그룹 정책을 이용한 장치 설치 제어 단계별 가이드
– USB 저장 장치 편

Microsoft MVP
Windows Development
신승운

- 목 차 -

1. 소개

이 단계별 가이드는 사용자가 설치할 수 있는 장치와 설치할 수 없는 장치를 지정하여 컴퓨터에서 장치 설치를 제어하는 방법에 대해 설명합니다.

이 가이드에서는 장치 설치 프로세스에 대해 설명하고 컴퓨터에서 사용되는 장치 드라이버 패키지와 장치를 일치시키는 데 사용되는 식별 문자열에 대해 소개합니다. 또한, 세 가지 장치 설치 제어 방법에 대해서도 설명합니다. 각 시나리오는 특정 장치 또는 장치 클래스의 설치를 허용 또는 금지하는 데 사용할 수 있는 방법을 단계별로 보여줍니다. 네 번째 시나리오는 이동식 장치 또는 이동식 미디어를 사용하는 장치에 대해 사용자에 대한 읽기 또는 쓰기 액세스를 거부하는 방법을 보여줍니다.

① 사용자가 그 어떠한 장치도 설치 못하게 방지

② 승인된 목록에 ("approved") 있는 장치만 사용자가 설치하도록 허용

- ✓ 목록에 없는 장치는 사용자가 설치할 수 없음

③ 금지된 목록에 ("prohibited") 있는 장치를 사용자가 설치하는 것을 방지

- ✓ 목록에 없는 장치는 사용자가 설치할 수 있음

④ 이동식 장치나 CD 및 DVD 버너, 플로피 디스크 드라이브, 외장 하드 드라이브 등과 같은 이동식 미디어, 미디어 플레이어, 스마트폰, 포켓 PC 장치 등과 같은 휴대용 장치에 대해 사용자에 대한 읽기 또는 쓰기 액세스를 거부

본 가이드에서는 USB 저장 장치를 예를 들어 설명합니다.

그룹 정책을 이용한 장치 설치 제어의 이점

- 데이터 도용의 위험 감소
  - ✓ 이동식 미디어를 연결 가능한 사용자 컴퓨터에 승인되지 않은 장치를 설치할 수 없다면, 사용자가 회사나 개인의 중요한 데이터를 무단으로 복사하는 것은 불가능함
  - ✓ 이동식 장치나 이동식 미디어를 사용하는 장치의 사용자에게 그룹정책을 적용하여 쓰기 액세스를 거부시킴으로써 데이터 도용 위험 감소함
  - ✓ 그룹 정책을 사용하여 사용자 그룹 단위로 접근 권한을 부여함

- 지원 비용 절감
  - ✓ 사용자는 오로지 Help Desk 에서 지원할 수 있는 장치만 설치할 수 있어서 지원 비용과 사용자 혼란을 줄일 수 있음

2. 시나리오 개요

이 가이드에서는 관리하는 컴퓨터에서 장치 설치 및 사용을 제어하는 방법을 설명합니다. 다수의 클라이언트 컴퓨터를 관리하는 환경에서는 Active Directory 에서 배포한 그룹 정책을 사용하여 이러한 설정을 적용해야 합니다. Active Directory 에서 그룹 정책을 배포하면 도메인의 구성원이거나 조직 구성 단위의 모든 컴퓨터에 설정을 적용할 수 있습니다.

다음은 이 가이드에 나와 있는 시나리오에 대한 설명입니다.

- **모든 장치 설치 금지**
  - ✓ 일반 사용자가 모든 장치를 설치하지 못하게 설정 가능
  - ✓ 단, 관리자는 모든 장치를 설치하거나 업데이트할 수 있게 설정 가능
- **사용자가 승인된 장치만 설치하도록 허용**
  - ✓ 승인된 장치 목록에 포함된 장치만 사용자가 설치하도록 허용
  - ✓ 사용자가 지정한 장치만 설치할 수 있도록 권한이 부여된 장치 목록 생성
- **금지된 장치들만 설치 금지**
  - ✓ 일반 사용자가 대부분의 장치를 설치할 수는 있지만, 금지된 장치 목록에 포함된 장치를 설치하지 못하게 설정 가능
  - ✓ 금지된 장치 목록에 있는 사용자 지정 장치를 제외한 모든 장치 설치 가능
- **이동식 미디어 저장 장치 사용 제어**
  - ✓ 일반 사용자가 이동식 저장장치 또는 USB 메모리 드라이브나 CD/DVD 버너와 같은 이동식 미디어가 있는 장치에 데이터를 쓰지 못하게 설정 가능
  - ✓ 읽기 액세스는 허용하지만 샘플 장치 및 컴퓨터의 CD/DVD 버너 장치에 대한 쓰기 액세스를 거부하도록 컴퓨터 정책 구성

3. 기술 검토

3.1. Windows 에서 장치 설치

장치는 Windows 가 어떠한 기능을 수행하기 위해 상호 작용하는 하드웨어로, Windows 는 장치 드라이버라는 소프트웨어를 통해서만 장치와 통신할 수 있습니다. Windows 는 장치를 감지하고 장치 유형을 인식한 다음 해당 유형과 일치하는 장치 드라이버를 찾아서 장치 드라이버를 설치합니다. Windows 는 다음 두 가지 유형의 식별자를 사용하여 장치 설치 및 구성 제어를 합니다. Windows 의 그룹 정책 설정을 통해 허용하거나 차단할 식별자를 지정할 수 있습니다.

두 가지 유형의 식별자는 다음과 같습니다.

- 장치 식별 문자열 (Device Identification Strings)
- 장치 설치 클래스 (Device Setup Classes)

3.1.1. 장치 식별 문자열 (Device Identification Strings)

Windows 가 컴퓨터에 한번도 설치되지 않은 장치를 감지하면 운영체제는 장치를 쿼리하여 장치 식별 문자열 목록을 검색합니다. 일반적으로 각 장치에는 장치 제조 업체가 할당하는 여러 개의 장치 식별 문자열이 있고, 동일한 장치 식별 문자열은 장치 드라이버 패키지의 일부인 .inf 파일에 포함됩니다. Windows 는 장치에서 검색한 장치 식별 문자열을 드라이버 패키지에 포함된 장치 식별 문자열과 일치시켜 설치할 장치 드라이버 패키지를 선택합니다.

Windows 는 장치를 드라이버 패키지에 일치시키기 위해 각 문자열을 사용합니다. 문자열은 장치에 대해 하나의 제조사 및 모델을 매칭하는 세부적인 정보에서부터 전체 장치 클래스에 적용하는 일반적인 정보까지 매우 다양한 정보를 포함하고 있습니다. 다음과 같이 두 가지 유형의 장치 식별 문자열이 있습니다.

- 하드웨어 ID (Hardware IDs)
- 호환성 ID (Compatible IDs)

3.1.1.1. 하드웨어 ID (Hardware IDs)

하드웨어 ID 는 장치와 드라이버 패키지 간의 가장 정확한 일치 정보를 제공하는 식별자입니다. 하드웨어 ID 목록의 첫 번째 문자열은 장치 ID (Device ID) 로, 장치의 제조사, 모델 및 버전 정보가 포함되어 있습니다. 목록에 있는 다른 하드웨어 ID 는 장치의 세부 정보를 덜 정확하게

일치시킵니다. 예를 들어, 하드웨어 ID 는 장치의 제조업체 및 모델은 식별하지만 특정 세부 버전 정보는 식별하지 못할 수 있습니다. 만약, 정확한 버전의 드라이버를 사용할 수 없는 경우, 이 구성표를 사용하면 Windows 에서 장치의 다른 버전에 대한 드라이버를 사용할 수 있습니다.

3.1.1.2. 호환성 ID (Compatible IDs)

운영체제가 장치 ID (Device ID) 또는 다른 하드웨어 ID 와 일치하는 것을 찾지 못하면 Windows 는 장치 드라이버를 선택하기 위해 이 식별자를 사용합니다. 호환성 ID 는 적합성이 감소하는 순서로 나열됩니다. 이러한 문자열은 선택 사항이며, 제공되는 경우 매우 일반적인 문자열입니다 (예: 디스크). 호환성 ID 를 사용하여 일치하는 항목을 만들 때 일반적으로 장치의 가장 기본적인 기능만 사용할 수 있습니다.

프린터, USB 저장 장치 또는 키보드와 같은 장치를 설치할 때, Windows 는 설치하려는 장치와 일치하는 드라이버 패키지를 검색합니다. 검색하는 동안, Windows 는 검색한 각각의 드라이버 패키지에 적어도 하나의 하드웨어 ID 또는 호환성 ID 에 대한 일치 항목에 대해 "순위 (Rank)" 를 할당합니다. 순위는 드라이버가 장치와 얼마나 정확하게 잘 일치하는지 나타내는 것으로, 낮은 순위 번호가 드라이버와 장치가 더 정확하게 일치하는 것임을 뜻합니다. 순위 0 은 가장 정확한 최적의 일치를 나타냅니다. 드라이버 패키지 안의 하나와 장치 ID 가 일치하면 다른 하드웨어 ID 중 하나와 일치하는 것보다 더 낮은 순위가 됩니다. 마찬가지로, 하드웨어 ID 와 일치하면 호환성 ID 중 하나와 일치하는 것보다 더 우수한 순위가 됩니다. Windows 가 모든 드라이버 패키지에 대한 순위를 지정한 후에는 가장 낮은 순위의 드라이버 패키지 하나가 설치됩니다.

일부 물리적 장치는 설치 시 하나 이상의 논리 장치를 생성합니다. 각 논리적 장치는 물리적 장치의 일부 기능을 처리할 수 있습니다. 예를 들어, 올인원 스캐너/팩스/프린터와 같은 다기능 장치는 각 기능에 대해 다른 장치 식별 문자열을 가질 수 있습니다.

