
- 이 옵션이 설정된 후에 처음 로그인하면 표준 정책에 따라 Windows에 인증하라는 메시지가 나타나며 다음에 다시 시작할 때 새로운 인증 요소를 사용해야 합니다.

Dell 보안 로그인 사용 안 함
이 옵션은 Windows에 로그인하는 모든 **Dell Data Protection | Access** 기능을 비활성화합니다. 이 옵션을 선택하면 표준 Windows 로그인 정책으로 전환됩니다.

메모:

- 로그인을 시도할 때 보안 Windows 로그인에 관한 오류가 나타나면 Dell 보안 로그인 옵션을 비활성화하고 다시 활성화하십시오.
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

시스템 재설정

시스템 재설정 기능은 플랫폼에 있는 모든 보안 하드웨어에서 모든 사용자 데이터를 지우는 데 사용됩니다. 예를 들어, 컴퓨터를 재사용(repurposing)하기 위해 사용됩니다. 이 옵션은 하드웨어 장치(예: ControlVault, TPM 및 지문 판독기)에 있는 모든 데이터뿐만 아니라 Windows 사용자 암호를 제외한 시스템에 있는 모든 암호를 지웁니다. Self-Encrypting Drive의 경우 이 기능은 데이터 보호 기능을 해제하여 드라이브 데이터의 액세스가 가능합니다.

시스템을 재설정하고 있다는 것을 알고 있음을 확인한 다음 **다음**을 클릭합니다. 시스템을 재설정하려면 설정되어 있는 각 보안 장치에 대한 암호를 입력해야 합니다.

- TPM 소유자
- ControlVault 관리자
- BIOS 관리자
- BIOS 시스템(pre-Windows)
- 하드 드라이브(BIOS)
- Self-Encrypting Drive 관리자

참고: Self-Encrypting Drive의 경우 모든 드라이브 사용자의 암호가 아니라 드라이브 관리자 암호만 필요합니다.

중요! 시스템 재설정 시 삭제된 데이터를 복구하는 유일한 방법은 이전에 저장된 보관소에서 복원하는 것입니다. 보관소가 없는 경우 이 데이터는 복구할 수 없습니다. Self-Encrypting Drive의 경우 설정된 데이터만 삭제되고, 드라이브의 개인 데이터는 삭제되지 않습니다.

자격 증명 보관 및 복원

자격 증명 보관 및 복원 기능은 ControlVault 및 TPM(Trusted Platform Module)에 보관된 모든 사용자 자격 증명(로그인 및 암호화 정보)을 백업하고 복원하는 데 사용됩니다. 이 데이터의 백업은 하드웨어 오류 발생 시 컴퓨터를 재프로비저닝하거나 데이터를 복원할 때 중요합니다. 이 경우에는 저장된 보관 파일에서 새 컴퓨터로 모든 자격 증명을 간단하게 복원할 수 있습니다.

시스템의 단일 사용자 또는 여러 사용자를 위해 자격 증명을 보관 또는 복원하는 것을 선택할 수 있습니다.

사용자 자격 증명은 등록된 지문 및 smartcard 데이터, TPM에 저장된 키 등과 같이 pre-Windows에 사용된 데이터로 구성되어 있습니다. TPM은 보안 응용 프로그램의 요청에 따라 키를 생성합니다. 예를 들어, 디지털 인증서를 생성하면 TPM에 키가 생성됩니다.

참고: TPM 키가 **Dell Data Protection | Access**에서 보관될 수 있는지 확인하려면 보안 응용 프로그램의 설명서를 참조하십시오. 일반적으로 키를 생성하는 데 “Wave TCG-Enabled CSP”를 사용하는 응용 프로그램이 지원됩니다.

자격 증명 보관

자격 증명을 보관하려면 다음을 수행해야 합니다.

- 시스템에서 본인 또는 모든 사용자의 자격 증명을 보관할지 지정합니다.
- 시스템(pre-Windows) 암호, ControlVault 관리자 암호 및 TPM 소유자 암호를 입력하여 보안 하드웨어에 인증을 제공합니다.
- 자격 증명 백업 암호를 생성합니다.
- **찾아보기** 단추를 사용해 보관 암호를 지정합니다. 하드 드라이브 오류가 발생해도 안전하도록 보관 위치를 USB 플래시 드라이브나 네트워크 드라이브와 같은 이동식 미디어로 지정해야 합니다.

