Dell Data Protection

콘솔 사용 설명서

Advanced Threat Protection 암호화 상태
인증 등록
Password Manager
v1.10

차례

1 소개 5

2 DDP Console 7

3 암호화 상태 9

4 등록 11

자격 증명 최초 등록 **11**

등록 추가 , 수정 또는 보기 **11**

암호 **12**

복구 질문 **12**

지문 **12**

모바일 장치 **13**

Security Tools Mobile 설정 13

모바일 장치와 컴퓨터 페어링 14

다른 모바일 장치 등록 14

컴퓨터와 모바일 장치 페어링 해제 15

일회용 암호를 사용하여 로그온 **16**

Security Tools Mobile 관리 작업 **16**

Security Tools Mobile 앱 PIN 재설정 16

Security Tools Mobile 앱 제거 16

스마트 카드 **17**

5 Password Manager 19

Password Manager 시작하기 **19**

로그온 관리 **20**

범주 추가 20

로그온 추가 20

자격 증명 가져오기 **21**

아이콘의 상황에 맞는 메뉴 **21**

트레이닝된 로그온 페이지 로그온 **22**

웹 도메인 지원 **22**

Windows 자격 증명 채우기 **23**

웹 사이트 제외 **23**

로그온 양식을 트레이닝하라는 프롬프트 메시지 비활성화 **24**

Password Manager 자격 증명 백업 및 복원 **24**

자격 증명 백업 24

자격 증명 복구 24

용어집 25

1

소개

Dell Data Protection | Security Tools 는 컴퓨터 보안 향상을 위해 쉽게 사용할 수 있는 직관적인 도구를 제공합니다 .

DDP Console 을 통해 다음 기능을 사용할 수 있습니다 .

- Security Tools 에 사용할 자격 증명 등록
- 암호 , 지문 , 및 스마트 카드를 포함하여 다중 요소 자격 증명의 장점 이용
- 암호를 분실한 경우 헬프 데스크에 연락하거나 관리자의 지원을 받지 않고 컴퓨터에 대한 액세스 복구
- 프로그램 데이터 백업 및 복원
- 쉽게 Windows 암호 변경
- 개인 환경설정 지정
- 암호화 상태 보기 (자체 암호화 드라이브가 있는 컴퓨터)

DDP Console

DDP Console 은 자격 증명을 등록 및 관리하고 자체 복구 질문을 구성할 수 있는 인터페이스입니다 .

다음과 같은 응용프로그램에 액세스할 수 있습니다 .

- 암호화 상태 도구는 사용자가 컴퓨터 드라이브의 암호화 상태를 볼 수 있는 응용 프로그램입니다 .
- 등록 도구는 사용자가 자격 증명을 설정 및 관리하고, 자체 복구 질문을 구성하고, 자신의 자격 증명 등록 상태를 볼 수 있는 응용 프로그램입니다 . 사용자는 관리자가 설정한 정책에 따라 각 유형의 자격 증명을 등록할 수 있습니다 .
- Password Manager는 사용자가 웹 사이트, Windows 응용 프로그램 및 네트워크 리소스에 로그온하는 데 필요한 데이터를 자동으로 입력하여 제출할 수 있는 응용 프로그램입니다 . 또한 Password Manager 를 통해 사용자가 로그온 암호를 변경하고 Password Manager 에서 유지 관리하는 암호가 대상 리소스와 동기화되도록 유지할 수 있습니다 .

이 안내서에서는 이러한 각 응용프로그램을 사용하는 방법에 대해 설명합니다 .

dell.com/support 에서 업데이트된 설명서가 있는지 정기적으로 확인하십시오 .

ProSupport 에 문의

지원받기 위해 Dell ProSupport 로 문의하기 전에 , 올바른 기술 전문가에게 신속히 연결될 수 있도록 전화할 때 서비스 태그를 준비하십시오 .

ProSupport 에 문의하려면 , 877-459-7304(내선번호 4310039) 로 전화하여 Dell Data Protection 제품에 대한 연중무휴 하루 24 시간 전화 지원을 받으십시오 .

dell.com/support 에서 Dell Data Protection 제품에 대한 온라인 지원도 가능합니다 . 온라인 지원에는 드라이버 , 매뉴얼 , 기술 자문 , FAQ 및 최근에 나타나는 문제도 포함됩니다 .

2

DDP Console

DDP Console 은 모든 컴퓨터 사용자가 컴퓨터 드라이브 및 파티션의 암호화 상태를 보고 관리하며 , 관리자의 정책에 따라 웹 사이트 , 프로그램 , 네트워크 리소스에 대한 로그온을 관리하고 , 인증 자격 증명을 쉽게 등록할 수 있도록 안전하게 응용 프로그램에 액세스하는 방법을 제공합니다 .

DDP Console 을 열려면 *데스크톱*에서 **DDP Console** 아이콘을 더블 클릭합니다 .

DDP Console 이 시작되면 홈 페이지에 다음과 같이 Security Tools 응용 프로그램이 나타납니다 .

- 암호화 상태
- 등록
- Password Manager

처음으로 자격 증명을 설정하려면 등록 타일에 있는 **시작하기** 링크를 선택합니다 . 마법사가 간단한 등록 절차를 안내합니다 . 자세한 정보는 자격 증명 최초 등록 섹션을 참조하십시오 .

탐색

응용 프로그램에 액세스하려면 해당 타일을 클릭합니다 .

제목 표시줄

응용 프로그램 내에서 홈 페이지로 돌아가려면 제목 표시줄의 왼쪽 모서리에서 활성 응용 프로그램의 이름 옆에 있는 뒤로 화살표를 클릭합니다 .

다른 응용 프로그램을 직접 탐색하려면 활성 응용 프로그램 이름 옆에 있는 아래쪽 화살표를 클릭하고 응용 프로그램을 선택합니다 .