DMI 를 사용하여 논리 장치를 사용하는 장치의 설치를 허용 또는 금지하는 경우, 해당 장치의 모든 장치 식별 문자열을 허용하거나 금지해야 합니다. 예를 들어, 사용자가 다기능 장치를 설치하려고 시도하고 물리적 및 논리적 장치에 대한 모든 식별 문자열을 허용하지 않았거나 금지하지 않았으면, 설치 시도 시 예기치 않은 결과가 발생할 수 있습니다.

3.1.2. 장치 설치 클래스 (Device Setup Classes)

장치 설치 클래스는 다른 유형의 식별 문자열입니다. 제조사는 장치 설치 클래스를 장치 드라이버 패키지의 장치에 할당합니다. 장치 설치 클래스는 동일한 방법으로 설치 및 구성된 장치를 그룹화합니다. 예를 들어 모든 CD 드라이브는 CDROM 장치 설치 클래스에 속하며 설치

시 동일한 설치 관리자를 사용합니다. 전역 고유 식별자 (GUID) 라고 불리는 긴 숫자는 각 장치 설치 클래스를 나타냅니다. Windows 가 시작되면 검색된 모든 장치에 대한 GUID 로 메모리 내 트리 구조가 만들어 집니다. Windows 는 장치 자체의 장치 설치 클래스에 대한 GUID 와 함께 장치가 연결된 버스의 장치 설치 클래스에 대한 GUID 를 트리에 삽입해야 할 수도 있습니다.

장치 설치 클래스를 사용하여 사용자의 장치 드라이버 설치를 허용하거나 금지하고자 할 때는 장치의 모든 장치 설치 클래스에 대한 GUID 를 지정해야 합니다. 그렇지 않으면 원하는 결과를 얻지 못할 수 있습니다. 설치하기를 원하는 데 설치가 실패하거나, 설치 실패하기를 원하는데 설치가 될 수 있습니다.

예를 들어, 올인원 스캐너/팩스/프린터와 같은 다기능 장치에는 일반적인 다기능 장치에 대한 GUID, 프린터 기능에 대한 GUID, 스캐너 기능에 대한 GUID, 팩스 기능에 대한 GUID 등이 있습니다. 개별 기능에 대한 GUID 는 다기능 장치 GUID 아래의 "하위 노드(child nodes)" 입니다. 하위 노드를 설치하려면 Windows 에서 상위 노드도 같이 설치해야 합니다. 다기능 장치에 대한 부모 GUID 의 장치 설치 클래스와 프린터 및 스캐너 기능에 대한 자식 GUID 의 설치를 허용해야 합니다.

3.2. 장치 설치 관련 그룹 정책 설정

장치 설치를 제어할 수 있도록 Windows (Vista 및 Windows Server 2008 이상) 에서는 여러 가지 정책 설정을 제공합니다. 이러한 정책 설정은 단일 컴퓨터에서 개별적으로 구성하거나 Active Directory 도메인의 그룹 정책을 사용하여 많은 수의 컴퓨터에 적용할 수 있습니다. 그룹 정책 설정을 독립실행형 (stand-alone) 컴퓨터 또는 Active Directory 도메인의 여러 컴퓨터에 적용할 때 그룹 정책 개체 편집기를 사용하여 정책 설정을 구성하고 적용합니다.

다음은 이 가이드에서 사용되는 DMI 정책 설정에 대한 간략한 설명입니다.

참고) 이러한 정책 설정은 정책 설정이 적용되는 컴퓨터에 로그온 하는 모든 사용자에게 영향을 줍니다. "Allow administrators to override device installation policy" 정책을 제외하고는 이러한 정책을 특정 사용자 또는 그룹에 적용할 수 없습니다. 이 정책은 이 섹션에서 기술된 다른 정책 설정으로 구성된 컴퓨터에 적용되는 장치 설치 제한으로부터 로컬 Administrators 그룹의 구성원을 제외합니다.

- **Prevent installation of devices not described by other policy settings.** (다른 정책 설정으로 기술되지 않은 장치 설치를 방지)

  이 정책 설정은 다른 정책 설정에 의해 구체적으로 기술되지 않은 장치 설치를 제어합니다. 이 정책 설정을 사용하면, "Allow installation of devices that match these device IDs" 정책 설정 혹은 "Allow installation of devices for these device classes" 정책

설정으로 기술하지 않는 한 사용자는 장치용 드라이버를 설치하거나 업데이트 할 수 없습니다. 이 정책 설정을 사용하지 않거나 구성하지 않으면, 사용자는 "Prevent installation of devices that match these device IDs" 혹은 "Prevent installation of devices for these device classes", "Prevent installation of removable devices" 정책 설정으로 기술되지 않은 장치에 대한 드라이버를 설치하고 업데이트할 수 있습니다.

- **Allow administrators to override device installation policy.** (관리자가 장치 설치 정책을 무시하도록 허용)

  이 정책 설정을 사용하면 로컬 Administrators 그룹의 구성원이 다른 정책 설정에 관계없이 모든 장치의 드라이버를 설치하고 업데이트할 수 있습니다. 이 정책 설정을 사용하면, 관리자는 "Add Hardware Wizard" 또는 "Update Driver Wizard" 를 사용하여 모든 장치의 드라이버를 설치하고 업데이트할 수 있습니다. 이 정책 설정을 사용하지 않거나 구성하지 않으면, 관리자에게 장치 설치를 제한하는 모든 정책 설정이 적용됩니다.

- **Prevent installation of devices that match these device IDs.** (장치 ID 와 일치하는 장치의 설치를 금지)

  이 정책 설정은 사용자가 설치할 수 없는 장치에 대한 플러그 앤 플레이 하드웨어 ID 및 호환성 ID 목록을 지정합니다. 이 정책 설정을 사용하면, 하드웨어 ID 또는 호환성 ID 가 이 목록에 있는 것과 일치하는 경우 사용자는 장치의 드라이버를 설치하거나 업데이트할 수 없습니다. 이 정책 설정을 사용하지 않거나 구성하지 않으면, 사용자는 장치 설치에 대한 다른 정책 설정에서 허용하는 대로 장치를 설치하고 드라이버를 업데이트할 수 있습니다.

  참고) 이 정책 설정은 사용자가 장치를 설치할 수 있는 다른 정책 설정보다 우선합니다. 이 정책 설정은 해당 장치를 설치할 수 있는 다른 정책 설정과 일치하는 경우에도 사용자가 장치를 설치할 수 없도록 합니다.

- **Prevent installation of drivers matching these device setup classes.** (장치 설치 클래스와 일치하는 드라이버 설치를 금지)

  이 정책 설정은 사용자가 설치할 수 없는 장치에 대한 플러그 앤 플레이 장치 설치 클래스 GUID 목록을 지정합니다. 이 정책 설정을 사용하면, 나열된 장치 설치 클래스 중 하나에 속한 장치를 설치하거나 업데이트 할 수 없습니다. 이 정책 설정을 사용하지 않거나 구성하지 않으면, 사용자는 장치 설치에 대한 다른 정책 설정에서 허용하는 대로 장치를 설치하고 업데이트 할 수 있습니다.

참고) 이 정책 설정은 사용자가 장치를 설치할 수 있는 다른 정책 설정보다 우선합니다. 이 정책 설정은 해당 장치를 설치할 수 있는 다른 정책 설정과 일치하는 경우에도 사용자가 장치를 설치하지 못하게 합니다.

- **Allow installation of devices that match any of these device IDs.** (장치 ID 중 하나와 일치하는 장치의 설치를 허용)

  이 정책 설정은 사용자가 설치할 수 있는 장치를 나타내는 플러그 앤 플레이 하드웨어 ID 및 호환성 ID 목록을 지정합니다. 이 설정은 "Prevent installation of devices not described by other policy settings" 정책 설정이 사용되고, 사용자가 장치를 설치하지 못하게 하는 정책 설정보다 우선 순위가 없는 경우에만 사용하도록 되어 있습니다. 이 정책 설정을 사용하면, "Prevent installation of devices that match these device IDs" 혹은 "Prevent installation of devices for these device classes", "Prevent installation of removable devices" 정책 설정에 의해 특별히 설치 금지되지 않은 경우 이 목록의 ID 와 일치하는 하드웨어 ID 또는 호환성 ID 를 사용하여 장치를 설치하고 업데이트할 수 있습니다. 다른 정책 설정으로 인해 사용자가 장치를 설치할 수 없으면, 이 정책 설정의 값으로도 장치가 기술되어 있어도 사용자가 설치할 수 없습니다. 이 정책 설정을 사용하지 않거나 구성하지 않고 다른 정책이 장치를 기술하지 않으면, "Prevent installation of devices not described by other policy settings" 정책 설정에 따라 사용자가 장치를 설치할 수 있는지 여부가 결정됩니다.

- **Allow installation of devices using drivers for these device classes.** (장치 클래스용 드라이버를 사용하는 장치의 설치를 허용)

  이 정책 설정은 사용자가 설치할 수 있는 장치를 설명하는 장치 설치 클래스 GUID 목록을 지정합니다. 이 설정은 "Prevent installation of devices not described by other policy settings" 정책 설정이 사용되고, 사용자가 장치를 설치하지 못하게 하는 정책 설정보다 우선 순위가 없는 경우에만 사용하도록 되어 있습니다. 이 설정을 사용하면, "Prevent installation of devices that match these device IDs" 혹은 "Prevent installation of devices for these device classes", "Prevent installation of removable devices" 정책 설정으로 해당 설치가 특별히 차단되지 않은 경우 사용자는 이 목록의 ID 중 하나와 일치하는 하드웨어 ID 또는 호환성 ID 가 있는 장치를 설치하고 업데이트 할 수 있습니다. 다른 정책 설정으로 인해 사용자가 장치를 설치할 수 없으면, 이 정책 설정의 값으로도 장치가 기술되어 있어도 사용자가 설치할 수 없습니다. 이 정책 설정을 사용하지 않거나 구성하지 않고 장치를 설명하는 다른 정책 설정이 없으면, "Prevent installation of devices not described by other policy settings" 정책 설정에 따라 사용자가 장치를 설치할 수 있는지 여부가 결정됩니다.

