Dell Data Protection | Security Tools

Installation Guide v1.10.1

범례

주의: 주의 아이콘은 지시를 따르지 않을 경우 하드웨어 손상 또는 데이터 손실의 가능성이 있음을 나타냅니다.

경고: 경고 아이콘은 재산 피해, 신체 상해 또는 사망의 가능성이 있음을 나타냅니다.

중요, 참고, 팁, 모바일, 또는 비디오: 정보 아이콘은 도움이 되는 정보를 나타냅니다.

Security Tools Installation Guide
2016 - 09

개정 A00

목차

1

소개

Dell Data Protection | Security Tools는 Dell 컴퓨터 관리자 및 사용자에게 보안 및 ID 보호를 제공합니다. DDP | Security Tools는 모든 Dell Latitude, Optiplex, Precision 컴퓨터와 일부 Dell XPS 노트북에 사전 설치되어 있습니다. DDP | Security Tools를 *재설치*해야 할 경우 이 안내서의 지침을 따르십시오. 추가 지원이 필요하면 www.dell.com/support > Endpoint Security Solutions를 참조하십시오.

개요

DDP | Security Tools는 고급 인증 지원과 자체 암호화 드라이브의 관리 및 PBA(부팅 전 인증) 지원을 제공하도록 설계된 종단 간 보안 솔루션입니다.

DDP | Security Tools는 암호, 지문 판독기 및 스마트 카드("비접촉식" 및 "접촉식" 모두)를 이용한 다단계 Windows 인증은 물론이고 자체 등록, 원-스텝 로그온(Single Sign-On[SSO]), 및 One-time Passwords(OTP)까지 지원합니다.

관리자는 최종 사용자에게 Security Tools를 지원하기 전에 DDP Security Console의 관리자 설정 도구를 사용해 부팅 전 인증 및 인증 정책을 활성화하는 등 Security Tools 기능을 구성할 수 있습니다. 하지만 기본 설정이 되어 있기 때문에 관리자나 사용자 모두 설치 및 활성화 후 바로 Security Tools를 사용하는 데 문제는 없습니다.

DDP Security Console

DDP Security Console은 관리자가 설정한 정책에 따라 사용자가 자신의 자격 증명을 등록 및 관리하고 자체 복구 질문을 구성할 수 있는 Security Tools 인터페이스입니다. 사용자는 다음과 같은 Security Tools 응용 프로그램에 액세스할 수 있습니다.

- 암호화 도구는 사용자가 컴퓨터 드라이브의 암호화 상태를 볼 수 있는 응용 프로그램입니다.
- 등록 도구는 사용자가 자격 증명을 설정 및 관리하거나, 자체 복구 질문을 구성하거나, 자신의 자격 증명 등록 상태를 볼 수 있는 응용 프로그램입니다. 이러한 권한은 관리자가 설정한 정책을 따릅니다.
- Password Manager는 사용자가 웹 사이트, Windows 응용 프로그램 및 네트워크 리소스에 로그온하는 데 필요한 데이터를 자동으로 입력하여 제출할 수 있는 응용 프로그램입니다. 또한 이 응용 프로그램을 통해 로그온 암호를 변경하고 Password Manager에서 유지 관리하는 암호가 대상 리소스와 동기화되도록 유지할 수 있습니다.

관리자 설정

관리자 설정 도구는 모든 컴퓨터 사용자에게 필요한 Security Tools를 구성하는 데 사용되며, 이를 통해 관리자는 인증 정책을 설정하거나, 사용자를 관리하거나, Windows 로그온 시 사용할 자격 증명을 구성할 수 있습니다.

관리자가 암호화 및 PBA(부팅 전 인증)를 활성화하거나, PBA 정책을 구성하거나, PBA 화면 텍스트를 사용자 지정할 수 있는 것도 이 도구 덕분입니다.

요구 사항으로 계속하십시오.

2

요구 사항

- DDP | Security Tools는 모든 Dell Latitude, Optiplex, Precision 컴퓨터와 일부 Dell XPS 노트북에 사전 설치되어 있으며 다음 최소 요구 사항을 충족합니다. DDP | Security Tools를 다시 설치할 경우 컴퓨터가 여전히 이러한 요구 사항을 충족하는지 확인하십시오. 자세한 내용은 www.dell.com/support > Endpoint Security Solutions를 참조하십시오.
- Windows 8.1은 자체 암호화 드라이브의 드라이브 1에 설치해서는 안 됩니다. Windows 8.1이 복구 파티션 드라이브 0을 만들면 부팅 전 인증을 위반하므로 이 운영 체제 구성은 지원되지 않습니다. 대신 드라이브 0으로 구성된 드라이브에 Windows 8.1을 설치하거나 임의의 드라이브에 대한 이미지로 Windows 8.1을 복원합니다.
- DDP | Security Tools는 동적 디스크를 지원하지 않습니다.
- 자체 암호화 드라이브가 장착된 컴퓨터에는 Hardware Crypto Accelerator를 사용할 수 없습니다. HCA의 프로비저닝을 방지하는 비호환성이 있습니다. Dell에서 판매하는 컴퓨터에는 HCA 모듈을 지원하는 자체 암호화 드라이브가 장착되어 있지 않습니다. 이 지원되지 않는 구성은 애프터마켓 구성입니다.
- DDP | Security Tools는 멀티 부팅 디스크 구성을 지원하지 않습니다.
- 클라이언트에 새 운영 체제를 설치하기 전에 BIOS에서 TPM(Trusted Platform Module)을 지웁니다.
- SED는 고급 인증이나 암호화를 제공하기 위해 TPM이 필요하지 않습니다.

Drivers

- Supported Opal compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

ⓘ **중요:**

Due to the nature of RAID and SEDs, SED management does not support RAID. The issue with "RAID=On" with SEDs is that RAID requires access to the disk to read and write RAID-related data at a high sector not available on a locked SED from start and cannot wait to read this data until after the user is logged on. Change the SATA operation in the BIOS from "RAID=On" to "AHCI" to resolve the issue. If the operating system does not have the AHCI controller drivers pre-installed, the operating system will blue screen when switched from "RAID=On" to "AHCI."

Client Prerequisites

- The full version of Microsoft .Net Framework 4.5 (or later) is required for Security Tools. All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5. However, if you are not installing on Dell hardware or are upgrading Security Tools on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version, prior to installing Security Tools to prevent installation/upgrade failures. To install the full version of Microsoft .Net Framework 4.5, go to https://www.microsoft.com/en-us/download/details.aspx?id=30653

  To verify the version of .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- Drivers and firmware for your authentication hardware must be up-to-date on your computer. To obtain drivers and firmware for Dell computers, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model. Based on your authentication hardware, download the following:
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smartcard Driver
  - Dell ControlVault

Other hardware vendors may require their own drivers.

The installer installs this component if not already installed on the computer:

Prerequisites

- Microsoft Visual C++ 2012 Update 4 or later Redistributable Package (x86/x64)

Software

Windows Operating Systems

The following table details supported software.

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 7 SP0-SP1

  - Enterprise

  - Professional

  ⓘ | 노트: Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.

- Microsoft Windows 8

  - Enterprise

  - Pro

  - Windows 8 (Consumer)

  ⓘ | 노트: Windows 8 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 8.1 - 8.1 Update 1

  - Enterprise Edition

  - Pro Edition

  ⓘ | 노트: Windows 8.1 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 10
  - Education Edition
  - Enterprise Edition
  - Pro Edition

ⓘ | 노트: Windows 10 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

Mobile Device Operating Systems

The following mobile operating systems are supported with Security Tools One-time Password feature.