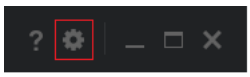
DDP Console 을 최소화하거나 , 최대화하거나 , 닫으려면 제목 표시줄의 오른쪽 모서리에서 해당 아이콘을 클릭합니다 .

DDP Console 을 최소화한 후 복원하려면 해당 시스템 트레이 아이콘을 더블 클릭합니다 .

도움말을 열려면 제목 표시줄에서 **?** 를 클릭합니다 .

DDP Console 상세정보

DDP Console, 정책 , 실행 중인 서비스 및 로그에 대한 상세정보를 보려면 제목 표시줄의 왼쪽에 있는 기어 아이콘을 클릭합니다 . 이 정보는 관리자가 기술 지원을 제공하는 데 필요할 수 있습니다 .



메뉴에서 항목을 선택합니다 .

메뉴 항목	용도
정보	버전 및 저작권 정보가 포함되어 있습니다 .
정보 표시	다음 정보가 포함되어 있습니다 . • 제품 버전 및 날짜 정보 • 이 컴퓨터에서 DDP Console 이 엔터프라이즈 또는 로컬 관리자에 의해 관리되는지 여부 • 운영 체제 , BIOS, 마더보드 및 TPM(Trusted Platform Module) 의 버전 번호
MS 정보	Microsoft Windows 시스템 정보 유틸리티를 실행하여 하드웨어 , 구성 요소 및 소프트웨어 환경에 대한 세부 정보를 표시합니다 .
복사 정보	모든 시스템 정보를 클립보드에 복사하여 관리자 또는 Dell ProSupport 에 보낼 수 있도록 이메일에 붙여 넣습니다 .
피드백	사용자가 이 제품에 대한 피드백을 Dell 에 제공할 수 있는 양식을 표시합니다 .
정책	이 컴퓨터에 적용되는 정책 계층을 표시합니다 .
서비스	실행 중인 서비스에 대한 상세정보를 표시합니다 .
지원	Dell ProSupport 웹 사이트에 연결합니다 .
로그	문제 해결을 위해 세부적인 로그 이벤트 목록을 표시합니다 .

3

암호화 상태

암호화 페이지에는 컴퓨터의 암호화 상태가 표시됩니다 . 디스크 , 드라이브 또는 파티션이 암호화되어 있지 않으면 상태는 *보호되지 않음*이라고 표시됩니다 . 드라이브 또는 파티션이 암호화되어 있으면 상태가 *보호됨*으로 표시됩니다 .

암호화 상태를 업데이트하려면 해당 디스크 , 드라이브 또는 파티션을 마우스 오른쪽 버튼으로 클릭한 후 **새로 고침**을 선택합니다 .

4

등록

등록 도구를 사용하면 사용자가 관리자 정책에 따라 자격 증명을 등록하거나 , 등록 상태를 수정 및 확인할 수 있습니다 .

DDP Consol 에 자격 증명을 처음 등록할 때 마법사가 암호 변경 , 복구 질문 , 지문 , 모바일 장치 및 스마트 카드를 등록할 수 있도록 안내해줍니다 . 정책에 따라 자격 증명을 각각 등록하거나 건너뛸 수 있습니다 . 초기 등록 후 등록 타일을 클릭하여 자격 증명을 추가하거나 수정할 수 있습니다 .

자격 증명 최초 등록

자격 증명을 처음으로 등록하려면 다음을 수행합니다 .

1. DDP Console 홈 페이지에서 등록 타일의 **시작하기** 링크를 클릭합니다 .
2. 시작 페이지에서 , **다음**을 클릭합니다 .
3. 인증 필요 대화 상자에서 Windows 암호를 사용하여 로그인하고 **확인**을 클릭합니다 .
4. 암호 페이지에서 Windows 암호를 변경하려면 새 암호를 입력한 후 확인하고 **다음**을 클릭합니다 .

   암호 변경을 건너뛰려면 **건너뛰기**를 클릭합니다 . 등록을 원하지 않을 때는 마법사에서 자격 증명을 건너뛸 수 있습니다 . 페이지로 돌아가려면 **뒤로**를 클릭합니다 .
5. 각 페이지의 지침을 수행하고 **다음** , **건너뛰기** 또는 **뒤로**와 같은 해당 버튼을 클릭합니다 .
6. 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 등록에 대한 자세한 정보를 알고 싶거나 자격 증명을 변경하려면 등록 추가 , 수정 또는 보기 섹션을 참조하십시오 .

등록 추가 , 수정 또는 보기

등록을 추가하거나 , 수정하거나 , 보려면 **등록** 타일을 클릭합니다 .

왼쪽 창의 탭에 사용 가능한 등록이 나열됩니다 . 나열되는 등록은 플랫폼 또는 하드웨어 유형에 따라 다릅니다 .

상태 페이지에 지원되는 자격 증명 , 해당 정책 설정 (필수 또는 해당 없음), 등록 상태가 표시됩니다 . 사용자가 관리자 정책에 따라 자신의 등록을 관리하는 것도 이 페이지에서 이루어집니다 .

- 처음 자격 증명을 등록하는 경우에는 해당 자격 증명 라인의 **등록**을 클릭합니다 .
- 기존에 등록된 자격 증명을 삭제하려면 **삭제**를 클릭합니다 .
- 정책에 따라 사용자가 보유한 자격 증명을 등록하거나 수정할 수 없는 경우 상태 페이지의 **등록** 및 **삭제** 링크가 비활성화됩니다 .
- 기존 등록을 변경하려면 왼쪽 창에서 해당 탭을 클릭합니다 .