이러한 정책 중 일부는 다른 정책보다 우선합니다. 아래 그림 1) 은 사용자가 장치를 설치할 수 있는지 여부를 결정하기 위해 Windows 가 정책을 어떻게 처리하는지에 대해 보여줍니다

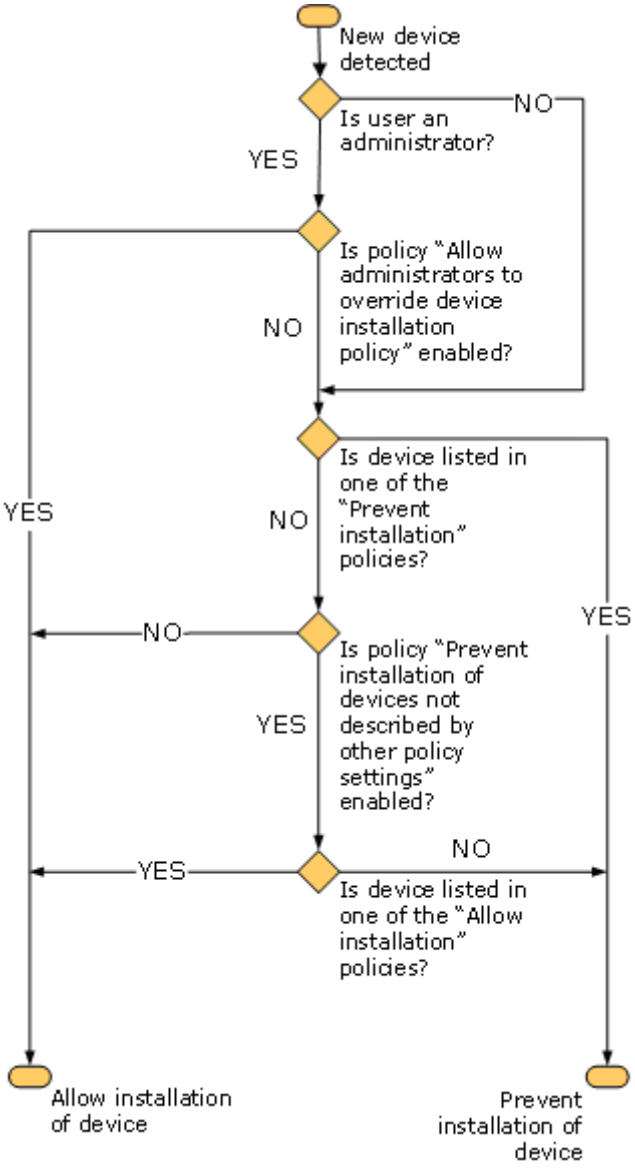

그림 1) 사용자가 장치를 설치할 수 있는지 여부를 결정할 때 Windows 가 정책을 처리하는 방법

3.3. 이동식 저장소 액세스의 그룹 정책 설정

Windows Vista 및 Windows Server 2008 에서 관리자는 사용자가 이동식 미디어 기반의 모든 장치에 대해 읽고 쓸 수 있는지에 대하여 컴퓨터 정책을 통하여 제어할 수 있습니다. 이러한 정책은 기밀 또는 기밀 자료가 이동식 미디어나 이동식 저장 장치에 기록되는 것을 방지하는데 사용될 수 있습니다.

이러한 정책 설정은 컴퓨터에 로그온 하는 모든 사용자에게 영향을 줍니다. 또한, 사용자 레벨이나 특정 사용자 계정에 한해 해당 정책 적용을 제한 할 수도 있습니다. Active Directory 환경에서 그룹 정책을 사용하는 경우, 단일 사용자 계정 외에도 사용자 그룹에 정책 설정을 적용할 수 있습니다. 또한 그룹 정책을 사용하면 다수의 컴퓨터에 이러한 정책을 효율적으로 적용할 수 있습니다.

이동식 저장소 액세스 정책 설정에는 관리자가 강제로 다시 부팅하도록 허용하는 설정도 포함하고 있습니다. 만약 제한 정책이 적용될 때 장치가 사용 중인 상태라면, 컴퓨터를 다시 시작할 때까지 정책이 적용되지 않을 수 있습니다.

정책 설정은 다음 두 위치에서 확인할 수 있습니다. "Computer Configuration₩Administrative Templates₩System₩Removable Storage Access" 정책 설정은 컴퓨터와 컴퓨터에 로그온 하는 모든 사용자에게 영향을 줍니다. "User Configuration₩Administrative Templates₩System₩Removable Storage Access" 정책 설정은 Active Directory 를 사용하여 그룹 정책이 적용되는 경우 그룹을 포함하여 정책 설정이 적용되는 사용자에게만 영향을 줍니다.

다음은 이동식 저장소 드라이브에 대한 읽기/쓰기 액세스를 제어할 수 있는 정책에 대한 설명입니다. 각 장치 범주는 읽기 액세스를 거부하는 정책과 쓰기 액세스를 거부하는 정책을 지원합니다.

- **강제 재부팅 시간 (초)**
  이동식 저장 장치에 대한 액세스 권한을 변경하기 위해 시스템이 다시 시작될 때까지 기다리는 시간(초)을 설정함

  참고) 만약 강제로 다시 시작하지 않으면, 시스템을 다시 시작할 때까지 변경 내용이 적용되지 않음

- **CD 및 DVD**
  USB 로 연결된 장치를 포함하여 CD 및 DVD 이동식 저장소 클래스의 장치에 대한 읽기 또는 쓰기 액세스를 거부할 수 있음

- **사용자 정의 클래스**
  사용자가 제공하는 목록에서 Device Setup Class GUID 가 있는 모든 장치에 대한 읽기 또는 쓰기 액세스를 거부할 수 있음

- **플로피 드라이브**
  USB 로 연결된 장치를 포함하여 플로피 드라이브 클래스의 장치에 대한 읽기 또는 쓰기 액세스를 거부 할 수 있음

- **이동식 디스크**
  USB 메모리 드라이브 또는 외부 USB 하드 디스크 드라이브와 같은 이동식 장치에 대한 읽기 또는 쓰기 액세스를 거부할 수 있음

- **테이프 드라이브**
  USB 로 연결된 장치를 포함하여 테이프 드라이브에 대한 읽기 또는 쓰기 액세스를 거부할 수 있음

- **WPD 장치**
  Windows 휴대용 장치 클래스의 장치에 대한 읽기 또는 쓰기 액세스를 거부할 수 있으며, 이러한 장치에는 미디어 플레이어, 휴대폰, Windows CE 장치 등과 같은 "스마트" 장치가 포함됨

- **모든 이동식 저장소 클래스: 모든 액세스 거부**
  이 목록의 어떠한 정책 설정보다 우선하며, 해당 정책이 활성화 된 경우, 이동식 저장소로 식별된 모든 장치에 대한 읽기 및 쓰기 권한을 거부함. 이 정책 설정을 비활성화하거나 구성하지 않으면, 이 목록의 다른 정책 설정에 따른 제한 사항에 따라 이동식 저장소 클래스에 대한 읽기 및 쓰기 권한이 허용됨

4. 시나리오를 완료하기 위한 요구 사항

- Windows Vista 가 구동되는 클라이언트 컴퓨터

  ✓ 이 가이드에서는 이 컴퓨터를 DMI-Client1 로 지칭합니다.

- USB 메모리 드라이브

  ✓ 이 가이드에서는 USB 메모리 드라이브를 예제로 사용합니다. 이 장치는 이동식 디스크 드라이브처럼 작동하며 "thumb drive", "flash drive" 또는 "keyring drive" 라고도 합니다. 대부분의 USB 메모리 드라이브에는 제조업체에서 제공하는 드라이버가 필요하지 않으며 이러한 장치는 Windows Vista 및 Windows Server 2008 에서 제공되는 드라이버에서 작동합니다.

  참고) 이 지침에서는 장치에 Windows Vista 및 Windows Server 2008 에 포함된 드라이버 외의 다른 드라이버는 요구하지 않는다고 가정합니다. 만약, 장치 제조업체의 드라이버가 필요한 경우라면, Windows 에서 드라이버 요구 메시지가 나타나면 드라이버 파일을 제공해야 합니다. 이 단계는 시나리오에 포함되어 있지 않습니다.

- (옵션) CD 또는 DVD 버너

  ✓ 읽기 전용의 이동식 미디어 장치를 만드는 방법을 보여줍니다. CD 또는 DVD 버너가 실제로 설치되어 있지 않아도 컴퓨터 정책을 설정할 수 있습니다. 그러나 만약 컴퓨터 정책이 유효한지 확인하려면 사용할 CD 또는 DVD 버너 장치가 있어야 합니다.

- DMI-Client1 의 보호된 관리자 계정에 대한 액세스

  ✓ 이 가이드에서는 이 계정을 TestAdmin 이라고 합니다. 이 가이드의 절차에서는 대부분의 단계에서 관리자 권한이 필요합니다. 별도로 지시하지 않는 한, 각각의 절차를 시작할 때 이 관리자 계정을 사용하여 DMI-Client1 에 로그인해야 합니다.