Mobile Device Operating Systems

Android Operating Systems

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS Operating Systems

- iOS 7.x
- iOS 8.x

Windows Phone Operating Systems

- Windows Phone 8.1
- Windows 10 Mobile

Hardware

Authentication

The following table details supported authentication hardware.

Authentication

Fingerprint Readers

- Validity VFS495 in Secure Mode
- Broadcom Control Vault Swipe Reader
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Authentec Eikon and Eikon To Go USB Readers

ⓘ | 노트: When using an external fingerprint reader, you must download and install the latest drivers required for your specific reader.

Contactless Cards

- Contactless Cards using Contactless Card Readers built-in to specified Dell laptops

Smart Cards

- PKCS #11 Smart cards using the ActivIdentity client

ⓘ | 노트: The ActivIdentity client is not pre-loaded and must be installed separately.

- Common Access Cards (CAC)

Authentication

ⓘ | 노트: With multi-cert CACs, at logon, the user selects the correct certificate from a list.

- CSP Cards
- Class B/SIPR Net Cards

The following table details Dell computer models supported with SIPR Net cards.

Dell Computer Models - Class B/SIPR Net Card Support

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Dell Computer Models - UEFI Support

Authentication features are supported with UEFI mode on select Dell computers running Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 with qualified Opal Compliant SEDs. Other computers running Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 support Legacy Boot mode.

The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- Optiplex 3240 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

ⓘ | 노트: Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.

노트: On a supported UEFI computer, after selecting **Restart** from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture. Some models display the PBA logon screen; other models display the Windows logon screen. Both logon screens are equally secure.

노트:

Ensure that the Enable Legacy Option ROMs setting is disabled in the BIOS.

To disable Legacy Option ROMs:

1 Restart the computer.
2 As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.
3 Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.
4 Select **Settings** > **General** > **Advanced Boot Options**.
5 Clear the **Enable Legacy Option ROMs** checkbox and click **Apply**.

Opal Compliant SEDs

For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

International Keyboards

- The following table lists international keyboards supported with Preboot Authentication.

노트: These keyboards are supported ***with UEFI only***.

International Keyboard Support - UEFI
• DE-CH - Swiss German
• DE-FR - Swiss French

Language Support

DDP | Security Tools is Multilingual User Interface (MUI) compliant and supports the following languages.

노트:

PBA localization is not supported in Russian, Traditional Chinese, or Simplified Chinese on UEFI computers..

Language Support	
• EN - English	• KO - Korean
• FR - French	• ZH-CN - Chinese, Simplified
• IT - Italian	• ZH-TW - Chinese, Traditional/Taiwan
• DE - German	• PT-BR - Portuguese, Brazilian
• ES - Spanish	• PT-PT - Portuguese, Portugal (Iberian)

Language Support

- JA - Japanese
- RU - Russian
- RU - Russian

Authentication Options

The following authentication options require specific hardware: Fingerprints, Smart Cards, Contactless Cards, Class B/SIPR Net Cards, and **authentication on UEFI computers**.

The One-time Password feature requires that a TPM is present, enabled, and owned. For more information, see Clear Ownership and Activate the TPM. OTP is not supported with TPM 2.0.

The following tables show authentication options available with Security Tools, by operating system, when hardware and configuration requirements are met.

Non-UEFI

	PBA					Windows Authentication				
	Password	**Fingerprint**	**Contacted Smart card**	**OTP**	**SIPR Card**	**Password**	**Fingerprint**	**Smart card**	**OTP**	**SIPR Card**
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

1. Available with a supported Opal SED.

UEFI

	PBA - on supported Dell computers					Windows Authentication				
	Password	**Fingerprint**	**Contacted Smart card**	**OTP**	**SIPR Card**	**Password**	**Fingerprint**	**Smart card**	**OTP**	**SIPR Card**
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. Available with a supported OPAL SED on supported UEFI computers.

상호 운용성

Dell Data Protection | Access 프로비저닝 해제 및 제거

컴퓨터에 DDP|A가 현재 설치되어 있거나 이전에 설치되어 있던 경우 Security Tools를 설치하기 **전에** DDP|A로 관리되는 하드웨어를 프로비저닝 해제한 후 DDP|A를 제거해야 합니다. DDP|A가 사용되지 않은 경우, DDP|A를 제거하고 설치 프로세스를 다시 시작합니다.

DDP|A로 관리되는 하드웨어를 프로비저닝 해제할 경우 지문 판독기, 스마트 카드 판독기, BIOS 암호, TPM, 자체 암호화 드라이브도 프로비저닝 해제됩니다.

: DDP|E encryption 제품을 실행 중인 경우 암호화 스윕을 중지 또는 일시 중지하십시오. Microsoft BitLocker를 실행 중인 경우 암호화 정책을 일시 중지하십시오. DDP|A가 제거되었고 Microsoft BitLocker 정책 일시 중지가 해제된 경우 http://technet.microsoft.com/en-us/library/cc753140.aspx에 나와 있는 지침에 따라 TPM을 초기화하십시오.

DDP|A로 관리되는 하드웨어 프로비저닝 해제

DDP|A를 시작하고 **Advanced(고급)** 탭을 클릭합니다.

시스템 재설정을 선택합니다. 이때 프로비저닝된 자격 증명을 입력하여 ID를 확인해야 합니다. DDP|A에서 자격 증명을 확인하면 다음 작업이 수행됩니다.

Dell ControlVault에서 프로비저닝된 모든 자격 증명 제거(있는 경우)

Dell ControlVault 소유자 암호 제거(있는 경우)

통합 지문 판독기에서 프로비저닝된 모든 지문 제거(있는 경우)

모든 BIOS 암호 제거(BIOS 시스템, BIOS 관리자, HDD 암호)

TPM(Trusted Platform Module) 지우기

DDP|A 자격 증명 공급자 제거

컴퓨터 프로비저닝이 해제되면 DDP|A가 컴퓨터를 다시 시작하여 Windows 기본 자격 증명 공급자를 복구합니다.

DDP|A 제거

인증 하드웨어가 프로비저닝 해제되면 DDP|A를 제거합니다.

DDP|A를 시작하여 시스템 재설정을 실행합니다.

DDP|A로 관리되는 모든 자격 증명 및 암호를 비롯하여 TPM(신뢰할 수 있는 플랫폼 모듈)도 제거됩니다.

설치 제거를 클릭하여 설치 프로그램을 시작합니다.

제거를 마치면 **예**를 클릭하여 다시 시작합니다.

: DDP|A를 제거하면 SED도 잠금 해제되고 부팅 전 인증이 제거됩니다.

TPM 초기화

- 로컬 관리자 그룹(또는 이와 동등)의 구성원이어야 합니다.
- 컴퓨터에 호환되는 BIOS 및 TPM이 장착되어 있어야 합니다.

이 작업은 OTP(일회용 암호)를 사용하는 경우에 필요합니다.

- http://technet.microsoft.com/en-us/library/cc753140.aspx의 지침을 따릅니다.

소유권 지우기 및 TPM 활성화

TPM의 소유권을 제거한 후 설정하려면 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2를 참조하십시오.

설치 및 활성화로 진행합니다.

3

설치 및 활성화

이 섹션에서는 로컬 컴퓨터에 DDP | Security Tools를 설치하는 방법에 대해 자세히 설명합니다. DDP | Security Tools를 설치 후 활성화하려면 컴퓨터에 관리자 권한으로 로그온해야 합니다.

노트:
설치가 진행되는 동안에는 외부(USB) 드라이브 삽입 또는 제거를 비롯하여 컴퓨터를 변경하지 마십시오.