  정책에 따라 자격 증명을 등록하거나 수정할 수 없는 경우 자격 증명의 등록 페이지에 " 정책에 의해 자격 증명 수정이 허용되지 않음 " 이라는 메시지가 표시됩니다 .

암호

Windows 암호를 변경하려면 다음을 수행합니다 .

1. **암호** 탭을 클릭합니다 .
2. 현재 Windows 암호를 입력합니다 .
3. 새 암호를 입력하고 확인을 위해 한 번 더 입력한 다음 **변경**을 클릭합니다 .

   변경된 암호가 즉시 적용됩니다 .
4. 등록 성공 대화 상자에서 **확인**을 클릭합니다 .

주 : Windows 암호는 Windows 에서 변경하는 것이 아니라 DDP Console 에서만 변경해야 합니다 . DDP Console 이 아닌 다른 곳에서 Windows 암호를 변경한 경우 암호 불일치로 인해 복구 작업이 필요합니다 .

복구 질문

복구 질문 페이지에서는 복구 질문과 답변을 생성 , 삭제 또는 변경할 수 있습니다 . 복구 질문은 암호가 만료되었거나 암호를 잊은 경우 등을 위해 사용자가 질의 응답 방식으로 Windows 계정에 액세스할 수 있는 기능입니다 .

주 : 복구 질문은 컴퓨터에 대한 액세스 권한을 복구하는 경우에만 사용되며 , 질문과 답변은 로그온하는 데 사용할 수 없습니다 .

아직 등록한 복구 질문이 없는 경우 다음을 수행합니다 .

1. **복구 질문** 탭을 클릭합니다 .
2. 미리 정의된 질문 목록에서 질문을 선택한 후 답변을 입력하고 확인을 위해 한 번 더 입력합니다 .
3. **등록**을 클릭합니다 .

주 : 이 페이지의 선택 항목을 지우고 다시 시작하려면 **재설정** 단추를 클릭하십시오 .

복구 질문이 이미 등록되어 있을 경우

복구 질문이 이미 등록되어 있더라도 복구 질문을 삭제하거나 다시 등록할 수 있습니다 .

1. **복구 질문** 탭을 클릭합니다 .
2. 다음과 같이 적절한 버튼을 클릭합니다 .
   - 복구 질문을 완전히 제거하려면 **삭제**를 클릭합니다 .
   - 복구 질문과 답변을 다시 정의하려면 **다시 등록**을 클릭합니다 .

지문

주 : 이 기능을 사용하려면 컴퓨터에 지문 판독기가 있어야 합니다 .

지문 등록 방법은 다음과 같습니다 .

1. **지문** 탭을 클릭합니다 .
2. 지문 페이지에서 등록할 손가락을 클릭합니다 .
3. 화면에 나타나는 지시에 따라 지문을 등록합니다 .

주 : 손가락이 4 회 성공적으로 스캔되어야만 등록을 마칠 수 있습니다 . 지문 등록을 완료하는 데 필요한 스캔 횟수는 각 스캔의 품질에 따라 다릅니다 . 지문의 최소 및 최대 개수는 관리자가 미리 정의합니다 .

4 정책에 따라 필요한 최소 지문 개수가 등록될 때까지 다음 손가락을 각각 클릭하여 스캔합니다 .

최소 지문 개수를 등록하지 않으면 대화 상자가 표시되어 알려줍니다 . 계속하려면 **확인**을 클릭합니다 .

5 필요한 개수의 지문 스캔을 완료하고 **저장**을 클릭합니다 .

스캔한 지문을 삭제하려면 지문 등록 페이지에서 등록을 취소할 강조 표시된 지문을 클릭하고 **예**를 클릭하여 삭제를 확인한 후 **저장**을 클릭합니다 .

모바일 장치

모바일 장치 등록에서는 OTP(일회용 암호) 기능을 사용할 수 있습니다 . OTP 를 사용하면 사용자가 컴퓨터와 페어링된 모바일 장치에서 Security Tools Mobile 앱을 통해 생성한 암호를 사용하여 Windows 에 로그온할 수 있습니다 . 또는 정책에 따라 허용되면 암호가 만료되거나 분실된 경우 OTP 기능을 사용하여 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다 .

주 : 컴퓨터의 구성에서 이를 지원하지 않거나 관리자가 설정한 정책에서 허용하지 않는 경우에는 DDP Console 에 모바일 장치 탭이 표시되지 않습니다 .

주 : 암호가 만료되거나 분실된 경우 , 정책 설정에 따라 컴퓨터에 대한 액세스 권한 복구 또는 로그온과 같이 OTP 기능을 사용할 수 있는 방법이 결정됩니다 . 하지만 로그온과 복구를 동시에 수행할 수는 없습니다 .

OTP 기능을 이용하려면 먼저 모바일 장치를 컴퓨터에 등록 (페어링) 해야 합니다 . 한 대의 컴퓨터에 사용자가 여러 명인 경우에도 사용자마다 모바일 장치 1 개를 컴퓨터에 등록할 수 있습니다 . 모바일 장치를 여러 컴퓨터에 등록하는 것도 가능합니다 .

장치가 이미 등록되어 있을 때 새 장치를 등록하면 자동으로 이전 장치가 언페어링됩니다 .

DDP Console 에서 :

1 DDP Console 등록 페이지에서 **모바일 장치** 탭을 클릭합니다 .

2 오른쪽 상단에서 **등록**을 클릭합니다 .

일회용 암호 등록 페이지가 열립니다 .

3 처음 페어링하는 컴퓨터인 경우 **예**를 선택합니다 .

a 모바일 장치에서 , App Store 에 있는 Dell Data Protection | Security Tools Mobile 앱을 다운로드합니다 .

b 컴퓨터에서 **다음**을 클릭합니다 .