  참고) Windows Vista 및 Windows Server 2008 에는 보호된 관리자 계정 개념이 도입되었습니다. 이 계정은 Administrators 그룹의 구성원이지만 기본적으로 보안 권한은 직접 사용되지 않습니다. 관리자의 높은 권한이 필요한 작업을 수행하려고 하면 해당 작업을 수행할 수 있는 권한을 요청하는 대화 상자가 나타납니다. 마이크로소프트에서는 가능한 한 기본 제공되는 관리자 계정 대신, 보호된 관리자 계정을 사용하는 것을 권장합니다.

- DMI-Client1 의 표준 사용자 계정에 대한 액세스

  ✓ 이 사용자 계정에는 그 어떠한 승격된 권한을 부여하는 특별한 구성원을 가지고 있지 않습니다. 이 가이드에서는 이 계정을 TestUser 라고 합니다. 지시가 있을 때만 이 계정으로 컴퓨터에 로그온 하십시오. 표준 사용자 계정을 사용하면 관리자의 높은 권한이 필요한 작업을 수행할 때 관리자 권한이 있는 계정의 자격 증명을 요청하는 대화 상자가 나타납니다.

4.1. 사전 요구 절차

사용자가 장치 설치를 허용 또는 금지하는 정책을 구현하기 전에, 장치의 장치 식별 문자열을 알아야 합니다. 또한 USB 메모리 드라이브 및 관련 드라이버를 완전히 제거하는 방법을 알아야 합니다. 다음 절차는 이 가이드의 시나리오를 성공적으로 실행하도록 컴퓨터를 구성합니다.

4.1.1. 사용자 계정 컨트롤 페이지에 응답

이 가이드에서는 Administrators 그룹의 구성원만 수행할 수 있는 작업을 수행해야 합니다. Windows Vista 및 Windows Server 2008 에서 관리자 권한이 필요한 작업을 수행하려고 하면, 다음과 같은 증상이 발생합니다.

- 기본 제공되는 Administrator 계정으로 로그인 한 경우 (권장하지 않는 계정) 에는 작업이 간단하게 진행됩니다. 기본 제공되는 관리자 계정은 기본적으로 비활성화되어 있습니다.
- 기본 제공되는 관리자 계정이 아닌 Administrators 그룹의 구성원인 경우에는 계속 진행할 수 있는 권한을 묻는 사용자 계정 컨트롤 (UAC, User Account Control) 대화 상자가 나타납니다. 만약, Continue 를 클릭하면 작업은 수행됩니다.
- 표준 사용자로 로그온 한 경우에는 작업을 수행하지 못할 수 있습니다. 작업에 따라 관리자 계정의 사용자 이름과 암호를 제공해야 하는 사용자 계정 컨트롤 페이지가 표시될 수 있습니다. 만약 유효한 자격 증명을 제공하면, 작업은 제공한 관리자 계정의 보안 하에서 실행됩니다. 만약 이러한 자격 증명을 제공할 수 없으면, 작업을 수행할 수 없습니다.

  ※ 중요) 관리 작업을 실행하기 위한 자격 증명이나 권한을 제공하기 전에, 시작한 작업에 대한 응답으로 User Account Control 페이지가 표시되는지 확인하십시오. 만약 예기치 않게 페이지가 나타나면, Details 버튼을 클릭하고 허용할 작업이 있는지 확인하십시오.

이 가이드에서는 이러한 절차를 수행할 때 발생하는 모든 사용자 계정 컨트롤 대화 상자를 설명하지는 않습니다. 관리자로 특정 작업을 실행하는 데 특별한 단계가 필요한 경우, 해당 단계는 가이드에 설명되어 있습니다.

4.1.2. USB 메모리 드라이브의 장치 식별 문자열 결정

이 단계를 수행하면 장치의 장치 식별 문자열을 확인할 수 있습니다. 만약 장치의 하드웨어 ID 및 호환성 ID 가 이 가이드에 표시된 것과 일치하지 않으면, 장치에 적합한 ID 를 사용하십시오.

> 참고) 다음 시나리오에서는 USB 메모리 드라이브를 설치한 다음 제거해야 합니다. 지시 사항은 장치에 Windows Vista 및 Windows Server 2008 에 포함된 드라이버 외의 다른 드라이버는 필요로 하지 않는다고 가정합니다. 만약 장치 제조업체가 제공하는 드라이버가 필요한 경우, Windows 에서 드라이버 요구 메시지가 나타나면 드라이버 파일을 제공해야 합니다. 이 단계는 시나리오에 포함되어 있지 않습니다.

두 가지 방법으로 장치의 하드웨어 ID 와 호환성 ID 를 확인할 수 있습니다. 운영체제에 포함된 그래픽 도구인 장치 관리자 (Device Manager) 또는 DDK (Driver Development Kit) 에서 다운로드 할 수 있는 명령줄 도구인 DevCon 을 사용할 수 있습니다. 다음은 USB 메모리 드라이브의 장치 식별 문자열을 확인할 수 있는 절차입니다.

> 중요) 이 절차는 USB 메모리 드라이브에만 적용됩니다. 만약 다른 유형의 장치를 사용하는 경우라면, 적절하게 단계를 조정해야 합니다. 중요한 차이점은 장치 관리자 계층에서 장치의 위치입니다. Disk Drives 노드 대신, 적당한 다른 노드에서 장치를 찾아야 합니다.

장치 관리자를 사용하여 장치 식별 문자열 찾기

① DMI-Client1₩TestAdmin 으로 컴퓨터 로그인

② USB 메모리 드라이브 연결 및 설치

③ 장치 관리자 실행 (시작 – 실행 – mmc devmgmt.msc 입력 후 실행)

④ User Account Control 대화상자가 나타나면, 표시 내용 확인한 다음 Continue 클릭

장치 관리자가 시작되고 컴퓨터에서 감지된 모든 장치를 나타내는 트리 구조가 표시됩니다. 트리의 맨 위에는 컴퓨터 이름이 있는 노드가 있습니다. 하위 노드에는 컴퓨터 장치들이 그룹화되어 있는 다양한 하드웨어 카테고리들이 표시됩니다.