DDP | Security Tools 설치

Security Tools 설치 방법:

1 DDP | Security Tools 설치 미디어에서 설치 파일을 찾습니다. 로컬 컴퓨터로 복사합니다.

노트: 설치 미디어를 www.dell.com/support > Endpoint Security Solutions에서 찾을 수 있습니다.

2 파일을 더블 클릭하여 설치 관리자를 시작합니다.

3 적절한 언어를 선택하고 **OK(확인)**를 클릭합니다.

4 시작 페이지가 나타나면 **Next(다음)**를 클릭합니다.

5 라이센스 계약을 읽고 약관에 동의한 후 **Next(다음)**를 클릭합니다.

6 **Next(다음)**를 클릭하여 Security Tools를 기본 위치인C:\Program Files\Dell\Dell Data Protection에 설치합니다. **다음을 선택합니다.**

7 **Install(설치)**을 클릭하고 설치를 시작합니다.

8 설치가 완료되면 컴퓨터를 다시 시작해야 합니다. **예**를 선택하고 **Finish(마침)**를 클릭합니다.
설치가 완료됩니다.

DDP | Security Tools 활성화

DP Security Console을 처음 실행하여 관리자 설정을 선택하면 활성화 마법사에 따라 활성화 프로세스가 시작됩니다.

DDP Security Console이 아직 활성화되지 않았지만 최종 사용자가 실행할 수 있습니다. 관리자가 DDP | Security Tools를 활성화한 후 설정을 사용자 지정하기에 앞서 최종 사용자가 DDP Security Console을 처음 사용하는 경우에는 기본값을 사용합니다.

Security Tools 활성화 방법:

1 관리자가 데스크톱 바로 가기에서 Security Tools를 실행합니다.

노트: 일반 사용자로 로그인하는 경우(표준 Windows 계정 사용) 관리자 설정 도구를 시작하려면 UAC 권한 상승을 요청해야 합니다. 일반 사용자는 먼저 관리자 자격 증명을 입력하여 관리자 설정 도구에 로그인한 후 메시지가 표시되면 관리자 암호(관리자 설정에 저장된 암호)를 한 번 더 입력합니다.

2 **Administrator Settings(관리자 설정)** 타일을 클릭합니다.

3 시작 페이지에서 **다음**을 클릭합니다.

4 DDP | Security Tools 암호를 생성한 후 **Next(다음)**를 클릭합니다.
DDP | Security Tools 관리자 암호는 Security Tools를 구성하기 전에 반드시 생성해야 합니다. 관리자 설정 도구를 실행할 때마다 이 암호가 필요하기 때문입니다. 암호는 8~32자로서 문자, 숫자 및 특수 문자가 각각 하나 이상 포함되어야 합니다

5 **백업 위치**에서 백업 파일을 저장할 위치를 지정한 후 **Next(다음)**를 클릭합니다. 백업 파일은 네트워크 드라이브나 이동식 미디어 중 한 곳에 저장해야 합니다. 백업 파일에는 이 컴퓨터의 데이터를 복구하는 데 필요한 키가 포함되어 있습니다. 따라서 Dell 지원 부서가 데이터 복구를 지원하려면 이 파일에 대한 액세스 권한이 필요합니다.

복구 데이터는 지정 위치로 자동 백업됩니다. 위치를 사용할 수 없는 경우(예: 백업 USB 드라이브를 삽입하지 않은 경우) DDP | Security Tools이 데이터를 백업할 위치를 묻는 메시지를 표시합니다. 암호화를 시작하려면 복구 데이터에 액세스해야 합니다.

6 요약 페이지에서 **적용**을 클릭합니다.

Security Tools 활성화가 완료되었습니다.

이제 관리자와 사용자가 기본 설정에 따라 Security Tools 기능을 이용할 수 있습니다.

4

관리자에 대한 구성 작업

관리자와 사용자는 Security Tools를 활성화한 후 추가 구성 없이 Security Tools 기본 설정을 통해 Security Tools를 바로 사용할 수 있습니다. 사용자가 Windows 암호를 입력하여 컴퓨터에 로그온하면 자동으로 Security Tools 사용자로 추가되지만 다단계 Windows 인증은 기본적으로 비활성화되어 있습니다. 암호화 및 부팅 전 인증 역시 비활성화가 기본 설정입니다.

Security Tools 기능을 구성하려면 컴퓨터의 관리자 권한이 필요합니다.

관리자 암호 및 백업 위치 변경

Security Tools를 활성화한 후 필요한 경우 관리자 암호와 백업 위치를 변경할 수 있습니다.

1 관리자가 데스크톱 바로 가기에서 Security Tools를 실행합니다.
2 **Administrator Settings(관리자 설정)** 타일을 클릭합니다.
3 인증 대화 상자에서 활성화 도중 설정한 관리자 암호를 입력한 다음 **OK(확인)**를 클릭합니다.
4 **Administrator Settings(관리자 설정)** 탭을 클릭합니다.
5 관리자 암호 변경 페이지에서 암호를 변경하고 싶다면 새 암호를 입력합니다. 새 암호는 8~32자로 문자, 숫자 및 특수 문자가 각각 하나 이상 포함되어야 합니다.
6 확인을 위해 암호를 한 번 더 입력한 다음 **Apply(적용)**를 클릭합니다.
7 복구 키의 저장 위치를 변경하려면 왼쪽 창에서 **백업 위치 변경**을 선택합니다.
8 새로운 백업 위치를 선택하고 **Apply(적용)**를 클릭합니다.
백업 파일을 네트워크 드라이브 또는 이동식 미디어에 저장해야 합니다. 백업 파일에는 이 컴퓨터의 데이터를 복구하는 데 필요한 키가 포함되어 있습니다. 따라서 Dell ProSupport가 데이터 복구를 지원하려면 이 파일에 대한 액세스 권한이 필요합니다.

복구 데이터는 지정 위치로 자동 백업됩니다. 위치를 사용할 수 없는 경우(예: 백업 USB 드라이브를 삽입하지 않은 경우) DDP | Security Tools이 데이터를 백업할 위치를 묻는 메시지를 표시합니다. 암호화를 시작하려면 복구 데이터에 액세스해야 합니다.

암호화 및 부팅 전 인증 구성

암호화 및 PBA(부팅 전 인증)는 컴퓨터에 자체 암호화 드라이브(SED)가 설치된 경우에 이용할 수 있습니다. 두 가지 모두 암호화 탭에서 구성 가능하지만 먼저 컴퓨터에 자체 암호화 드라이브가 설치되어 있어야 표시됩니다. 암호화나 PBA 중 한 가지를 활성화할 경우 나머지 하나도 활성화됩니다.

암호화 및 PBA 활성화에 앞서, 복구 옵션으로 복구 질문을 등록하고 활성화하는 것이 좋습니다. 그래야만 암호를 잊더라도 복구가 가능하기 때문입니다. 자세한 정보는 로그인 옵션 구성을 참조하십시오.

암호화 및 부팅 전 인증 구성 방법:

1 DDP Security Console에서 **관리자 설정** 타일을 클릭합니다.
2 컴퓨터에서 백업 위치 액세스가 가능한지 확인합니다.

> **노트:** 암호화가 활성화되어 있는 상태에서 "백업 위치를 찾을 수 없음"이라는 메시지가 표시되고 백업 위치는 USB 드라이브로 지정되어 있다면, 드라이브가 연결되어 있지 않거나 백업 시 사용한 슬롯이 아닌 다른 슬롯에 연결되어 있는 것입니다. 네트워크 드라이브가 백업 위치일 때 이러한 메시지가 표시되는 이유는 컴퓨터에서 네트워크 드라이브에 액세스하지 못하기 때문입니다. 백업 위치를 변경해야 할 경우에는 **관리자 설정** 탭에서 **백업 위치 변경**을 선택하여 백업 위치를 현재 슬롯이나 액세스 가능한 드라이브로 변경합니다. 위치를 조정한 후 몇 초가 지나면 암호화 활성화 프로세스를 진행할 수 있습니다.