중요 참고:

- 사용자가 자격 증명 정보를 복원하는 데 이 정보가 필요할 수 있으므로 보관 장소를 기록합니다.
- 데이터를 복원할 수 있도록 자격 증명 백업 암호를 기록합니다. 이 암호는 복구할 수 없으므로 중요합니다.
- TPM 소유자 암호를 모르는 경우 시스템 관리자에게 문의하거나 컴퓨터의 TPM 설정 지침을 참조하십시오.

자격 증명 복원

자격 증명을 복원하려면 다음을 수행해야 합니다.

- 시스템에서 본인 또는 모든 사용자의 자격 증명을 복원할지 지정합니다.
- 보관 위치로 이동하고 보관 파일을 선택합니다.
- 보관 설정 시 생성된 자격 증명 백업 암호를 입력합니다.
- 시스템(pre-Windows) 암호, ControlVault 관리자 암호 및 TPM 소유자 암호를 입력하여 보안 하드웨어에 인증을 제공합니다.

메모:

- 자격 증명 복원에 실패했다는 오류 메시지가 나타나고 복원을 수행하기 위해 여러 번 시도한 경우 다른 보관 파일에 복원을 시도하십시오. 그래도 복원에 성공하지 못하면 다른 자격 증명 보관소를 생성하고 새로운 보관소에서 복원을 시도하십시오.

- TPM 키를 복원하지 못했다는 오류가 나타나면 자격 증명 보관소를 생성한 다음 BIOS에서 TPM을 지우십시오. TPM을 지우려면 컴퓨터를 재부팅하고 다시 시작하려고 할 때 **F2** 키를 눌러 BIOS 설정에 액세스한 다음 보안>TPM 보안으로 이동하십시오. 그런 다음 TPM 소유권을 재설정하고 자격 증명을 다시 복원하십시오.
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

암호 관리

암호 관리 창에서 관리자는 시스템에 있는 모든 보안 암호를 생성하거나 변경할 수 있습니다.

- 시스템(또는, Pre-Windows)*
- 관리자*
- 하드 드라이브*
- ControlVault
- TPM 소유자
- TPM 마스터
- TPM Password Vault
- Self-Encrypting Drive

메모:

- 현재 플랫폼 구성에 해당하는 암호만 표시할 수 있습니다. 따라서 이 창은 시스템 구성 및 상태에 따라 변경됩니다.
- 위에서 별표(*)가 있는 암호는 BIOS 암호이며, 시스템 BIOS를 통해서 변경할 수도 있습니다.
- BIOS 관리자가 암호 변경 사항을 거부한 경우 BIOS 수준의 암호는 생성하거나 변경할 수 없습니다.
- Self-Encrypting Drive의 **setup** (설정) 링크를 클릭하면 Self-Encrypting Drive Setup Wizard가 실행되며, **manage** (관리)를 클릭하면 사용자는 하나 이상의 Self-Encrypting Drive 암호를 변경할 수 있습니다.
- TPM Password Vault에 대한 **manage** (관리) 링크를 클릭하면 TPM 키를 보호하는 암호를 보거나 변경할 수 있는 창이 표시됩니다. 암호가 필요한 TPM 키가 생성되면, 암호가 무작위로 생성되어 볼트에 저장됩니다. 사용자는 TPM 마스터 암호를 생성할 때까지 TPM 암호를 관리할 수 없습니다.

Windows 암호 복잡성 규칙

Dell Data Protection | Access 는 다음 암호가 시스템의 Windows 암호 복잡성 규칙을 준수하도록 보장합니다.

- TPM 소유자 암호

시스템의 Windows 암호 복잡성 규칙을 확인하려면 다음 단계를 따르십시오.

1. 제어판에 액세스합니다.
2. 관리 도구를 두 번 클릭합니다.
3. 로컬 보안 정책을 두 번 클릭합니다.
4. 계정 정책을 확대한 후 암호 정책을 선택합니다.