⑤ 목록을 열기 위해 Disk drives 더블 클릭

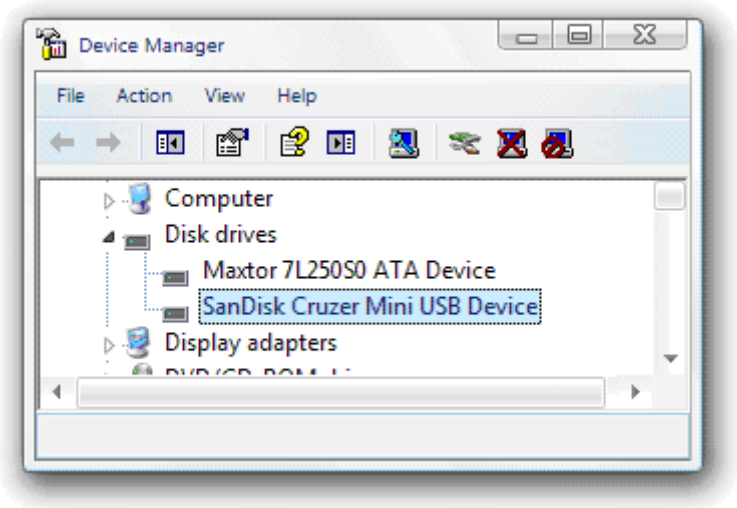

그림 2) 더블 클릭으로 USB 디스크 드라이브 열기

⑥ USB 메모리 드라이브에서 마우스 우클릭하여 Properties 클릭, Device Properties 대화상자 실행

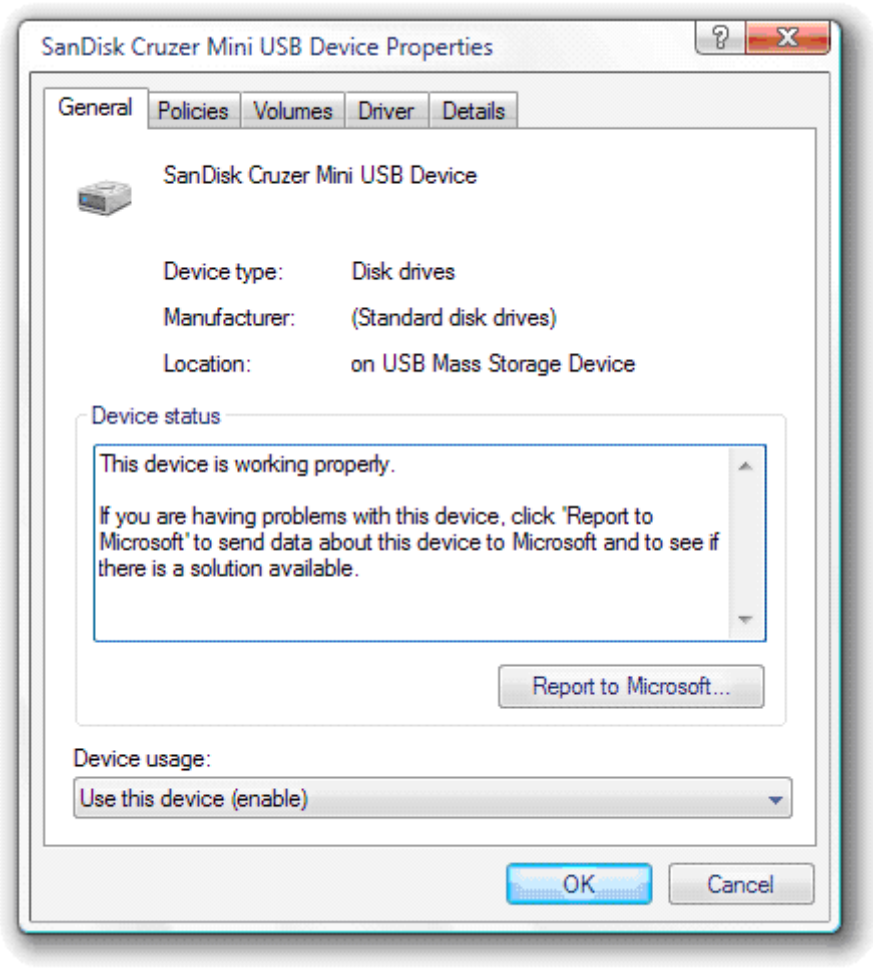

그림 3) USB 드라이브에 대한 장치 속성 대화화 상자 실행

⑦ Details 탭 클릭

⑧ Property 목록에서 Hardware Ids 클릭

⑨ Value 값 아래에 표시된 문자열 기록

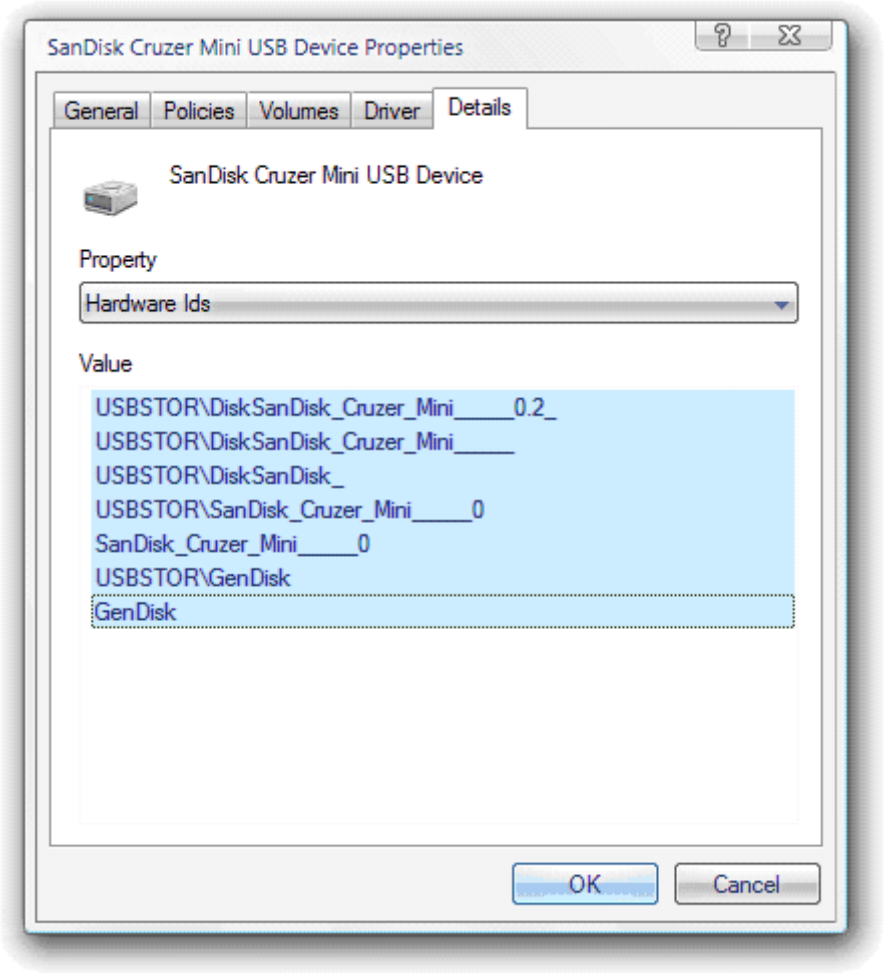

그림 4) USB 드라이브 속성 창에 표시된 문자열 기록

참고) 문자 전체 선택한 후 Ctrl-C 키를 눌러 클립보드에 문자열을 복사할 수 있습니다. 많은 하드웨어 IDs 들은 다양한 밑줄 문자들을 가지고 있기 때문에 식별자를 지정해야 할 때 붙여 넣을 수 있는 텍스트 파일로 복사하는 것이 도움이 됩니다. 이러한 접근 방법은 승인된 장치 또는 금지된 장치 목록에 특정 식별자를 추가해야 할 때 오류가 발생할 가능성을 크게 줄일 수 있습니다.

⑩ Property 목록에서 Compatible Ids 클릭

⑪ Value 값 아래에 표시된 문자열 기록

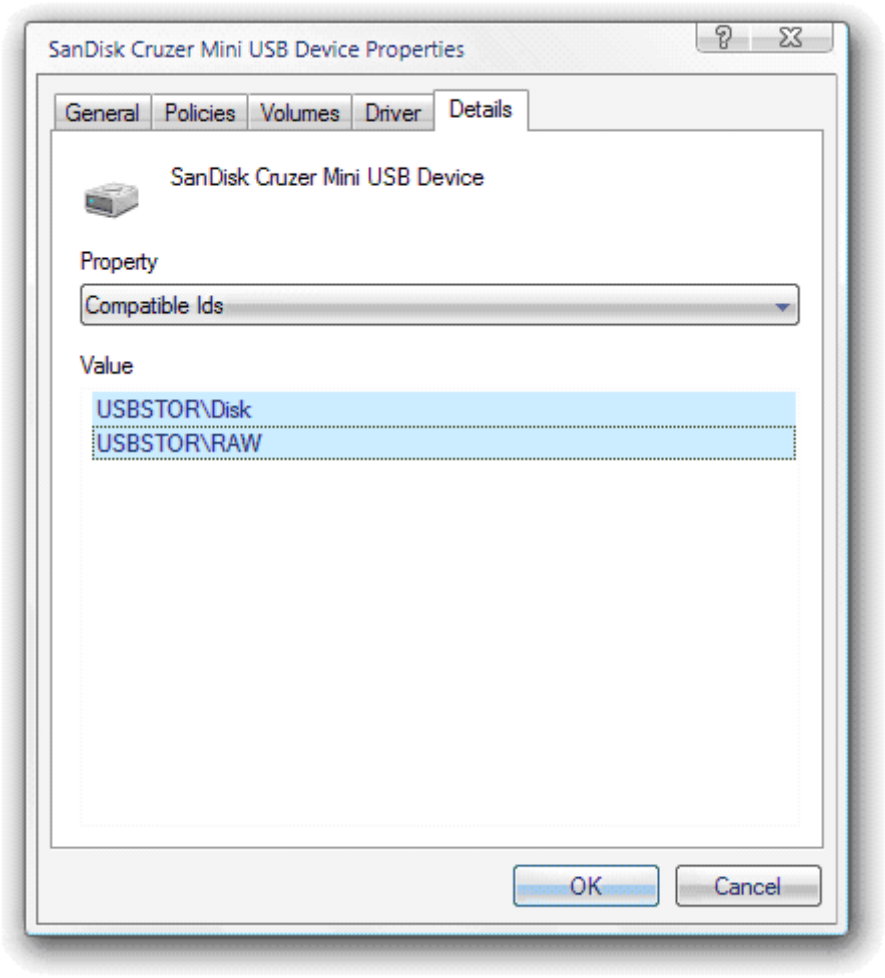

그림 5) USB 드라이브 속성 창에 표시된 문자열 기록

참고) DevCon 명령어 기반 도구를 사용하여 장치 식별 문자열을 확인할 수도 있습니다. DevCon 파일은 Microsoft 도움말 및 지원 사이트에서 다운로드 할 수 있습니다.

4.1.3. USB 메모리 드라이브 삭제

USB 메모리 드라이브를 사용하는 경우, 일반적으로 USB 포트에서 드라이브를 당겨 꺼낼 수 있습니다. 그러나, 이 가이드에서는 안정적인 컴퓨터 상태에서 각 시나리오가 시작되도록 하기 위해서 장치 드라이버를 제거해야 합니다. 만약 지시에 따라 장치를 제거하고 삭제하지 않으면, 아래 시나리오에서 테스트한 정책이 적용되지 않으며 예상되는 결과가 표시되지 않습니다. 장치를 제거하고 삭제할 때 이 가이드에서 지시하는 단계를 사용하십시오.

중요) 마지막 단계까지 진행할 때까지 USB 포트에서 장치를 물리적으로 분리하지 마십시오.

USB 메모리 드라이브 삭제하기

① DMI-Client1₩TestAdmin 으로 컴퓨터 로그인

② 장치 관리자 실행 (시작 – 실행 – mmc devmgmt.msc 입력 후 실행)

③ User Account Control 대화상자가 나타나면, 표시 내용 확인한 다음 Continue 클릭

④ USB 메모리 드라이브 항목에서 우클릭한 다음, Uninstall 클릭

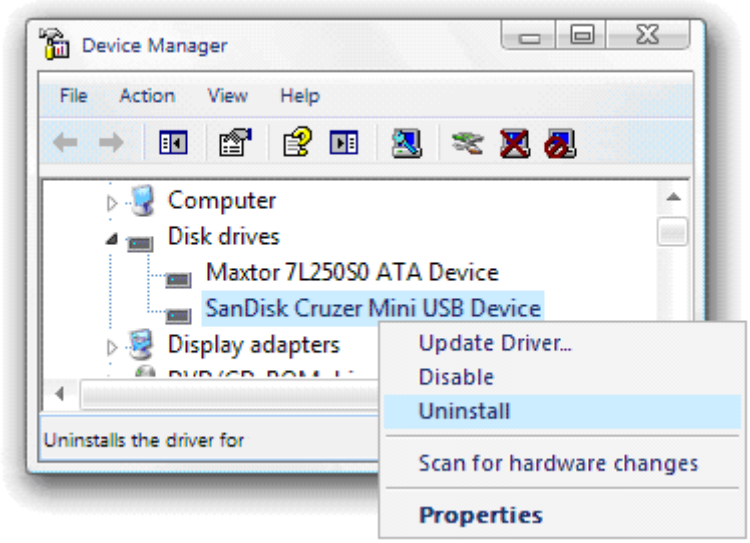

그림 6) 우클릭하여 USB 메모리 드라이브 삭제

⑤ Confirm Device Removal 대화 상자에서, 삭제 처리 절차를 완료하기 위해 OK 클릭

⑥ 윈도우에서 삭제 처리 절차가 완료되면 장치 관리자 트리에서 장치 항목이 제거됨

⑦ USB 포트에서 USB 메모리 드라이브 분리

5. 모든 장치 설치 금지

이 시나리오는 모든 장치 설치를 금지하고 기존 장치를 새 장치 드라이버로 업데이트 할 수 없게 하는 제한적인 구성을 구현하는데 필요한 일반적인 단계를 설명합니다. 사용자는 관리자의 승인 없이 장치를 설치하거나 사용할 수 없습니다. 관리자는 필요에 따라 모든 장치를 설치하거나 업데이트 할 수 있습니다.