3 **Encryption(암호화)** 탭, **Encrypt(암호화)**를 차례로 클릭합니다.

4 시작 페이지에서 **다음**을 클릭합니다.

5 부팅 전 정책 페이지에서 다음 값을 변경 또는 확인하고 **Next(다음)**를 클릭합니다.

캐시되지 않은 사용자 로그인 시도	알려지지 않은 사용자가 로그인을 시도할 수 있는 횟수(이전에 해당 컴퓨터에 로그인한 적이 없는 사용자[캐시된 자격 증명이 없음])입니다.
캐시된 사용자 로그인 시도	캐시된 사용자가 로그인을 시도할 수 있는 횟수입니다.
복구 질문 응답 시도	사용자가 올바른 대답을 입력하기 위해 시도할 수 있는 횟수입니다.
암호화 지우기 암호 사용	사용하려면 선택합니다.
암호화 지우기 암호 입력	보안 메커니즘으로 사용하는 최대 100자의 단어 또는 코드입니다. PBA 인증 중에 사용자 이름 또는 암호 필드에 이 단어나 코드를 입력하면 모든 사용자에 대한 인증 토큰이 삭제되고 SED가 잠깁니다. 그 후에는 관리자만 강제로 장치를 잠금 해제할 수 있습니다. 비상 시에 암호화 지우기 암호를 사용하지 않으려면 이 필드를 비워두십시오.

6 부팅 전 사용자 지정 페이지에서 부팅 전 인증(PBA) 화면에 표시할 사용자 지정 텍스트를 입력하고 **Next(다음)**를 입력합니다.

부팅 전 제목 텍스트	이 텍스트는 PBA 화면 위쪽에 표시됩니다. 이 필드를 비워두면 제목이 표시되지 않습니다. 텍스트가 줄바꿈되지 않으므로 17자 이상을 입력하면 잘릴 수 있습니다.
지원 정보 텍스트	이 텍스트는 PBA 지원 정보 페이지에 표시됩니다. 헬프 데스크 또는 보안 관리자에게 연락하는 방법에 대한 구체적인 지침을 포함하도록 메시지를 사용자 지정하는 것이 좋습니다. 이 필드에 텍스트를 입력하지 않으면 사용자가 지원 연락처 정보를 사용할 수 없게 됩니다. 텍스트 줄바꿈은 문자 수준이 아닌 단어 수준으로 발생합니다. 예를 들어, 한 단어의 길이가 약 50자보다 긴 경우 줄바꿈되지 않고 스크롤 바가 없으므로 텍스트가 잘립니다.
법적 고지 사항 텍스트	이 텍스트는 사용자가 장치에 로그온하도록 허용되기 전에 표시됩니다. 예를 들어 "확인을 클릭하면 적용 가능한 컴퓨터 사용 정책을 준수하는 것에 동의하는 것입니다." 같은 텍스트를 표시합니다. 이 필드에 텍스트를 입력하지 않으면 텍스트나 확인/취소 버튼이 표시되지 않습니다. 텍스트 줄바꿈은 문자 수준이 아닌 단어 수준으로 발생합니다. 예를 들어, 한 단어의 길이가 약 50자보다 긴 경우 줄바꿈되지 않고 스크롤 바가 없으므로 텍스트가 잘립니다.

7 요약 페이지에서 **적용**을 클릭합니다.

8 메시지가 나타나면 **시스템 종료**를 클릭합니다.
시스템을 완전히 종료해야 암호화를 시작할 수 있습니다.

9 시스템을 종료한 후 컴퓨터를 다시 시작하십시오.
이제 Security Tools에서 인증을 관리합니다. 사용자는 부팅 전 인증 화면에서 Windows 암호를 입력하여 로그인해야 합니다.

암호화 및 부팅 전 인증 설정 변경

처음 암호화를 활성화하고 부팅 전 정책 및 사용자 지정을 구성한 후에는 암호화 탭에서 다음 작업이 가능해집니다.

부팅 전 정책 또는 사용자 지정 변경 - **Encryption(암호화)** 탭, **Change(변경)**를 차례로 클릭합니다.

설치 제거 등을 위한 SED 암호 해독 - **암호 해독**을 클릭합니다.

처음 암호화를 활성화하고 부팅 전 정책 및 사용자 지정을 구성한 후에는 부팅 전 설정 탭에서 다음 작업이 가능해집니다.

부팅 전 정책 또는 사용자 지정 변경 - **Preboot Settings(부팅 전 설정)** 탭을 클릭하고 **부팅 전 사용자 지정** 또는 **부팅 전 로그온 정책**을 선택합니다.

제거 지침은 제거 작업을 참조하십시오.

인증 옵션 구성

관리자 설정 인증 탭의 컨트롤을 사용하여 사용자 로그인 옵션을 설정하고 각각에 대한 설정값을 사용자 지정할 수 있습니다.

ⓘ | **노트:** OTP(일회용 암호) 옵션은 TPM의 설치, 활성화, 소유권이 갖춰져 있지 않으면 복구 옵션에 표시되지 않습니다.

로그인 옵션 구성

로그인 옵션 페이지에서는 로그온 정책을 구성할 수 있습니다. 기본적으로 지원되는 모든 자격 증명은 사용 가능한 옵션에 표시됩니다.

로그인 옵션 구성 방법:

왼쪽 창의 인증에서 **로그인 옵션**을 선택합니다.

설정하려는 역할을 선택하려면 **로그인 옵션 적용 대상** 목록에서 **사용자** 또는 **관리자**를 선택합니다. 이 페이지의 변경 사항은 모두 선택한 역할에만 적용됩니다.

인증 시 사용 가능한 옵션을 설정합니다.

기본적으로 각각의 인증 방법은 다른 인증 방법과 함께 사용하지 않고 개별적으로 사용하도록 구성되어 있습니다. 다음과 같은 방법으로 기본값을 변경할 수 있습니다.

인증 옵션의 조합을 설정하려면 사용 가능한 옵션 아래에서 ⁄을 클릭하여 첫 번째 인증 방법을 선택합니다. 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 선택하고 **확인**을 클릭합니다.

예를 들어, 로그온 자격 증명으로 지문과 암호를 모두 요청할 수 있습니다. 대화 상자에서, 지문 인증을 통해 사용해야 하는 두 번째 인증 방법을 선택합니다.

각 인증 방법을 개별적으로 사용할 수 있도록 하려면 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 **적용 안 함**으로 설정된 채로 두고 **확인**을 클릭합니다.

로그인 옵션을 제거하려면 사용 가능한 옵션의 로그인 옵션 페이지에서 **X**를 클릭하고 인증 방식을 제거할 수 있습니다.

새로운 조합의 인증 방식을 추가하려면 **옵션 추가**를 클릭합니다.

사용자가 잠금 해제되어 컴퓨터 액세스를 복구하려고 할 때는 다음과 같이 복구 옵션을 설정합니다.

사용자가 컴퓨터에 대한 액세스 권한을 다시 얻기 위해 사용할 질문 및 답변을 정의하려면 **복구 질문**을 선택합니다.