장치 개요

장치 창은 관리자가 시스템에 설치되어 있는 모든 보안 장치를 관리하기 위해 사용합니다. 각 장치에 대한 상태와 펌웨어 버전과 같은 추가 상세 정보를 볼 수 있습니다. 각 장치의 정보를 보려면 **표시**를 클릭하고 섹션을 축소하려면 **숨기기**를 클릭하십시오. 관리할 수 있는 장치는 플랫폼에 포함된 것에 따라 다음과 같습니다.

TPM(Trusted Platform Module)
ControlVault®
Self-Encrypting Drive
인증 장치 정보

TPM(Trusted Platform Module)

Dell Data Protection | Access 및 TPM을 통해 제공되는 고급 보안 기능을 사용하려면 TPM 보안 칩이 활성화되어 있어야 하며 TPM의 소유권이 설정되어 있어야 합니다.

장치 관리의 Trusted Platform Module 창은 시스템에서 TPM이 감지된 경우에만 표시됩니다.

TPM 관리
이 기능을 통해 시스템 관리자는 TPM을 관리할 수 있습니다.

상태
TPM의 상태를 *active*(활성) 또는 *inactive*(비활성)로 표시합니다. "Active"(활성) 상태는 TPM이 BIOS에서 활성화되어 설정할 준비가 되어 있다는 것을 의미합니다(예: 소유권을 가져올 수 있음). TPM이 활성화되어 있지 않은 경우 TPM은 관리할 수 없으며 보안 기능에 액세스할 수 없습니다.

TPM이 시스템에서 감지되지만 활성화되어 있지 않은 경우 시스템 BIOS에 들어가지 않고 이 창에서 **activate** (활성화) 링크를 클릭하면 활성화할 수 있습니다. 이 기능을 이용해서 TPM을 활성화시킨 다음에는 컴퓨터를 재부팅해야 합니다. 재부팅하는 동안 변경 사항을 적용할지 묻는 메시지가 표시될 수도 있습니다.

참고: 이 응용 프로그램에서 TPM을 활성화할 수 있는 기능은 모든 플랫폼에서 지원되는 것은 아닙니다. 지원되지 않는 경우 시스템 BIOS에서 활성화해야 합니다. 이 작업을 수행하려면 시스템을 재부팅하고 Windows가 로딩되기 전에 **F2** 키를 눌러 BIOS 설정에 들어가서 보안>TPM 보안으로 이동한 다음 TPM을 활성화하십시오.

deactivate (비활성화) 링크를 클릭하면 여기서도 TPM을 *비활성화*할 수 있습니다. TPM을 비활성화하면 고급 보안 기능을 사용할 수 없게 됩니다. 단, 비활성화해도 TPM 설정을 변경하거나 TPM에 저장된 정보 또는 키를 삭제하거나 변경하지 않습니다.

소유됨
소유권(예: "소유됨")의 상태를 표시하여 TPM 소유자를 설정하거나 변경할 수 있습니다. 보안 기능을 사용하려면 TPM 소유권을 설정해야 합니다. 소유권을 설정하기 전에 TPM를 활성화해야 합니다.

소유권을 설정하는 과정은 TPM 소유권 암호를 생성하는 사용자(관리자 권한을 가진)로 구성됩니다. 이 암호를 정의하면 소유권이 설정되고 TPM을 사용할 수 있게 됩니다.

참고: TPM 소유자 암호는 시스템의 Windows 암호 복잡성 규칙을 따라야 합니다.

중요! Dell Data Protection | Access 에서 고급 보안 기능에 액세스하기 위해 필요하므로 TPM 소유자 암호를 분실하거나 잊어버리지 않는 것이 중요합니다.

잠김
TPM의 상태를 *locked*(잠김) 또는 *unlocked*(잠김 해제)로 표시합니다. "잠금"은 TPM의 보안 기능입니다. TPM은 정해진 횟수만큼 TPM 소유자 암호를 잘못 입력하면 잠금 상태가 됩니다. TPM 소유자는 여기에서 TPM의 잠금을 해제할 수 있습니다. TPM 소유자 암호 입력이 필요합니다.

메모:

- TPM의 소유권을 설정할 수 없다는 오류 메시지가 나타날 경우 시스템 BIOS에서 TPM을 지운 다음 소유권을 다시 설정해 보십시오. TPM을 지우려면 컴퓨터를 재부팅하고 다시

시작하려고 할 때 **F2** 키를 눌러 BIOS 설정에 액세스한 다음 보안 >TPM 보안으로 이동하십시오.