Security Tools Mobile 설정

1 Security Tools Mobile 앱을 엽니다 .

2 PIN 을 만들어 입력하고 Security Tools Mobile 앱에 액세스합니다 .

주 : 모바일 장치가 잠겨있지 않더라도 정책에 따라 PIN 이 필요할 수도 있습니다 . 모바일 장치의 잠금 해제에 PIN 을 사용하지 않더라도 Security Tools Mobile 앱에 액세스하려면 PIN 이 필요합니다 .

3 **컴퓨터 등록**을 선택합니다 . (필요한 경우 , 모바일 화면 왼쪽 상단을 눌러 명령어에 액세스합니다 .)

코드가 모바일 장치에 표시됩니다 . 코드 길이와 영숫자 조합은 관리자 정책에 따라 다릅니다 .

모바일 장치와 컴퓨터 페어링

1 컴퓨터의 DDP Console 모바일 코드 페이지에서 :

a 모바일 장치의 코드를 해당 필드에 입력합니다 .

b **다음**을 클릭합니다 .

c 장치 페어링 페이지에서 다음 중 하나를 선택합니다 .

QR 코드 - QR 코드가 표시됩니다 .

또는

직접 입력 - 24 자리 페어링 코드가 표시됩니다 .

2 모바일 장치에서 :

a **장치 페어링**을 누릅니다 .

b 컴퓨터에서 선택한 것과 동일한 페어링 옵션 (**QR 코드 스캔** 또는 **직접 입력**) 을 선택합니다 .

c 다음 중 하나를 선택합니다 .

- **QR 코드** Code 의 경우 , QR 코드를 스캔할 컴퓨터 화면 앞에 모바일 장치를 놓습니다 .
  모바일 장치에 표시되는 숫자 인증 코드를 확인하고 **다음**을 누릅니다 .

주 : *스캔 도중 문제가 발생하였습니까 ?* 바가 표시되면 다시 시도하거나 **직접 입력**을 선택하십시오 .

- **직접 입력**의 경우 , 컴퓨터에서 나온 24 자리 페어링 코드를 입력하고 **완료**를 누릅니다 .
  모바일 장치에 표시되는 숫자 인증 코드를 확인하고 **다음**을 누릅니다 .

3 컴퓨터의 DDP Console 에서 :

a **다음**을 클릭합니다 .

b 모바일 장치에 표시된 인증 코드를 입력하고 **다음**을 클릭합니다 .

c 필요한 경우 모바일 장치의 이름을 수정합니다 .

d **적용**을 클릭합니다 .
장치가 페어링됩니다 .

4 모바일 장치에서 :

a **계속**을 누릅니다 .

b 필요한 경우 컴퓨터의 이름을 수정하고 **완료**를 누릅니다 .

c **마침**을 누릅니다 .

다른 모바일 장치 등록

새 장치를 등록하면 이전 장치의 페어링이 자동으로 해제됩니다 . 페어링을 해제하는 데 별도의 단계를 수행할 필요가 없습니다 .

컴퓨터와 모바일 장치 페어링 해제

다른 장치를 등록하지 않고 컴퓨터와 모바일 장치의 페어링을 해제하려면 다음 중 하나를 선택합니다 .

- DDP Console 에서 : 등록 상태 페이지에서 모바일 장치 자격 증명 옆의 **삭제**를 클릭합니다 .
- 모바일 장치에서 :
  1. Security Tools Mobile 앱을 실행합니다 .
  2. 왼쪽 상단에서 메뉴 표시줄을 눌러 드로어를 엽니다 .
  3. **컴퓨터 삭제**를 누릅니다 .
  4. 페어링을 해제할 컴퓨터를 선택합니다 .
  5. **제거** (Android) 를 선택하거나 **완료** (iOS) 를 누릅니다 .

     확인 메시지가 나타납니다 .
  6. 등록된 모든 컴퓨터를 장치에서 제거하려면 **모두 제거**를 선택합니다 .
     모두 제거 옵션은 여러 대의 컴퓨터를 제거하거나 , 페어링된 컴퓨터만 제거하는 경우에 나타납니다 .
     - 등록된 컴퓨터를 제거하고 PIN 을 제거하려면 **기본 설정값 복원**을 선택합니다 . 기본 설정값을 복원하면 등록된 컴퓨터 모두와 Security Tools Mobile 앱에 액세스할 때 사용하는 PIN 이 제거됩니다 .
     - 등록된 컴퓨터에서 나가려면 **취소**를 선택합니다 .

일회용 암호를 사용하여 로그온

주 : OTP 인증은 Windows 로그온에만 사용할 수 있습니다 .

OTP 를 사용하여 잠긴 컴퓨터에 대한 액세스 권한을 다시 얻을 수 있도록 복구하거나 , Windows 로그온을 수행할 수 있으며 , 둘 다 수행할 수는 없습니다 .

정책에서 허용하고 로그온 화면에 OTP 기호 가 표시되는 경우 OTP 를 사용하여 Windows 에 로그온할 수 있습니다 .

OTP 를 사용하여 로그온하려면 다음을 수행합니다 .

1 컴퓨터의 Windows 로그온 화면에서 OTP 아이콘 을 선택합니다 .

2 모바일 장치에서 Security Tools Mobile 앱을 열고 PIN 을 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 ***Security Tools*** 가 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 .

주 : 필요한 경우 새로 고침 기호 를 클릭하여 새 코드를 가져옵니다 . 첫 번째 두 개의 OTP 가 새로 고침된 후 다른 OTP 가 생성될 때까지 30 초 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 30 초를 기다린 후 다시 시도하십시오 .

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

OTP 를 복구 목적으로 사용한 경우에는 컴퓨터에 대한 액세스 권한을 다시 얻은 후 화면 지침에 따라 암호를 재설정하십시오 .