복구 질문을 사용하지 않으려면 이 옵션을 선택 취소합니다.

사용자가 모바일 장치를 사용해 액세스 권한을 복구하도록 하려면 **OTP(일회용 암호)**를 선택합니다. OTP(일회용 암호)를 복구 방법으로 선택할 경우 Windows 로그온 화면의 로그인 옵션으로 사용할 수는 없습니다.

OTP 기능을 로그온 옵션으로 사용하려면 복구 옵션에서 이 옵션을 선택 취소하십시오. OTP 기능을 복구 옵션에서 선택 취소하면 OTP에 등록된 사용자가 한 명만 있더라도 OTP 옵션이 Windows 로그온 페이지에 표시됩니다.

: 관리자는 OTP 사용 방법을 인증 또는 복구 목적으로 제어할 수 있습니다. OTP 기능은 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. 로그인 옵션 필드인 **로그인 옵션 적용 대상**에서 선택한 항목에 따라 컴퓨터의 모든 사용자 또는 모든 관리자에게 구성이 적용됩니다.

복구 옵션 아래에 일회용 암호 옵션이 나열되지 않으면 컴퓨터의 구성에서 이 옵션을 지원하지 않는 것입니다. 자세한 내용은 요구 사항을 참조하십시오.

사용자가 로그온 자격 증명을 잊거나 잃어버린 경우 헬프 데스크로 연락하도록 하려면 복구 옵션 아래에서 복구 질문과 일회용 암호 확인란을 모두 선택 취소합니다.

사용자가 인증 자격 증명을 등록할 수 있는 기간을 설정하려면 **유예 기간**을 선택합니다.

유예 기간 기능을 통해, 구성된 로그인 옵션의 적용 시작일을 선택할 수 있습니다. 로그인 옵션 적용 날짜 이전에 이를 구성하고, 사용자의 등록 기간을 설정할 수 있습니다. 기본적으로 이 정책은 즉시 적용됩니다.

로그인 옵션 적용 날짜를 *즉시*에서 다른 날짜로 변경하려면 유예 기간 대화 상자에서 드롭다운 메뉴를 클릭하고 **지정된 날짜**를 선택합니다. 날짜 필드의 오른쪽에 있는 아래쪽 화살표를 클릭하여 달력을 표시하고 날짜를 선택합니다. 정책은 선택한 날짜의 약 오전 12시 1분부터 시작됩니다.

사용자는 다음에 Windows에 로그온할 때 필요한 자격 증명을 등록하라는 알림을 수신할 수도 있고(기본값), 정기적인 미리 알림을 설정할 수도 있습니다. *사용자에게 알림* 드롭다운 목록에서 미리 알림 간격을 선택합니다.

:

사용자에게 표시되는 미리 알림은 미리 알림이 트리거되었을 때 사용자가 Windows 로그온 화면에 있는지 또는 Windows 세션 안에 있는지에 따라 약간 다릅니다. 부팅 전 인증 로그온 화면에는 미리 알림이 나타나지 않습니다.

유예 기간 중 기능

지정된 유예 기간 동안 사용자가 변경된 로그인 옵션을 충족하는 데 필요한 최소 자격 증명을 등록하지 않았으면 로그인할 때마다 추가 자격 증명 알림이 표시됩니다. 메시지에는 '*추가 자격 증명을 등록할 수 있습니다.*'라는 내용이 표시됩니다.

추가 자격 증명을 사용할 수 있지만 필수 사항은 아닌 경우 정책이 변경된 후 메시지가 한 번만 표시됩니다.

알림을 클릭하면 컨텍스트에 따라 다음과 같은 결과가 나타납니다.

등록된 자격 증명이 없는 경우 관리자는 컴퓨터 관련 설정을 구성하고 사용자는 가장 일반적인 자격 증명을 등록할 수 있는 설정 마법사가 표시됩니다.

처음으로 자격 증명을 등록한 후 알림을 클릭하면 DDP 보안 콘솔 내에 설정 마법사가 표시됩니다.

유예 기간 만료 후 기능

유예 기간이 만료되면 로그인 옵션에서 요구하는 자격 증명을 등록해야만 로그온할 수 있습니다. 사용자가 로그인 옵션을 충족하지 않는 자격 증명 또는 자격 증명의 조합으로 로그온하도록 시도하면 Windows 로그온 화면 위에 설정 마법사가 표시됩니다.

사용자가 필요한 자격 증명을 성공적으로 등록하면 Windows에 로그인됩니다.

사용자가 필요한 자격 증명을 성공적으로 등록하지 않거나 마법사를 취소하면 Windows 로그온 화면으로 돌아갑니다.

선택한 역할에 대한 설정을 저장하려면 **적용**을 클릭합니다.

Password Manager 인증 구성

Password Manager 페이지에서 사용자가 Password Manager에 인증하는 방법을 구성할 수 있습니다.

Password Manager 인증 구성 방법:

왼쪽 창의 인증에서 **Password Manager**를 선택합니다.

설정하려는 역할을 선택하려면 **로그인 옵션 적용 대상** 목록에서 **사용자** 또는 **관리자**를 선택합니다. 이 페이지의 변경 사항은 모두 선택한 역할에만 적용됩니다.

(선택사항) **인증을 요구하지 않음** 확인란을 선택하면 선택된 사용자 역할이 Password Manager에 저장된 자격 증명을 통해 모든 소프트웨어 응용 프로그램 및 인터넷 웹사이트에 자동 로그인됩니다.

인증 시 사용 가능한 옵션을 설정합니다.

기본적으로 각각의 인증 방법은 다른 인증 방법과 함께 사용하지 않고 개별적으로 사용하도록 구성되어 있습니다. 다음과 같은 방법으로 기본값을 변경할 수 있습니다.

인증 옵션의 조합을 설정하려면 사용 가능한 옵션 아래에서 ⁄을 클릭하여 첫 번째 인증 방법을 선택합니다. 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 선택하고 **확인**을 클릭합니다.

예를 들어, 로그온 자격 증명으로 지문과 암호를 모두 요청할 수 있습니다. 대화 상자에서, 지문 인증을 통해 사용해야 하는 두 번째 인증 방법을 선택합니다.

각 인증 방법을 개별적으로 사용할 수 있도록 하려면 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 **적용 안 함**으로 설정된 채로 두고 **확인**을 클릭합니다.

로그인 옵션을 제거하려면 사용 가능한 옵션의 로그인 옵션 페이지에서 **X**를 클릭하고 인증 방식을 제거할 수 있습니다.

새로운 조합의 인증 방식을 추가하려면 **옵션 추가**를 클릭합니다.

선택한 역할의 설정을 저장하려면 **적용**을 클릭합니다.

 : 기본값 단추를 선택하면 설정이 초기 값으로 복구됩니다.

복구 질문 구성

복구 질문 페이지에서는 개인적인 복구 질문 및 답변을 정의할 때 사용자에게 나타나는 질문을 선택할 수 있습니다. 사용자는 암호가 만료되었거나 암호를 잊었을 때 이 복구 질문을 이용해 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다.

복구 질문 구성 방법:

왼쪽 창의 인증에서 **복구 질문**을 선택합니다.

복구 질문 페이지에서 사전 정의된 복구 질문을 3개 이상 선택합니다.

옵션으로, 사용자가 선택할 수 있는 사용자 지정 질문을 최대 3개까지 목록에 추가할 수 있습니다.

복구 질문을 저장하려면 **적용**을 클릭합니다.