- TPM 소유자 암호를 변경할 수 없다는 오류 메시지가 나타나면 TPM 데이터(자격 증명 보관소)를 보관하고 BIOS에서 TPM을 지우고 TPM의 소유권을 다시 설정한 다음 TPM 데이터를 복원하십시오(자격 증명 복원).
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

Dell ControlVault®

Dell ControlVault®(CV)는 pre-Windows 로그인 동안 사용된 사용자 자격 증명(예: 사용자 암호 또는 등록된 지문 데이터)을 위한 안전한 하드웨어 저장소입니다. **장치 관리**의 ControlVault 창은 시스템에서 ControlVault가 감지된 경우에만 표시됩니다.

ControlVault 관리

다음 기능을 통해 시스템 관리자는 시스템의 ControlVault를 관리할 수 있습니다.

상태

ControlVault의 상태를 *active* (활성) 또는 *inactive*(비활성)로 표시합니다. "inactive"(비활성) 상태는 ControlVault를 시스템의 보관에 사용할 수 없다는 것을 의미합니다. 시스템에 ControlVault가 있는지 확인하려면 Dell 시스템 문서를 참조하십시오.

암호

ControlVault 관리자 암호가 설정되어 있는지 나타내며 암호를 설정하거나 변경(이미 설정한 경우)할 수 있습니다. 시스템 관리자만 이 암호를 설정하거나 변경할 수 있습니다. 다음을 수행하려면 ControlVault 관리자 암호를 설정해야 합니다.

- 자격 증명 보관 또는 복원을 수행합니다.
- 사용자 데이터(모든 사용자)를 지웁니다.

참고: ControlVault 관리자 암호가 설정되어 있지 않을 때 보관 또는 복원을 시도하면 관리자인 경우 암호를 생성하라는 메시지가 나타납니다.

등록된 사용자

사용자가 현재 ControlVault에 저장되어 있는 로그인 자격 증명(예: 암호, 지문 또는 smartcard 데이터)을 가지고 있는지 나타냅니다.

사용자 데이터 지우기

ControlVault의 데이터는 어느 시점(예: 사용자가 인증에 사용할 pre-Windows 자격 증명을 사용하거나 등록하는 데 문제가 있는 경우)에서는 지워야 할 필요가 있습니다. 단일 사용자 또는 여러 사용자에 대한 ControlVault에 저장된 모든 데이터는 이 창에서 지울 수 있습니다.

플랫폼에서 모든 사용자 데이터를 지우려면 ControlVault 관리자 암호를 입력해야 합니다. 또한, pre-Windows 자격 증명이 등록되어 있는 경우 시스템(pre-Windows) 암호를 입력하라는 메시지가 나타납니다. 모든 사용자 데이터를 지우면 ControlVault 관리자 암호 및 시스템 암호는 재설정됩니다. 하지만, 이 방법은 ControlVault 관리자 암호를 지우는 유일한 방법이라는 점을 명심하십시오.

참고: 모든 사용자 데이터를 지우면 컴퓨터를 재부팅하라는 메시지가 나타납니다. 시스템이 제대로 기능하려면 재부팅하는 것이 중요합니다.

ControlVault 관리자 암호는 단일 사용자의 자격 증명을 지우기 위해 설정할 필요가 없습니다. **사용자 데이터 지우기**를 클릭하면 지우려는 ControlVault 자격 증명을 가지고 있는 사용자를 선택하라는 메시지가 나타납니다. 사용자를 선택하고 나면 시스템 암호를 입력하라는 메시지가 나타납니다(pre-Windows 자격 증명이 등록된 경우에만).