5.1. 모든 장치의 설치를 금지하기 위한 필수 구성 요소

이 시나리오의 절차를 완료하려면, "4.1.3. USB 메모리 드라이브 삭제하기" 절차를 참고하여 시스템에 설치된 USB 메모리 드라이브를 제거해야 합니다.

5.2. 모든 장치의 설치를 금지하기 위한 단계

- 모든 장치 설치를 금지하기 위한 정책 구성
- 관리자가 장치 설치 제한을 무시할 수 있도록 정책 구성
- 사용자별 제한 설정 정책 적용 테스트

5.2.1. 모든 장치 설치를 금지하기 위한 정책 구성

모든 장치의 설치 또는 업데이트를 금지하는 정책을 구성하려면

① DMI-Client1₩TestAdmin 으로 컴퓨터 로그인

② 그룹정책 편집기 실행 (시작 – 실행 – mmc gpedit.msc 입력 후 실행)

③ User Account Control 대화상자가 나타나면, 표시 내용 확인한 다음 Continue 클릭

④ 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Device Installation – Device Installation Restrictions 으로 이동

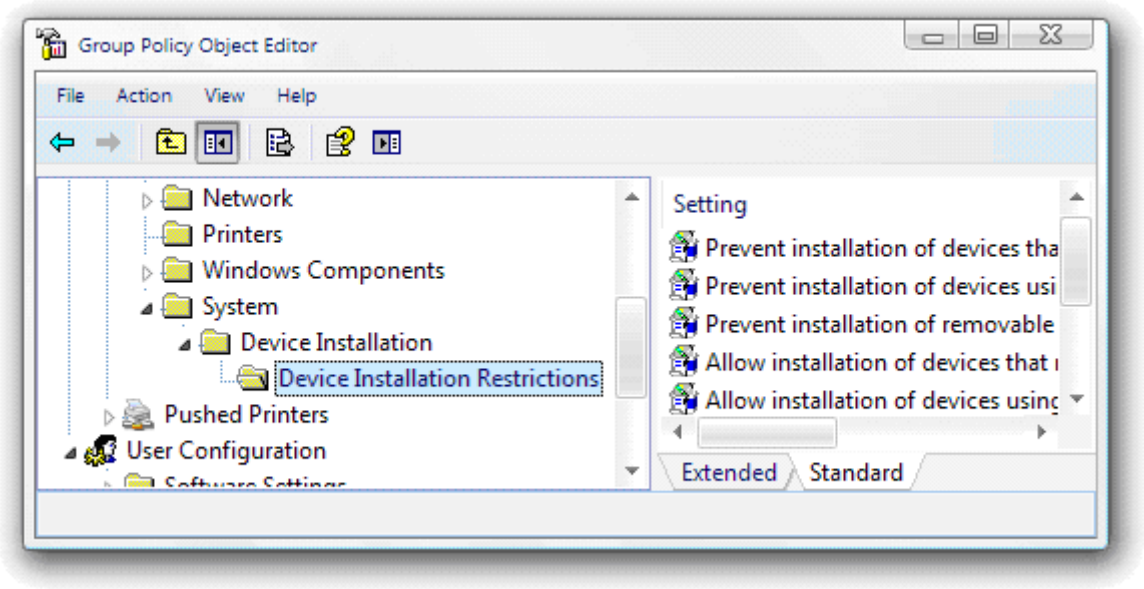

그림 7) 그룹정책 편집기 화면

⑤ 오른쪽 세부 정보 표시 패널에서, Prevent installation of devices not described by other policy settings 항목 우클릭하여 Properties 클릭

⑥ 현재 설정에 대한 정책 대화 상자가 실행

⑦ Setting 탭에서, 정책을 활성화하기 위해 Enabled 클릭

⑧ 설정을 저장하기 위해 OK 클릭

5.2.2. 관리자가 장치 설치 제한을 무시할 수 있도록 정책 구성

다음 정책을 통해 관리자는 방금 활성화한 정책을 포함하여 다른 장치 설치 정책 설정에 의한 제한 사항에 대해 영향을 받지 않도록 재정의 할 수 있습니다.

장치 설치 제한을 무시할 수 있도록 관리자를 허용하는 정책을 구성하려면

① 오른쪽 세부 정보 표시 패널에서, Allow administrators to override device installation policy 항목 우클릭 후, Properties 항목 클릭

② 현재 설정에 대한 정책 대화 상자가 실행

③ Setting 탭에서, 정책을 활성화하기 위해 Enabled 클릭

④ 설정을 저장하기 위해 OK 클릭

⑤ 이제 두 가지 정책 모두 상태가 활성화된 것으로 표시

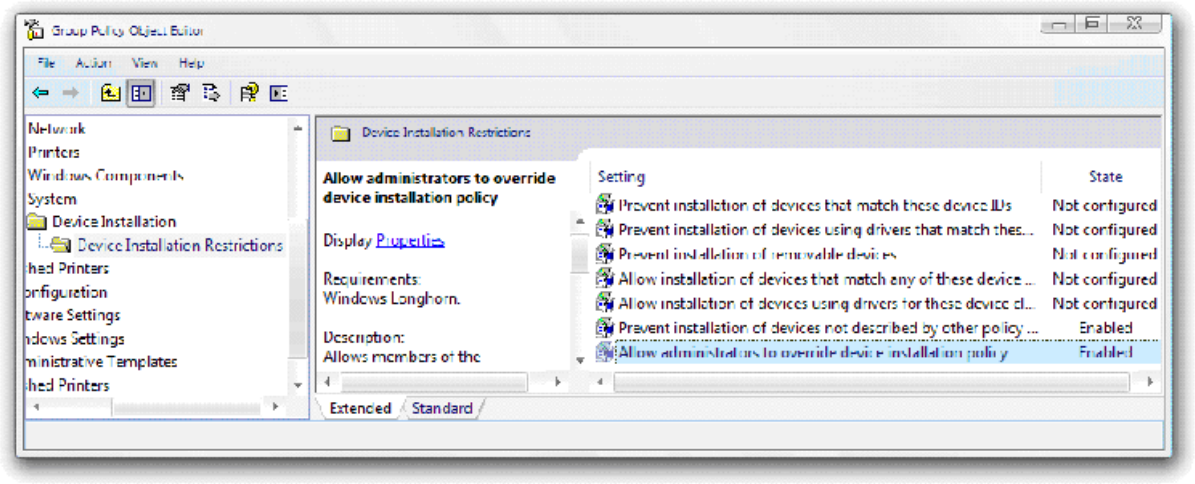

그림 8) 두 가지 정책의 상태가 활성화로 표시

5.2.3. 사용자별 제한 설정 정책 적용 테스트

두 정책을 모두 사용하도록 설정한 경우, 정책을 컴퓨터에 적용하고 장치 설치를 시도하여 제한 정책이 작동하는지 확인할 수 있습니다.

사용자별 제한 설정 정책 적용 테스트를 하려면,

① 만약 컴퓨터에 장치가 이미 설치되어 있다면, "4.1.3. USB 메모리 드라이브 삭제하기" 절차를 참고하여 컴퓨터에서 해당 장치를 삭제하고 제거

② 현재 그룹정책 설정을 수동 업데이트 (시작 – 실행 – gpupdate /force 입력 후 실행)

③ 그룹정책 설정 업데이트가 완료되면, 컴퓨터를 로그오프하고, DMI-Client1₩TestUser 로 로그인

④ 장치관리자 실행 (시작 – 실행 – mmc devmgmt.msc 입력 후 실행)