지문 스캔 인증 구성

지문 스캔 인증 구성 방법:

왼쪽 창의 인증 아래에서 **지문**을 선택합니다.

등록에서 사용자가 등록할 수 있는 최소 및 최대 지문 개수를 설정합니다.

지문 스캔 민감도를 설정합니다.

민감도가 낮을수록 잘못된 스캔을 수락할 가능성과 허용 편차가 증가합니다. 가장 높게 설정하면 올바른 지문이 거부될 수도 있습니다. 민감도가 높을수록 타인 수락 오류율이 1/10,000로 낮아집니다.

지문 판독기의 버퍼에서 모든 지문 스캔과 자격 증명 등록을 제거하려면 **판독기 지우기**를 클릭합니다. 이때 데이터는 현재 추가한 데이터만 제거되고, 이전 세션에서 저장한 스캔과 등록은 삭제되지 않습니다.

설정을 저장하려면 **적용**을 클릭합니다.

OTP(일회용 암호) 인증 구성

OTP(일회용 암호) 기능을 사용하려면 사용자가 모바일 장치에서 Dell Data Protection | Security Tools Mobile 앱을 사용하여 일회용 암호를 생성하고 컴퓨터에 해당 암호를 입력합니다. 암호는 한 번만 사용할 수 있으며 제한된 기간 동안에만 유효합니다.

관리자가 보안을 더욱 강화하려면 암호를 요청하여 모바일 응용 프로그램의 안전 여부를 확인할 수 있습니다.

모바일 장치 및 OTP의 보안 강화는 모바일 장치 페이지에서 설정을 구성하면 가능합니다.

OTP 인증 구성 방법:

왼쪽 창의 인증에서 **모바일 장치**를 선택합니다.

사용자에게 모바일 장치에서 암호를 입력하여 Security Tools Mobile 앱에 액세스하도록 요청하려면 **암호 필요**를 선택합니다.

: 모바일 장치를 컴퓨터에 등록한 후에 *암호 필요* 정책을 활성화하면 모든 모바일 장치의 등록이 해제됩니다. 이 정책이 활성화되면 모바일 장치를 다시 등록하라는 메시지가 표시됩니다.

암호 필요 확인란이 선택되어 있으면 사용자가 모바일 장치의 잠금을 해제해야 Security Tools Mobile 앱에 액세스할 수 있습니다. 장치 잠금이 모바일 장치에 표시되지 않더라도 암호를 요구하게 됩니다.

OTP(일회용 암호) 길이를 선택하려면 **일회용 암호 길이**에서 요구할 암호 문자 수를 선택합니다.

사용자가 OTP를 정확히 입력해야 하는 횟수를 선택하려면 **허용되는 사용자 로그인 시도**에서 **5~30**까지 숫자 하나를 선택합니다.

최대 횟수에 도달한 경우 OTP 기능은 사용자가 모바일 장치를 다시 등록할 때까지 사용할 수 없습니다.

: OTP 외에 인증 방식을 한 가지 이상 추가로 설정하는 것이 좋습니다.

스마트 카드 등록 구성

DDP|Security Tools는 비접촉식과 접촉식, 두 가지 방식의 스마트 카드를 지원합니다.

접촉식 카드는 카드를 삽입할 스마트 카드 판독기가 필요하며, 도메인 컴퓨터와만 호환됩니다. CAC 및 SIPRNet 카드는 모두 접촉식입니다. 이 카드는 고급 특성상 사용자가 카드를 삽입하여 로그온한 후 인증서를 선택해야 합니다.

비접촉식 카드는 비도메인 컴퓨터 및 도메인 사양으로 구성된 컴퓨터에서 지원됩니다.

사용자는 사용자 계정 하나당 접촉식 스마트 카드 1개, 혹은 비접촉식 카드 여러 개를 등록할 수 있습니다.

부팅 전 인증에서는 스마트 카드가 지원되지 않습니다.

: 다수의 카드가 등록된 계정에서 1개의 스마트 카드 등록을 제거할 경우 모든 카드가 동시에 등록 해제됩니다.

스마트 카드 등록 구성 방법:

관리자 설정 도구의 인증 탭에서 **스마트 카드**를 선택합니다.

고급 권한 구성

고급 최종 사용자 옵션을 수정하려면 **고급**을 클릭합니다. *고급* 아래에서 필요에 따라 사용자가 자격 증명을 직접 등록하고 등록된 자격 증명을 수정하여 원스텝 로그온을 수행할 수 있도록 허용할 수 있습니다.

다음 확인란을 선택하거나 지웁니다.

사용자의 자격 증명 등록 허용 - 기본적으로 확인란이 선택되어 있습니다. 사용자가 관리자의 개입 없이 자격 증명을 등록할 수 있습니다. 확인란을 지울 경우 관리자가 자격 증명을 등록해야 합니다.

사용자의 등록된 자격 증명 수정 허용 - 기본적으로 확인란이 선택되어 있습니다. 선택되어 있으면 사용자가 관리자의 개입 없이 등록된 자격 증명을 수정하거나 삭제할 수 있습니다. 확인란을 지울 경우 자격 증명을 일반 사용자가 수정하거나 삭제할 수 없으며, 관리자가 수정하거나 삭제해야 합니다.

: 사용자의 자격 증명을 등록하려면 관리자 설정 도구의 *사용자* 페이지로 이동하여 사용자를 선택하고 **등록**을 클릭합니다.

원스텝 로그온 허용 - 원스텝 로그온이란 SSO(Single Sign-on)를 말합니다. 확인란이 기본적으로 선택되어 있습니다. 이 기능을 활성화할 경우 사용자는 부팅 전 인증 화면에서만 자격 증명을 입력하면 됩니다. 사용자가 Windows에 자동으로 로그온됩니다. 이 확인란을 선택 취소하면 여러 차례 로그온해야 할 수도 있습니다.

 : 이 옵션은 **사용자의 자격 증명 등록 허용** 설정도 선택되어 있어야 사용할 수 있습니다.

완료되면 **적용**을 클릭합니다.

스마트 카드 및 생체 인식 서비스(선택 사항)

Security Tools에서 스마트 카드 및 생체 인식 장치 관련 서비스의 시작 유형을 "자동"으로 변경하고 싶지 않다면 서비스 시작 기능을 비활성화할 수 있습니다.

이 기능을 비활성화하면 Security Tools가 다음 세 가지 서비스를 시작하지 않습니다.

SCardSvr - 컴퓨터가 판독하는 스마트 카드에 대한 액세스를 관리합니다. 이 서비스가 중지되면 컴퓨터에서 스마트 카드를 판독할 수 없습니다. 이 서비스가 비활성화되면 서비스에 명시적으로 의존된 모든 서비스가 시작되지 않습니다.

SCPolicySvc - 스마트 카드가 제거되면 사용자의 데스크톱이 잠기도록 시스템을 구성할 수 있습니다.

WbioSrvc - Windows 생체 인식 서비스를 통해 클라이언트 응용 프로그램은 생체 인식 하드웨어 또는 샘플에 직접 액세스하지 않고도 생체 인식 데이터를 캡처, 비교, 조종, 저장할 수 있습니다. 이 서비스는 권한이 부여된 SVCHOST 프로세스에서 호스팅됩니다.

이 기능을 비활성화하면 실행해야 하는 필요한 서비스와 관련된 경고도 표시되지 않습니다.

자동 서비스 시작 사용 안 함

기본적으로 레지스트리 키가 없거나 값이 0으로 설정되어 있는 경우 이 기능이 사용됩니다.

Regedit를 실행합니다.

다음 레지스트리 항목을 찾습니다.