메모:

- ControlVault 관리자 암호를 생성할 수 없다는 오류 메시지가 나타나면 자격 증명을 보관하고 ControlVault에서 모든 사용자 데이터를 지우며 컴퓨터를 재부팅하고 암호를 다시 생성해 보십시오.
- 단일 사용자에 대해 ControlVault에서 자격 증명을 지울 수 없다는 오류 메시지가 나타나면 자격 증명을 보관하고 모든 사용자 데이터를 지운 다음 해당 단일 사용자에 대한 데이터를 다시 지워 보십시오.
- 모든 사용자에 대해 ControlVault에서 자격 증명을 지울 수 없다는 오류 메시지가 나타나면 시스템 재설정을 시도해 보십시오. **중요!** 모든 사용자 보안 데이터를 지우게 되므로 재설정을 수행하기 전에 시스템 재설정 도움말 항목을 검토하십시오.
- ControlVault 및 TPM 데이터를 백업할 수 없다는 오류 메시지가 나타나면 시스템 BIOS에서 TPM을 비활성화하십시오. 이 작업은 컴퓨터를 재부팅하고 백업을 시작하여 BIOS 설정에 액세스하려고 할 때 **F2** 키를 누른 다음 >TPM 보안으로 이동하면 수행됩니다. 그런 다음 TPM을 재활성화하고 ControlVault 데이터를 다시 보관하십시오.
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

Self-Encrypting Drive: 고급

Dell Data Protection | Access 는 데이터 암호화가 드라이브 하드웨어에 임베드되어 있는 Self-Encrypting Drive의 하드웨어 기반 보안 기능을 관리합니다. 이 관리 기능은 드라이브 잠금이 활성화된 상태에서는 인증된 사용자만이 암호화된 데이터에 액세스할 수 있도록 보장하는 데 사용됩니다.

Device Management (장치 관리)의 Self-Encrypting Drive 창은 하나 이상의 SED(Self-Encrypting Drive)가 시스템에 존재하는 경우에만 표시됩니다.

중요! 드라이브가 설정된 후에는 Self-Encrypting Drive 데이터 보호 및 드라이브 잠금이 "활성화"됩니다.

드라이브 관리
이 기능을 통해 드라이브 관리자는 드라이브 보안 설정을 관리할 수 있습니다. 드라이브 보안 설정을 변경한 경우 드라이브를 껐다 켜야 변경 내용이 적용됩니다.

데이터 보호
Self-Encrypting Drive의 데이터 보호 상태를 *enabled*(활성) 또는 *disabled*(비활성)로 표시합니다. "enabled"(활성화) 상태는 드라이브 보안이 설정되었음을 의미하지만, 드라이브 *잠금*이 설정될 때까지는 사용자가 pre-Windows에서 액세스 시 드라이브에 인증할 필요가 없습니다.

여기에서 Self-Encrypting Drive 데이터 보호를 비활성화할 수 있습니다. 비활성화되면 Self-Encrypting Drive의 모든 고급 보안 기능은 해제되고 드라이브는 독립 실행형 드라이브로 실행됩니다. 데이터 보호를 비활성화하면 드라이브 관리자 및 드라이브 사용자의 자격 증명과 같은 모든 보안 설정을 삭제하기도 합니다. 하지만, 이 기능은 드라이브의 사용자 데이터를 변경하거나 제거하지 않습니다.

잠금
Self-Encrypting Drive에 대해 *enabled*(활성) 또는 *disabled*(비활성) 상태를 표시합니다. 잠긴 드라이브 동작에 대한 자세한 내용은 Self-Encrypting Drive 항목을 참조하십시오.

여기서 일시적으로 드라이브 잠금을 비활성화하는 것이 필요할 수 있습니다. 이 방법은 드라이브 잠금이 비활성화되어 있는 경우 드라이브에 액세스하는 데 자격 증명이 필요하지 않아 모든 플랫폼 사용자가 드라이브 데이터에 액세스할 수 있게 되므로 권장되지 않습니다. 드라이브 잠금을 비활성화하면드라이브 관리자 및 드라이브 사용자의 자격 증명 또는 드라이브에 있는 사용자 데이터를 포함해 모든 보안 설정을 삭제하지는 않습니다.

주의! Dell Data Protection | Access 응용 프로그램을 제거할 경우 먼저 Self-Encrypting Drive 데이터를 비활성화하고 드라이브의 잠금을 해제해야 합니다.

드라이브 관리자
현재 드라이브 관리자를 표시합니다. 드라이브 관리자는 여기에서 드라이브 관리자인 사용자를 변경할 수 있습니다. 새로운 관리자는 시스템에서 관리자 권한을 가진 유효한 Windows 사용자여야 합니다. 시스템에는 하나의 드라이브 관리자만 있을 수 있습니다.