⑤ 아래와 같은 경고 메시지가 보이면, 장치관리자에서 변경할 수 있는 권한이 없다는 것을 의미

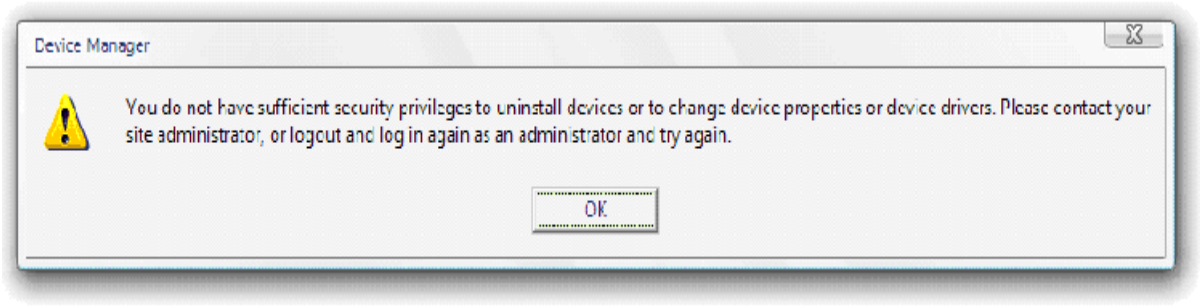

그림 9) 권한이 없다라는 경고 메시지

⑥ OK 클릭하여 메시지 확인하면 장치관리자가 실행되고 컴퓨터의 장치들이 보임

⑦ USB 메모리 드라이브를 컴퓨터에 연결

⑧ 장치 설치가 완료될 때까지, 장치관리자의 Other devices 노드에 장치가 표시됨

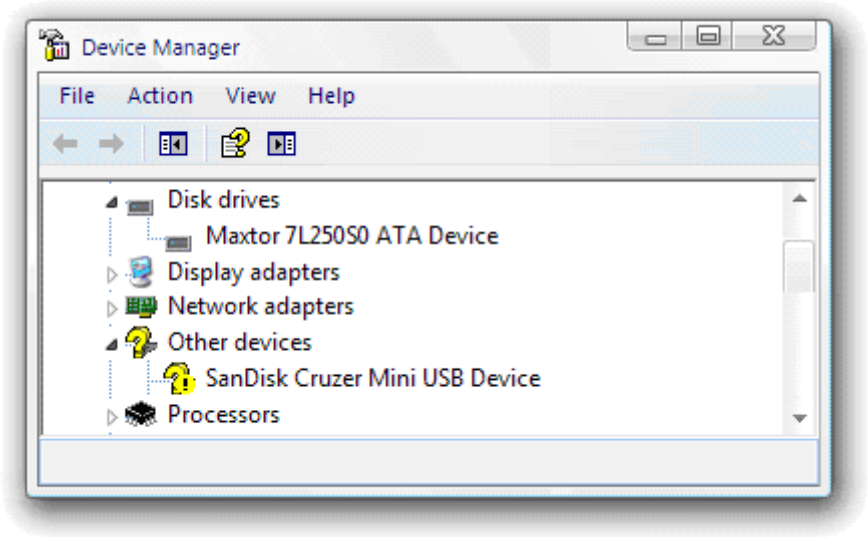

그림 10) 설치가 완료될 때까지 Other devices 노드에 표시됨

⑨ 관리자 권한 없는 표준 사용자로 로그온하고 장치 설치 제한 정책으로 인해 다음과 같은 대화상자가 나타남

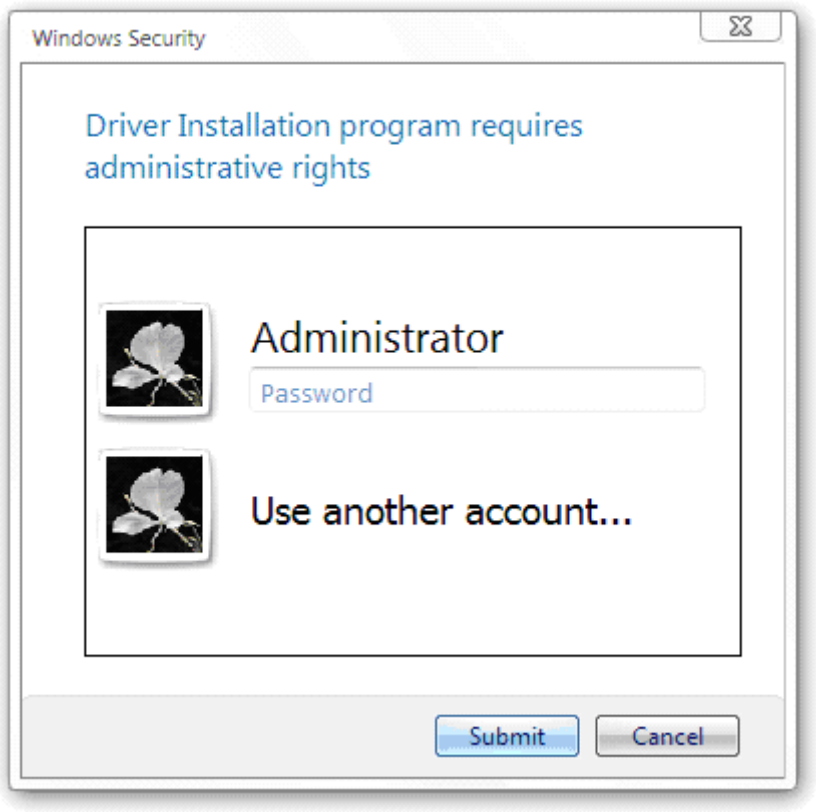

그림 11) 관리자 권한 없이 표준 사용자로 로그온 했을 때 보여지는 메시지

⑩ 일반적인 사용자 응답을 시뮬레이션 하기 위해, Locate 클릭하고 드라이버 소프트웨어 설치 (권장)

⑪ 관리자 권한이 있는 계정의 사용자 이름과 암호를 묻는 User Account Control 대화 상자가 실행됨

⑫ 사용자는 제공할 관리자 자격 증명이 없으므로, 사용자 시도를 중단하기 위해 Cancel 를 클릭

⑬ 장치 드라이버 설치가 실패되고 장치는 계속 Other devices 노드에 남아 있으면서 작동하지 않음

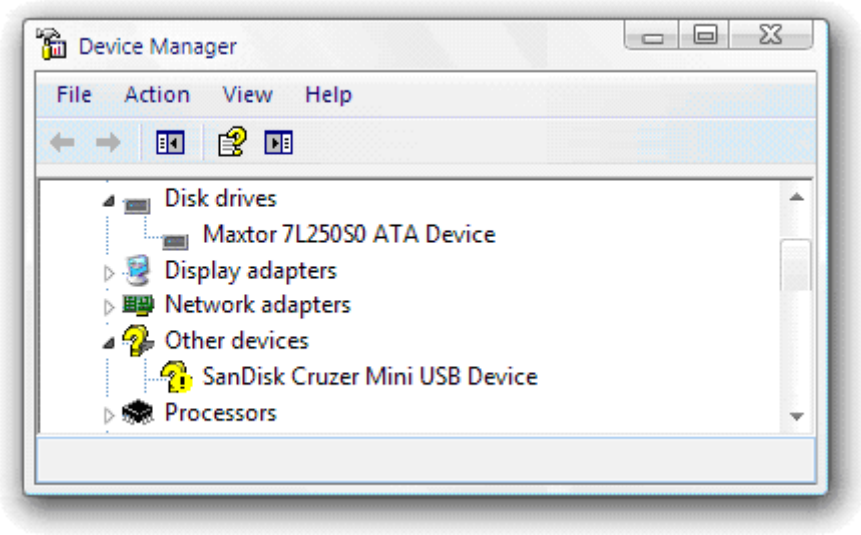

그림 12) 장치 설치 실패하여 장치가 작동하지 않음

6. 사용자가 승인된 장치만 설치하도록 허용

이 시나리오는 "5. 모든 장치 설치 금지" 시나리오를 기반으로 합니다. 이 시나리오에서는 허용된 장치 목록을 정책에 추가하고 USB 메모리 드라이브에 대한 하드웨어 ID 를 포함시킵니다.

6.1. 사용자가 승인된 장치만 설치하도록 허용하기 위한 필수 구성 요소

이 작업을 완료하려면, "5. 모든 장치 설치 금지" 시나리오의 모든 단계를 완료해야 합니다.

6.2. 사용자가 승인된 장치만 설치하도록 허용하는 단계

이 섹션에서는 권한이 부여된 장치 목록을 만들어 "5. 모든 장치 설치 금지" 에 지정된 제한 목록에 허용된 장치를 추가합니다.

6.2.1. 권한이 부여된 장치 목록 생성

승인된 장치 목록을 만들려면,

① DMI-Client1₩TestAdmin 계정으로 컴퓨터 로그온

② 만약 컴퓨터에 장치가 이미 설치되어 있다면, 컴퓨터에서 해당 장치를 삭제하고 제거

③ 그룹정책 편집기 실행 (시작 – 실행 – gpedit.msc 입력 후 실행)

④ 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Device Installation – Device Installation Restrictions 으로 이동

⑤ 오른쪽 세부 정보 패널에서 Allow installation of devices that match any of these device IDs 우클릭 후 Properties 클릭