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

사용하려면 0으로 설정합니다. 사용하지 않으려면 1로 설정합니다.

사용자 인증 관리

관리자 설정 인증 탭의 컨트롤은 사용자 로그온 옵션을 설정하거나 각 옵션 설정을 사용자 지정하는 데 사용됩니다.

사용자 인증 관리 방법:

1 관리자 권한으로 **관리자 설정** 타일을 클릭합니다.

2 **Users(사용자)** 탭을 클릭하고 사용자를 관리하거나 사용자 등록 상태를 확인합니다. 이 탭의 기능은 다음과 같습니다.

- 새로운 사용자 등록
- 자격 증명 추가 또는 변경
- 사용자의 자격 증명 제거

ⓘ **노트:**

로그인 및 **세션**에 사용자의 등록 상태가 표시됩니다.

로그인 상태가 **정상**이면 사용자가 로그온하는 데 필요한 모든 등록이 완료된 것입니다. **세션** 상태가 **정상**이면 사용자가 Password Manager를 사용하는 데 필요한 모든 등록이 완료된 것입니다.

둘 중 하나의 상태가 **미완료**이면 사용자가 추가 등록을 완료해야 합니다. 필요한 등록을 확인하려면 **Administrator Settings(관리자 설정)** 도구를 선택하고 **사용자** 탭을 엽니다. 회색 확인 표시 상자는 완료되지 않은 등록을 나타냅니다. 또는 **등록** 타일을 클릭하고 **상태** 탭의 **정책** 열에서 나열된 필요한 등록을 검토합니다.

새 사용자 추가

: 새 Windows 사용자가 Windows에 로그인하거나 자격 증명을 등록하면 자동으로 추가됩니다.

기존 Windows 사용자의 등록 프로세스를 시작하려면 **Add User(사용자 추가)**를 클릭합니다.
사용자 선택 대화 상자가 표시되면 **개체 유형**을 선택합니다.
텍스트 상자에 사용자의 개체 이름을 입력하고 **Check Names(이름 확인)**를 클릭합니다.
모두 마쳤으면 **OK(확인)**를 클릭합니다.
등록 마법사가 열립니다.

지침에 대한 사용자 자격 증명을 등록하거나 변경으로 계속합니다.

사용자 자격 증명 등록 또는 변경

관리자가 사용자를 대신하여 사용자의 자격 증명을 등록하거나 변경할 수 있지만, 복구 질문에 대답 및 사용자의 지문 스캔과 같은 몇 가지 등록 작업은 사용자가 있어야 합니다.

사용자 자격 증명을 등록하거나 변경하려면 다음을 수행합니다.

관리자 설정에서 **Users(사용자)** 탭을 클릭합니다.
사용자 페이지에서 **등록**을 클릭합니다.
시작 페이지에서, **다음**을 클릭합니다.
인증 필요 대화 상자에서 사용자의 Windows 암호를 사용하여 로그인하고 **OK(확인)**를 클릭합니다.
암호 페이지에서 사용자의 Windows 암호를 변경하려면 새 암호를 입력한 후 확인하고 **Next(다음)**를 클릭합니다.
암호 변경을 건너뛰려면 **건너뛰기**를 클릭합니다. 등록을 원하지 않을 때는 마법사에서 자격 증명을 건너뛸 수 있습니다. 페이지로 돌아가려면 **뒤로**를 클릭합니다.
각 페이지의 지침을 수행하고 **다음**, **건너뛰기**, 또는 **뒤로** 중 적절한 단추를 클릭합니다.
요약 페이지에서 등록된 자격 증명을 확인한 후 등록을 모두 마쳤으면 **적용**을 클릭합니다.
자격 증명 등록 페이지로 돌아가서 정보를 변경하려면 원하는 페이지에 이를 때까지 **뒤로**를 클릭합니다.

자격 증명 등록 또는 변경에 대한 자세한 내용은 *Dell Data Protection | Console 사용 설명서*를 참조하십시오.

등록된 자격 증명 1개 제거

Administrator Settings(관리자 설정) 타일을 클릭합니다.
Users(사용자) 탭을 클릭하고 변경할 사용자를 찾습니다.
제거할 자격 증명의 녹색 확인 표시 위로 마우스를 이동합니다. ⊗로 변경됩니다.
⊗ 기호를 클릭하고 **Yes(예)**를 클릭하여 삭제를 확인합니다.

: 사용자가 등록한 자격 증명이 하나인 경우에는 이러한 방식으로 자격 증명을 제거할 수 없습니다. 또한 이 방법으로 암호를 제거할 수 없습니다. 컴퓨터에 대한 사용자의 액세스 권한을 완전히 제거하려면 제거 명령을 사용하십시오.

사용자의 등록된 자격 증명 모두 제거

Administrator Settings(관리자 설정) 타일을 클릭합니다.
Users(사용자) 탭을 클릭하고 제거할 사용자를 찾습니다.
Remove(제거)를 클릭합니다. (사용자의 설정값 아래쪽에 제거 명령이 빨간색으로 표시됨)
제거되면 사용자가 다시 등록할 때까지 컴퓨터에 로그온할 수 없습니다.

5

제거 작업

DDP | Security Tools는 최소한 **로컬 관리자** 권한이 있어야 제거할 수 있습니다.

DDP | Security Tools 제거

이 응용 프로그램을 제거할 때는 반드시 다음 순서를 따라야 합니다.

1. DDP | Client Security Framework
2. DDP | Security Tools Authentication
3. DDP | Security Tools

컴퓨터에 자체 암호화 드라이브가 있는 경우 다음 지침에 따라 제거를 실행하십시오.

1 SED를 프로비저닝 해제합니다.
   a 관리자 설정에서 **Encryption(암호화)** 탭을 클릭합니다.
   b **암호 해독**을 클릭하고 암호화를 비활성화합니다.
   c SED 암호화가 비활성화되면 컴퓨터를 다시 시작합니다.
2 Windows 제어판에서 **프로그램 제거**로 이동합니다.

   노트: 시작 > 제어판 > 프로그램 및 기능 > 프로그램 제거로 이동하십시오.
3 **Client Security Framework**를 제거하고 컴퓨터를 다시 시작합니다.
4 Windows 제어판에서 **Security Tools Authentication**을 제거합니다.
   사용자 데이터의 보존 여부를 묻는 메시지가 표시됩니다.

   Security Tools를 다시 설치할 계획이라면 **Yes(예)**를 클릭합니다. 그렇지 않다면 **아니요**를 클릭합니다.

   제거가 완료되면 컴퓨터를 다시 시작합니다.
5 Windows 제어판에서 **Security Tools**를 제거합니다.
   이 응용 프로그램과 구성 요소를 완전히 제거할지 묻는 메시지가 표시됩니다.

   Yes(예)를 클릭합니다.

   제거 완료 대화 상자가 표시됩니다.
6 **es, I want to restart my computer now(예, 컴퓨터를 지금 다시 시작합니다)**와 **Finish(마침)**를 차례대로 클릭합니다.
7 컴퓨터가 다시 시작되고 제거가 완료됩니다.

6

복구

사용자 자격 증명이 만료되었거나 잊은 경우를 위해 다음과 같은 복구 옵션이 지원됩니다.

- **일회용 암호(OTP)**: 사용자는 등록된 모바일 장치의 Security Tools Mobile 앱에서 OTP를 생성하여 Windows 로그온 화면에 입력하면 액세스 권한을 다시 얻을 수 있습니다. 이 옵션은 사용자가 모바일 장치를 컴퓨터의 Security Tools에 등록한 경우에만 사용 가능합니다. OTP 기능을 사용하여 복구하려면 OTP를 사용하여 컴퓨터에 로그온한 적이 없어야 합니다.