드라이브

등록된 드라이브 사용자와 현재 등록된 사용자 수를 표시합니다. 지원되는 최대 사용자 수는 Self-Encrypting Drive(현재 Seagate 드라이브의 경우 4명의 사용자, Samsung 드라이브의 경우 24명의 사용자)에 따라 다릅니다.

Windows 암호 동기화

Windows 암호 동기화(WPS) 기능은 사용자의 Self-Encrypting Drive 암호를 Windows 암호와 동일하게 자동 설정합니다. 이 기능은 드라이브 관리자에게는 사용될 수 없으며 드라이브 사용자에만 사용할 수 있습니다. WPS 기능은 암호를 일정한 간격(예: 90일 간격)으로 변경해야 하는 엔터프라이즈 환경에서 사용할 수 있습니다. 이 옵션이 활성화되어 있는 경우 이러한 Windows 암호가 변경되면 모든 사용자의 Self-Encrypting Drive 암호가 자동으로 업데이트됩니다.

참고: Windows 암호 동기화(WPS)가 활성화되면 사용자의 Self-Encrypting Drive 암호는 변경할 수 없으며, 드라이브 암호가 자동으로 업데이트되게 하려면 해당 Windows 암호를 변경해야 합니다.

마지막 기억 사용자 이름

이 옵션이 활성화되면 입력한 마지막 사용자 이름은 pre-Windows 인증 화면의 **Username**(사용자 이름) 필드에 기본으로 표시됩니다.

사용자 이름 선택

이 옵션이 활성화되면 사용자는 pre-Windows 인증 화면의 **Username**(사용자 이름) 필드에서 모든 드라이브 사용자 이름을 볼 수 있습니다.

암호화 정보 삭제

이 옵션은 Self-Encrypting Drive에 있는 모든 데이터를 "삭제"하기 위해 사용할 수 있으며, 실제로 데이터를 삭제하는 것이 아니라 데이터를 암호화하기 위해 사용한 키를 삭제하여 해당 데이터를 사용할 수 없게 만드는 것입니다. 암호화 정보 삭제 후에는 드라이브 데이터를 복구할 방법이 없으며, Self-Encrypting Drive 데이터 보호는 비활성화되어 드라이브는 재사용할 준비가 됩니다.

메모:

- Self-Encrypting Drive 관리 기능과 관련된 오류가 나타날 경우 컴퓨터를 완벽하게 종료(재부팅 아님)하고 다시 시작하십시오.
- 특정 오류 메시지에 대한 보다 상세한 정보를 원하는 경우 wave.com/support/Dell 로 이동하십시오.

인증 장치 정보

장치 관리에서 인증 장치 정보 창은 시스템에서 연결된 모든 인증 장치(예: 지문 판독기, 기존 또는 contactless smartcard 판독기)의 정보 및 상태를 표시합니다.

기술 지원

Dell Data Protection | Access 소프트웨어에 대한 기술 지원은 http://www.wave.com/support.dell.com 에서 확인하십시오.

Wave TCG-Enabled CSP

Wave Systems TCG(Trusted Computing Group)-Enabled CSP(Cryptographic Service Provider)는 **Dell Data Protection | Access** 응용 프로그램에 포함되어 있으며 응용 프로그램에서 직접 호출되거나 설치된 CSP 목록에서 선택 가능한 방식으로 CSP가 필요할 때마다 사용 가능합니다. 가능한 경우 TPM이 키를 생성하도록 보장하고 키와 암호를 **Dell Data Protection | Access** 에서 관리하게 하려면 “Wave TCG-Enabled CSP"를 선택하십시오.

Wave Systems TCG-enabled CSP는 응용 프로그램에 MSCAPI를 통해 직접 TCG 호환 플랫폼에서 제공되는 기능을 사용하도록 지원합니다. TCG-Enhanced MSCAPI CSP 모듈은 TSS(Trusted Software Stack) 공급자와 관련된 공급업체별 요건과 상관 없이 TPM의 비대칭 키 기능을 제공하고 TPM에서 제공하는 강화된 보안 기능을 활용합니다.

참고: Wave TCG-enabled CSP에서 생성된 TPM 키가 암호를 요청하고 사용자가 TPM 마스터 암호를 생성한 경우 각 키의 암호는 무작위로 생성되어 TPM 암호 볼트에 저장됩니다.