Security Tools Mobile 관리 작업

이 작업은 모바일 장치의 Security Tools Mobile 앱을 통해 수행됩니다 .

Security Tools Mobile 앱 PIN 재설정

Security Tools Mobile 앱 PIN 을 재설정하려면 다음을 수행합니다 .

1 오른쪽 상단의 메뉴 옵션을 누릅니다 .

2 **PIN 재설정**을 선택합니다 .

3 새 PIN 을 입력하고 확인을 위해 한 번 더 입력합니다 .

Security Tools Mobile 앱 제거

모바일 장치에서 :

1 장치와 컴퓨터를 언페어링합니다 .

2 모바일 장치에서 일반적으로 앱을 삭제하는 방식으로 Security Tools Mobile 앱을 삭제하거나 설치 제거합니다 .

스마트 카드

주 : 이 기능을 사용하려면 컴퓨터에 스마트 카드 판독기가 필요합니다 .

스마트 카드 등록 방법은 다음과 같습니다 .

1. **스마트 카드** 탭을 클릭합니다 .
2. 카드 유형에 따라 다음과 같이 스마트 카드를 등록합니다 .
   - 스마트 카드를 카드 판독기에 삽입합니다 .
   - 비접촉식 카드의 경우 카드를 판독기 위에 , 혹은 가까이 놓고 기다립니다 .
3. 카드가 감지되면 녹색 확인란과 *카드 등록*이 표시됩니다 . **카드 등록**을 선택합니다 .
4. 등록 성공 대화 상자에서 **확인**을 클릭합니다 .

사용자에게 등록되어 있는 스마트 카드를 모두 해제하려면 스마트 카드 등록 페이지에서 **계정에서 등록된 카드 제거**를 선택합니다 .

5

Password Manager

Password Manager 를 사용하면 웹 사이트 , Windows 프로그램 및 네트워크 리소스에 자동으로 로그온하고 하나의 도구에서 로그온 자격 증명을 관리할 수 있습니다 . 또한 Password Manager 를 통해 사용자가 로그온 암호를 변경하고 Password Manager 에서 유지 관리하는 암호가 대상 리소스와 동기화되도록 유지할 수 있습니다 .

Password Manager 는 Internet Explorer 및 Mozilla Firefox 에서 지원되며 , Microsoft 계정 (이전의 Windows Live ID) 에서는 지원되지 않습니다 .

주 : Password Manager 를 Firefox 에서 실행하려면 Password Manager 확장 프로그램을 설치하고 등록해야 합니다 . Mozilla Firefox 에 확장 프로그램을 설치하는 방법은 https://support.mozilla.org/ 를 참조하십시오 .

주 : Mozilla Firefox 의 Password Manager 아이콘 사용법 (사전 트레이닝 및 트레이닝 아이콘) 은 Microsoft Internet Explorer 에서의 사용법과 다릅니다 .

- Password Manager 아이콘의 더블 클릭 기능은 사용할 수 없습니다 .
- 드롭다운 컨텍스트 메뉴에 기본 작업이 굵게 표시되지 않습니다 .
- 페이지에 로그온 양식이 여러 개 있으면 Password Manager 아이콘이 여러 개 표시될 수 있습니다 .

주 : 웹 로그온 페이지의 구조는 계속해서 변경되므로 Password Manager 가 일부 웹 사이트를 지원하지 않을 수도 있습니다 .

Password Manager 시작하기

Password Manager 는 사용자가 작업을 수행할 때 사용자의 로그온 자격 증명을 수집하여 저장합니다 . Security Tools 가 설치된 직후 Password Manager 를 사용할 수 있습니다 . 로그온 페이지에 자격 증명을 입력하면 Password Manager 가 로그온 양식을 감지하여 Password Manager 의 자격 증명 저장 여부를 선택할 수 있습니다 .

선택할 수 있는 옵션은 아래와 같이 세 가지입니다 .

- **로그온 저장**을 클릭하여 로그온 자격 증명을 Password Manager 에 저장합니다 .
- 로그온을 저장하지 ***않으면*** 웹 사이트 또는 프로그램에 로그온할 때마다 로그온 자격 증명을 다시 저장하라는 메시지가 표시됩니다 . 메시지가 표시되지 않도록 하려면 **이 사이트에서는 표시하지 않음**을 선택합니다 . 웹 사이트 제외 목록에 레코드가 생성됩니다 . 자세한 내용은 웹 사이트 제외를 참조하십시오 .
- 자격 증명을 저장하지 않으려면 **로그온을 저장하지 않음**을 클릭합니다 .

이 대화 상자는 이전에 웹 사이트 또는 프로그램에 대해 자격 증명을 저장했지만 , 다른 사용자 이름이나 암호를 입력하는 경우에도 표시됩니다 . 새 사용자 이름을 사용할 경우 **로그온 저장**을 선택하면 새 자격 증명 세트가 저장됩니다 . 이전에 저장한 사용자 이름과 새 암호를 사용할 경우 **로그온 저장**을 선택하면 원래 자격 증명이 새 암호로 업데이트됩니다 .

로그온 관리

로그온 관리자를 사용하면 웹 사이트 , Windows 프로그램 및 네트워크 리소스에 대한 모든 로그온을 쉽게 중앙에서 관리할 수 있습니다 .

로그온 관리자를 열려면 다음을 수행합니다 .

1 DDP Console 홈 페이지에서 **Password Manager** 타일을 클릭합니다 .

2 **로그온 관리자** 탭을 클릭합니다 .

아래와 같이 로그온 및 범주를 추가하여 정렬하고 필터링할 수 있습니다 .