  ① **노트:** OTP(일회용 암호) 기능을 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. 소유권 지우기 및 TPM 활성화의 지침을 따릅니다. OTP는 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. 자세한 내용은 로그인 옵션 구성을 참조하십시오.
- **복구 질문:** 사용자가 개인 질문에 정확히 답변하면 컴퓨터에 대한 액세스 권한을 다시 얻게 됩니다. 이 옵션은 관리자가 복구 질문을 구성 및 활성화한 후 사용자가 복구 질문을 등록한 경우에만 사용 가능합니다. 또한 부팅 전 인증 화면과 Windows 로그온 화면 모두에서 지원되어 컴퓨터에 대한 액세스 권한을 다시 얻을 수 있습니다.

위 두 가지 복구 방법을 이용하려면 먼저 복구 질문을 등록하거나 모바일 장치를 컴퓨터의 Security Tools에 등록하여 복구 준비를 마쳐야 합니다.

자체 복구, Windows 로그온 복구 질문

Windows 로그온 화면에서 액세스 권한을 복구하기 위해 복구 질문에 답변하려면 다음을 수행합니다.

1 복구 질문을 사용하려면 **계정에 액세스할 수 없습니까?**를 클릭합니다.
등록 단계에서 선택한 복구 질문이 표시됩니다.

2 답변을 입력하고 **OK(확인)**를 클릭합니다.
질문에 대한 답변을 성공적으로 입력하면 액세스 권한 복구 모드로 전환됩니다. 다음은 실패한 자격 증명에 따라 달라집니다.

- 잘못된 Windows 암호를 입력한 경우에는 암호 변경 화면이 나타납니다.
- 지문 인식이 실패한 경우에는 지문을 다시 등록할 수 있도록 지문 등록 페이지가 나타납니다.

자체 복구, PBA 복구 질문

부팅 전 인증 화면에서 액세스 권한을 복구하기 위해 복구 질문에 답변하려면 다음을 수행합니다.

1 부팅 전 인증 화면에서 사용자 이름을 입력합니다.

2 화면의 왼쪽 하단에서 **옵션**을 선택합니다.

3 옵션 메뉴에서 **암호 분실**을 선택합니다.

4 복구 질문에 답변하고 **Sign In(로그인)**을 클릭합니다.

자체 복구, OTP(일회용 암호)

다음은 Windows 암호가 만료되었거나 암호를 잊은 경우, 혹은 최대 허용 로그온 시도 횟수를 초과한 경우에 컴퓨터에 대한 액세스 권한을 복구하기 위해 OTP(일회용 암호) 기능을 사용하는 방법에 대한 절차입니다. OTP(일회용 암호) 옵션은 사용자가 모바일 장치를 등록한 경우, 그리고 OTP를 Windows 로그온에 사용하지 않은 경우에만 지원됩니다.

노트: OTP(일회용 암호) 기능을 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP는 Windows 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. 관리자는 복구와 인증 중 어떤 용도로 사용할지 정책을 설정하거나, 혹은 비활성화할 수도 있습니다.

컴퓨터에 대한 액세스 권한 복구 용도로 OTP를 사용하는 방법:

1 Windows 로그온 화면에서, OTP 아이콘  을 선택합니다.

2 모바일 장치에서 Security Tools Mobile 앱을 열고 암호를 입력합니다.

3 액세스할 컴퓨터를 선택합니다.

모바일 장치에 컴퓨터 이름이 표시되지 않는 경우 다음 상태 중 하나 때문일 수 있습니다.

- 모바일 장치가 액세스하려는 컴퓨터에 등록되지 않았거나 페어링되어 있지 않습니다.
- Windows 사용자 계정이 두 개 이상인 경우 액세스하려는 컴퓨터에 DDP | Security Tools가 설치되어 있지 않거나, 컴퓨터와 모바일 장치를 페어링하는 데 사용한 계정과 다른 사용자 계정에 로그온하려고 시도하는 중입니다.

4 **OTP(일회용 암호)**를 누릅니다.

모바일 장치 화면에 암호가 표시됩니다.

노트: 필요한 경우 새로 고침 기호  를 클릭하여 새 코드를 가져옵니다. 첫 번째 두 개의 OTP가 새로 고침된 후 다른 OTP가 생성될 때까지 30초 정도가 지연됩니다. 컴퓨터와 모바일 장치가 모두 동일한 암호를 동시에 인식하려면 서로 동기화되어야 합니다. 하지만 암호를 차례대로 빠르게 생성하려고 하면 컴퓨터와 모바일 장치의 동기화가 해제되어 OTP 기능이 작동하지 않을 수 있습니다. 이러한 문제가 발생할 경우 두 장치가 다시 동기화될 때까지 30초를 기다린 후 다시 시도하십시오.

5 컴퓨터의 Windows 로그온 화면에서 모바일 장치에 표시된 암호를 입력하고 **Enter**를 누릅니다.

6 컴퓨터의 복구 모드 화면에서 **Windows 암호 분실**을 선택하고 화면에 나타나는 지시에 따라 암호를 재설정합니다.

7

용어집

프로비저닝 해제 - 프로비저닝을 해제하면 PBA 데이터베이스가 제거되고 PBA가 비활성화됩니다. 프로비저닝을 해제하려면 시스템을 종료해야 합니다.

일회용 암호(OTP) – OTP는 단 한 번만 사용할 수 있는 암호로, 제한된 기간 동안에만 유효합니다. OTP를 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP를 이용하려면 Security Console 및 Security Tools Mobile 앱을 사용하여 모바일 장치와 컴퓨터를 페어링해야 합니다. Security Tools Mobile 앱에서 생성된 모바일 장치의 암호는 Windows 로그온 화면에서 컴퓨터에 로그온하는 데 사용됩니다. 정책에 따라, 컴퓨터에 로그온할 때 OTP를 사용한 적이 없으면 암호가 만료되거나 분실한 경우 OTP 기능을 사용하여 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다. OTP 기능은 그 밖에 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. OTP 보안은 생성된 암호가 1회용이며 유효 기간이 짧다는 점에서 다른 인증 방식의 보안보다 강력하다고 할 수 있습니다.

PBA(부팅 전 인증) – PBA(부팅 전 인증)는 BIOS 또는 부팅 펌웨어를 확장하는 기능을 하며 운영 체제 외부에서 신뢰할 수 있는 인증 계층으로 안전한 변조 방지 환경을 보장합니다. PBA는 사용자에게 올바른 자격 증명이 있는지 확인할 때까지 하드 디스크에서 운영 체제 등의 데이터를 읽을 수 없도록 합니다.

SSO(Single Sign On) - SSO는 부팅 전 및 Windows 로그온에서 다단계 인증을 사용할 경우 로그온 프로세스를 간소화합니다. 이 기능을 사용할 경우 부팅 전에만 인증이 필요하며 사용자는 Windows에 자동으로 로그온됩니다. 사용하지 않을 경우에는 여러 번 인증이 필요할 수 있습니다.

TPM(Trusted Platform Module) – TPM은 안전한 저장, 측정, 증명의 세 가지 주요 기능을 제공하는 보안 칩입니다. Encryption 클라이언트는 안전한 저장 기능 때문에 TPM을 사용합니다. TPM도 소프트웨어 자격 증명 모음에 대해 암호화된 컨테이너를 제공할 수 있습니다. TPM은 OTP(일회용 암호) 기능을 사용하려는 경우에도 필요합니다.