- 로그온 추가 - 새로운 로그온 자격 증명 세트를 추가합니다 . 정책에 따라 , 로그온을 추가하려면 Security Tools 에 저장된 자격 증명을 입력해야 할 수도 있습니다 .
- 범주 추가 - 정렬 및 필터링을 목적으로 새로운 범주 (이메일 , 스토리지 , 뉴스 , 기업 리소스 , 소셜 미디어 등) 를 추가합니다 .

정렬 : 계정 , 사용자 이름 또는 범주별로 로그온을 정렬합니다 . 열 제목을 클릭하면 해당 열을 따라 정렬됩니다 .

필터 : 선택한 범주에 속하는 로그온을 제외하고 모두 숨기려면 *보기* 목록에서 범주를 선택합니다 . 필터를 제거하려면 *모두*를 선택합니다 .

다음과 같이 로그온을 관리할 수 있습니다 .

- 시작 - 웹 사이트 또는 프로그램을 열고 사용자 설정을 기반으로 로그온 자격 증명을 제출합니다 .
- 편집 - 웹 사이트 또는 프로그램의 저장된 로그온 데이터를 변경할 수 있습니다 .
- 삭제 - Password Manager 에서 저장된 로그온 데이터를 제거할 수 있습니다 .
- 추가 - 새 로그온 , 범주 또는 새 로그온 데이터를 추가할 수 있습니다 .

범주 추가

로그온을 생성할 때 분류할 수 있도록 로그온을 추가하기 전에 범주 (예 : 이메일 , 스토리지 , 뉴스 , 기업 리소스 및 소셜 미디어) 를 만듭니다 . 그런 다음 로그온을 범주별로 정렬하고 필터링할 수 있습니다 .

범주를 추가하려면 로그온 관리자 페이지에서 **범주 추가**를 클릭하고 범주 이름을 입력한 후 **저장**을 클릭합니다 .

로그온 추가

1 로그온 관리자 페이지에서 **로그온 추가**를 클릭합니다 .

로그온을 추가하려면 정책에 따라 인증이 필요할 수도 있습니다 .

2 웹 사이트 또는 프로그램을 열어 로그온합니다 .

3 로그온 추가 대화 상자에서 **계속**을 클릭합니다 .

4 다음에 표시되는 대화 상자에서 아래의 정보를 입력합니다 .

- **범주** - 정렬할 웹 사이트 또는 프로그램 로그온에 대한 범주를 선택합니다 . 범주를 추가하지 않은 경우에는 이 목록이 비어 있습니다 .
- **계정 이름** - 미리 입력된 이름을 그대로 사용하거나 , 웹 사이트 또는 프로그램의 이름을 입력합니다 .
- **감지되지 않은 제목** - 이러한 필드는 Password Manager 에 의해 사용자가 로그온 페이지에서 로그온 정보를 입력하는 필드로 감지됩니다 . 일반적으로 이 필드에는 사용자 이름 또는 이메일과 암호가 포함됩니다 .

5 필드 이름이 검색되지 않는 제목으로 표시되거나 , 로그온 필드로 잘못된 필드가 포함된 경우에는 **추가 필드** 버튼을 클릭하여 필드 이름을 편집하거나 필드를 제거합니다 .

6 추가 필드 대화 상자에서 **감지되지 않은 제목**을 클릭하고 각 필드에 대해 올바른 필드 이름을 입력합니다.

추가 필드 대화 상자가 표시되면 필드의 이름을 변경하는 데 도움이 되도록 로그온 추가 대화 상자에서 활성 상태인 필드가 강조 표시됩니다.

로그온하는 데 필드가 필요하지 않은 경우 로그온 정보에서 제외하려면 해당 필드의 확인란을 선택 해제합니다.

7 변경 내용을 저장하려면 **확인**을 클릭합니다.

8 로그온 추가 대화 상자에서 로그온하는 데 필요한 필드를 완료합니다.

주: 기존 로그온이 저장되므로 웹 사이트 또는 프로그램의 암호 변경 기능으로 이동해야 암호를 변경할 수 있습니다.

9 Password Manager 가 로그온 정보를 자동으로 채우고 제출하도록 하려면 **로그인 데이터를 자동으로 제출**을 선택합니다.

10 **저장**을 클릭합니다.

로그온 관리자 페이지에 웹 사이트 또는 프로그램 로그온이 표시됩니다.

자격 증명 가져오기

웹 브라우저에 저장된 자격 증명을 Password Manager 로 가져올 수 있습니다.

1 Password Manager 도구에서 **자격 증명 가져오기**를 선택합니다.

2 가져올 브라우저를 선택하고 **스캔**을 클릭합니다.

3 메시지가 프롬프트되면 선택한 브라우저의 암호를 입력합니다.

주: 가져오기를 실행해도 암호를 가져오지 못하는 경우에는 브라우저에 가져올 수 있는 데이터가 저장되어 있는지 확인해야 합니다. Firefox 를 사용하고 있다면 Sync 에 로그온합니다. 자격 증명 가져오기를 다시 시도하십시오.

아이콘의 상황에 맞는 메뉴

웹 사이트 또는 프로그램을 방문하면 Password Manager 아이콘이 표시됩니다.

는 로그온 양식을 트레이닝할 수 있다는 것을 나타냅니다.

가 표시되지 않으면 로그온 양식이 이미 트레이닝 된 것입니다. 아이콘을 더블 클릭하여 프로그램 또는 웹 사이트에 로그온합니다.

아이콘을 클릭하면 로그온 양식의 트레이닝 여부에 따라 컨텍스트 메뉴에 서로 다른 옵션이 표시됩니다.

현재 로그온 필드가 트레이닝되지 않은 경우 컨텍스트 메뉴에 다음 옵션이 표시됩니다.

Password Manager 에 추가	로그온 추가 대화 상자를 엽니다.
아이콘 설정	사용자가 트레이닝 가능한 로그온 페이지에서 Password Manager 아이콘의 표시를 구성할 수 있습니다.
Password Manager 열기	*Password Manager 관리* 도구를 시작하고 로그온 관리자 페이지를 엽니다.
도움말	온라인 도움말이 열립니다.

현재 로그온 필드가 이미 트레이닝되었기 때문에 다음과 같은 옵션이 컨텍스트 메뉴에 표시됩니다.

로그온 데이터 채우기	로그온 양식을 트레이닝하면서 선택한 사항에 따라 자동으로 로그온되거나, 로그온 데이터를 제출할 수 있도록 사용자 이름과 암호 필드를 채웁니다.
로그온 편집	로그온 편집 대화 상자가 열립니다.
로그온 추가	로그온 추가 대화 상자가 열립니다.

Password Manager 열기	로그온 관리자 페이지가 열립니다 .
도움말	온라인 도움말이 열립니다 .

Password Manager 아이콘이 로그온 양식과 함께 표시되지 않으면 브라우저의 암호 저장 기능을 다음과 같이 비활성화합니다 .

- Mozilla Firefox 인 경우 : 메뉴 아이콘 > 옵션 > 보안 > **사이트에 입력하는 암호 기억** 확인란 선택 취소
- Internet Explorer 인 경우 : 기어 아이콘 > 인터넷 옵션 > 내용 탭 > 자동 완성 설정 > **양식에 사용할 사용자 이름과 암호** 확인란 선택 취소

트레이닝된 로그온 페이지 로그온

웹 사이트 또는 프로그램 로그온을 열면 Password Manager 가 페이지가 트레이닝되었는지 여부를 감지합니다 . 트레이닝된 경우 로그온 영역에 Password Manager 아이콘이 표시됩니다 . 트레이닝되지 않은 경우 트레이닝되지 않은 양식에 대한 프롬프트가 비활성화되어 있지 않으면 Password Manager 아이콘이 표시됩니다 .

로그온하려면 다음 중 하나를 선택합니다 .

- 등록된 자격 증명을 스캔합니다 . 지문이나 스마트 카드를 등록한 경우에는 등록된 지문을 지문 판독기와 접촉하거나 등록된 카드를 카드 판독기에 제시합니다 .
- Password Manager 아이콘을 클릭하고 컨텍스트 메뉴에서 **로그온 데이터 채우기**를 선택합니다 .
- 다음과 같이 Password Manager 단축키 조합을 누릅니다 . **Ctrl+Win+H**. Password Manager 팝업에 트레이닝된 사이트가 표시되어 빠르게 사이트를 시작할 수 있습니다 .

주 : 단축기 조합은 DDP Console > Password Manager > 설정에서 변경 가능합니다 .

사이트 또는 프로그램에 대해 둘 이상의 로그온이 저장된 경우 사용할 계정을 선택하라는 메시지가 표시됩니다 .

웹 도메인 지원

특정 웹 도메인의 로그온 페이지를 트레이닝하였지만 다른 로그온 페이지에서 해당 웹 도메인 계정에 액세스하려는 경우에는 새로운 로그온 페이지로 이동합니다 . 이때 기존 로그온을 사용할 것인지 또는 Password Manager 에 새 로그온을 추가할 것인지를 묻는 메시지가 나타납니다 .

- *로그온 사용*을 클릭하면 이전에 생성한 계정으로 로그온됩니다 . 다음에 새 로그온 페이지에서 해당 계정에 액세스하면 이전에 생성된 계정으로 자동 로그온됩니다 .
- *로그온 추가*를 클릭하면 로그온 추가 대화 상자가 표시됩니다 .

Windows 자격 증명 채우기

일부 프로그램에서는 Windows 자격 증명을 사용하여 로그온할 수 있습니다 .

사용자 이름과 암호를 입력하지 않고 *로그온 추가* 및 *로그온 편집* 대화 상자의 드롭다운 메뉴에서 Windows 자격 증명을 선택합니다 .

사용자 이름은 다음 형식 중 하나를 선택합니다 .

- Windows 사용자 이름
- Windows 사용자 기본 이름
- Windows 도메인 \ 사용자 이름
- Windows 도메인

암호는 Windows 암호를 사용합니다 .

이 옵션은 수정할 수 없습니다 .

기존 암호 사용

Password Manager 에서 암호를 변경했을 가능성도 있지만 이때 프로그램은 새 암호를 거부합니다 . 이 경우 프로그램에서 최신 암호 대신 기존 암호 (이전에 이 로그온 페이지에 입력한 암호) 를 사용할 수 있습니다 .

암호 이력을 선택합니다 . 인증이 되고 나면 , 암호 이력 목록에서 예전 암호를 선택하라는 프롬프트가 표시됩니다 . 이 목록에는 일곱 개의 암호가 포함되어 있습니다 .

웹 사이트 제외

웹 사이트가 Password Manager 에 의해 관리되지 않도록 하려면 **웹 사이트 제외** 탭을 클릭합니다 .

제외된 웹 사이트의 특징은 다음과 같습니다 .

- Password Manager 아이콘이 호출되지 않습니다 .
- 사용자가 자동으로 로그인되지 않습니다 .
- 암호 미리 알림 메시지를 표시하지 않습니다 .

제외 목록에 새 웹 사이트를 추가하려면 다음을 수행합니다 .

1. **웹 사이트 제외** 탭을 클릭합니다 .
2. **웹 사이트 추가**를 클릭합니다 .
3. 제외할 웹 사이트의 URL 을 입력합니다 .
4. **저장**을 클릭합니다 .

웹 사이트를 제외하면 해당 웹 사이트가 Password Manager 에서 관리되지 않습니다 . 제외를 복원하려면 웹 사이트 제외 목록에서 웹 사이트를 삭제하기만 하면 됩니다 . 제외 목록에서 웹 사이트를 제거하려면 ✕를 클릭합니다 .

웹 사이트를 여러 개 추가한 후 다음을 수행할 수 있습니다 .

- 목록을 웹 사이트별로 오름차순 또는 내림차순으로 정렬하려면 웹 사이트 열 머리글을 클릭합니다 .
- 목록 내에서 검색하려면 검색 필드에 URL 의 일부를 입력합니다 . 입력 내용에 따라 목록이 필터링됩니다 .

로그온 양식을 트레이닝하라는 프롬프트 메시지 비활성화

기존에 트레이닝된 로그온을 유지할 수 있지만 새로운 로그온 양식을 트레이닝하라는 프롬프트 메시지를 비활성화할 수도 있습니다 .

새로운 로그온 프롬프트 메시지의 비활성화 방법 :

1 DDP 보안 콘솔을 엽니다 .

2 Password Manager 타일을 클릭합니다 .

3 **설정** 탭을 클릭합니다 .

4 **로그온 화면에 있을 때 로그온을 추가하라는 메시지 표시** 확인란을 선택 취소합니다 .

Password Manager 자격 증명 백업 및 복원

Password Manager 에서 관리하는 로그온 데이터를 안전하게 백업할 수 있습니다 . 이 데이터는 Password Manager 가 보호하는 모든 컴퓨터에서 복원할 수 있습니다 .

주 : 백업되는 Password Manager 데이터에 운영 체제나 PBA(부팅 전 인증) 로그온 자격 증명 또는 지문과 같은 자격 증명별 정보는 포함되지 않습니다 .

자격 증명 백업

자격 증명을 백업하려면 다음을 수행합니다 .

1 **자격 증명 백업** 탭을 클릭하여 백업 프로세스를 설정합니다 .

2 **찾아보기**를 클릭하고 원하는 백업 위치로 이동합니다 .

데이터를 로컬 드라이브에 백업할 때는 휴대용 스토리지나 네트워크 드라이브에 데이터를 백업하라는 권장 사항이 표시됩니다 .

3 암호를 입력하고 확인합니다 . 이번에 백업된 자격 증명을 나중에 복원해야 할 경우 이 암호를 사용해야 합니다 .

4 **백업**을 클릭합니다 .

5 Windows 암호를 입력하십시오 .

6 성공 대화 상자에서 **확인**을 클릭합니다 .

주 : 실행한 백업 작업의 텍스트 로그를 보려면 을 클릭하고 **로그**를 선택합니다 .

자격 증명 복구

자격 증명을 복구하려면 백업 위치가 유효해야 합니다 .

자격 증명 복구 방법 :

1 **자격 증명 복구** 탭을 클릭합니다 .

2 **찾아보기**를 클릭하여 백업 파일로 이동한 다음 파일 암호를 입력합니다 .

3 **복구**를 클릭합니다 .

경고 : Password Manager 데이터를 복구하면 기존 데이터를 덮어쓰게 됩니다 . 백업 생성 후 추가된 로그온 및 기타 데이터는 사라집니다 .

4 Next(다음) 를 클릭합니다 .

주 : 복원 작업의 텍스트 로그를 보려면 제목 표시줄에서 아이콘을 클릭하고 **로그**를 선택합니다 .

용어집

OTP(일회용 암호) – 일회용 암호는 단 한 번만 사용할 수 있는 암호로 , 제한된 기간 동안에만 유효합니다 . OTP 를 사용하려면 TPM 을 설치하고 , 활성화해야 하며 , 소유권을 가지고 있어야 합니다 . OTP 를 이용하려면 DDP Console 및 Security Tools Mobile 앱을 사용하여 모바일 장치와 컴퓨터를 페어링해야 합니다 . Security Tools Mobile 앱에서 생성된 모바일 장치의 암호는 컴퓨터의 Windows 로그온 화면에서 로그온하는 데 사용됩니다 . 정책에 따라 , 컴퓨터에 로그온할 때 OTP 를 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 1 회용이며 유효 기간이 짧다는 점에서 다른 인증 방식의 보안보다 강력하다고 할 수 있습니다 .

Preboot Authentication (PBA) – 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 . PBA 는 사용자에게 올바른 자격 증명이 있는지 확인할 때까지 하드 디스크에서 운영 체제 등의 데이터를 읽을 수 없도록 합니다 .

TPM(Trusted Platform Module) – TPM 은 안전한 저장 , 측정 , 증명의 세 가지 주요 기능을 제공하는 보안 칩입니다 . DDP|E 는 안전한 저장 기능 때문에 TPM 을 사용합니다 . TPM 은 DDP|E 소프트웨어 자격 증명 보관과 DDP|E HCA 암호화 키 보호를 위한 암호화된 컨테이너를 제공할 수도 있습니다 . TPM 은 프로비저닝하는 것이 좋습니다 . TPM 은 DDP|E HCA, BitLocker Manager, OTP(일회용 암호) 기능을 사용하려는 경우에 필요합니다 .

보호됨 – 자체 암호화 드라이브 (SED) 의 경우 , SED 가 활성화되고 부팅 전 인증 (PBA) 이 배포되면 컴퓨터가 보호됩니다 .

자격 증명 – 자격 증명은 지문이나 Windows 암호 등과 같은 개인의 신원을 증명하는 수단입니다 .

자체 암호화 드라이브 (SED) - 미디어에 저장된 모든 데이터를 자동으로 암호화하고 미디어 외부로 이동되는 모든 데이터의 암호를 자동으로 해독하는 암호화 메커니즘이 기본으로 내장되어 있는 하드 드라이브입니다 . 이 유형의 암호화는 사용자에게 투명하게 표시됩니다 .


0 XXXXXA0 X