⑥ 현재 설정에 대한 정책 대화 상자가 실행

⑦ Setting 탭에서, 정책을 활성화하기 위해 Enabled 클릭

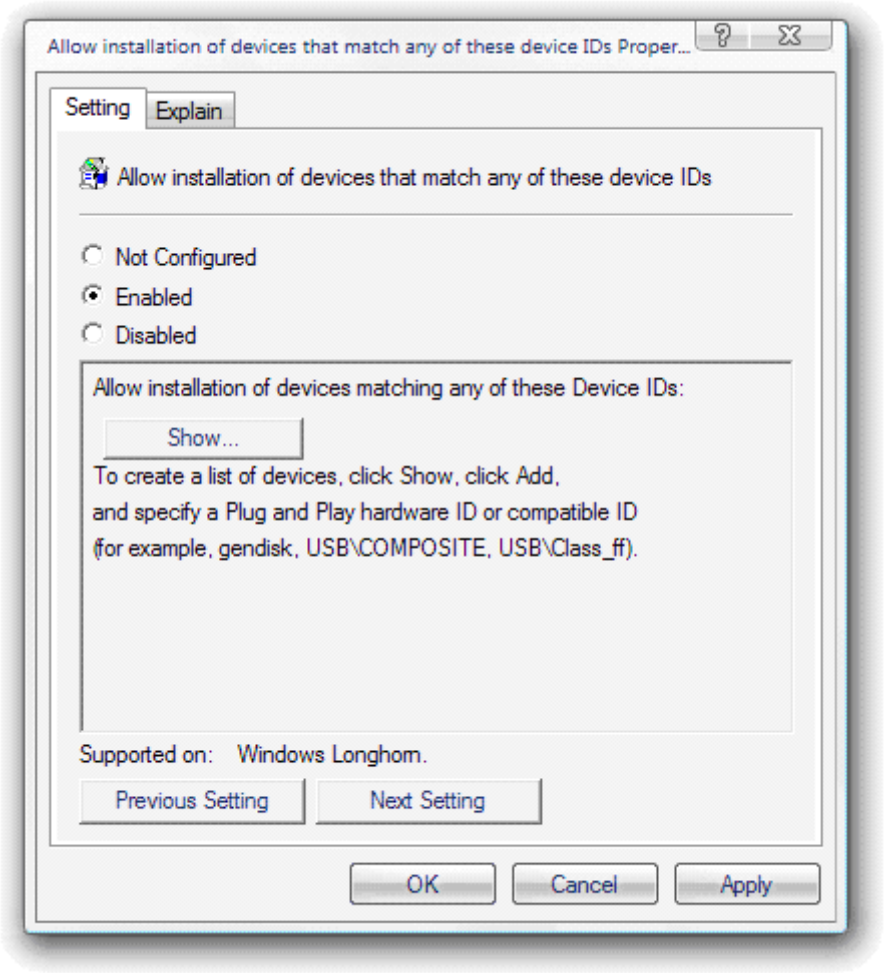

그림 13) 정책을 활성화하기 위해 Enabled 선택

⑧ Show Contents 대화 상자 안의 허용된 장치 목록을 보기 위해 Show 클릭 (기본적으로 해당 목록은 비어 있음.)

⑨ Add Item 대화 상자를 열기 위해 Add 클릭

⑩ 해당 장치의 장치 ID 값을 입력

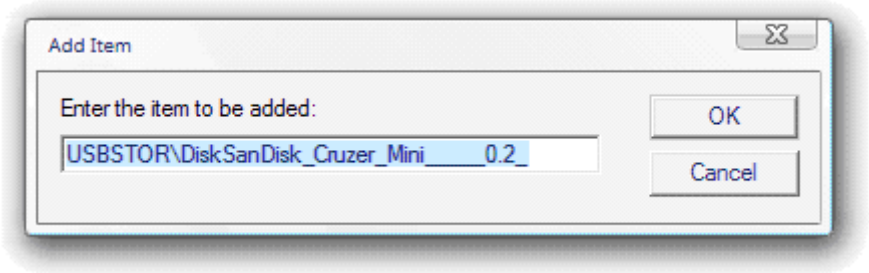

그림 14) USB 장치에 대한 장치 ID 입력

⑪ Show Contents 대화 상자로 나오기 위해 OK 클릭, 추가한 장치 ID 가 목록에 보임

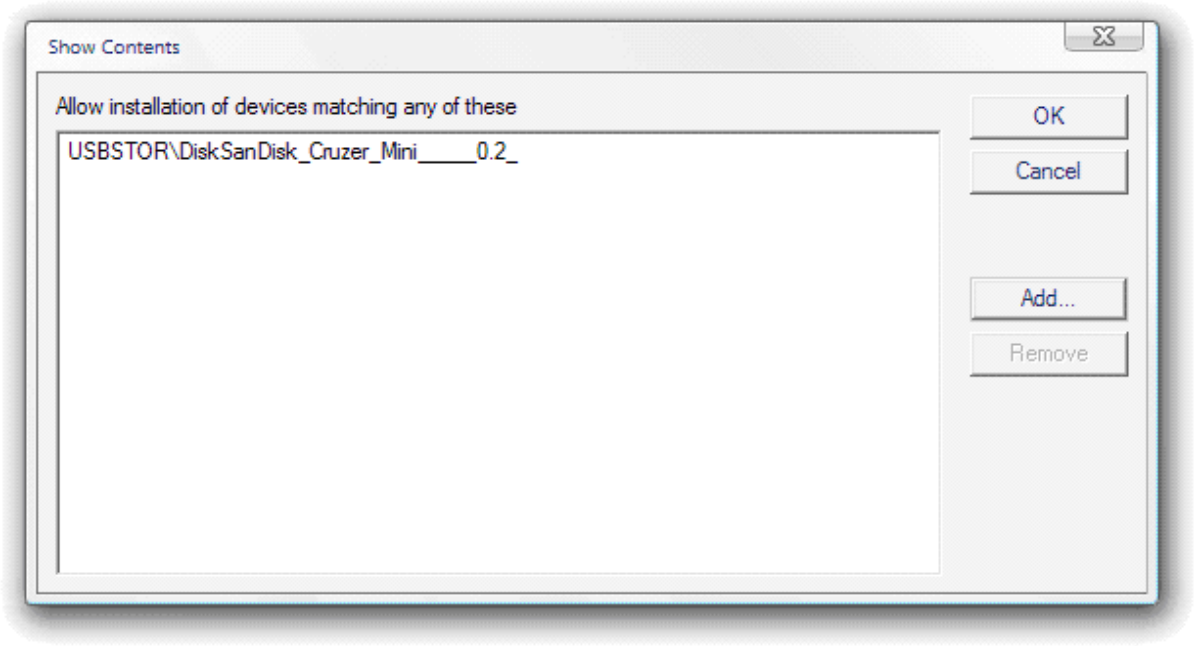

그림 15) 설치 승인된 장치 목록

⑫ 새로운 그룹 정책을 저장하기 위해 OK 클릭

6.2.2. 권한이 부여된 장치 설정 정책 적용 테스트

해당 정책 설정을 활성화하면 컴퓨터에 적용하고 장치 설치를 시도할 수 있습니다.

권한이 부여된 장치 목록을 테스트하려면,

① 현재 그룹정책 설정을 수동 업데이트 (시작 – 실행 – gpupdate /force 입력 후 실행)

② 그룹정책 수동 업데이트가 완료되면, 컴퓨터를 로그오프하고 DMI-Client1₩TestUser 로 로그온

③ 장치관리자 실행 (시작 – 실행 – mmc devmgmt.msc 입력 후 실행)

④ 아래와 같은 경고 메시지가 보이면, 장치관리자에서 변경할 수 있는 권한이 없다는 것을 의미

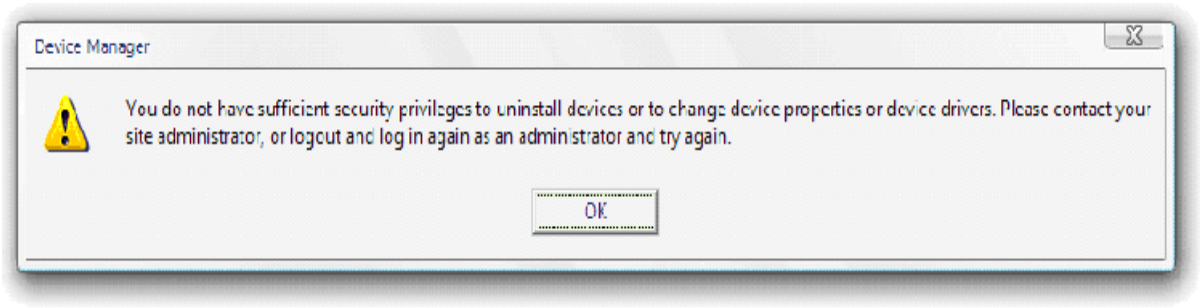

그림 16) 권한이 없다라는 경고 메시지

⑤ OK 클릭하여 메시지 확인하면 장치관리자가 실행되고 컴퓨터의 장치들이 보임

⑥ 컴퓨터에 USB 메모리 드라이브 연결

⑦ 윈도우가 설치를 완료할 때까지, 해당 장치는 Other Devices 노드에 위치함

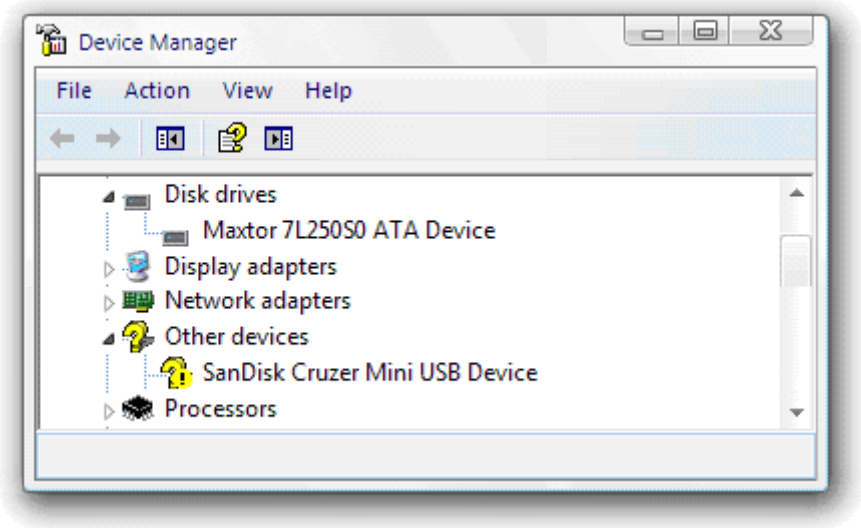

그림 17) 설치가 완료될 때까지 Other devices 목록에 해당 장치 표시

⑧ 윈도우에서 설치가 완료되면, 장치는 장치관리자의 Disk Drives 노드로 이동 후 정상 작동하게 됨

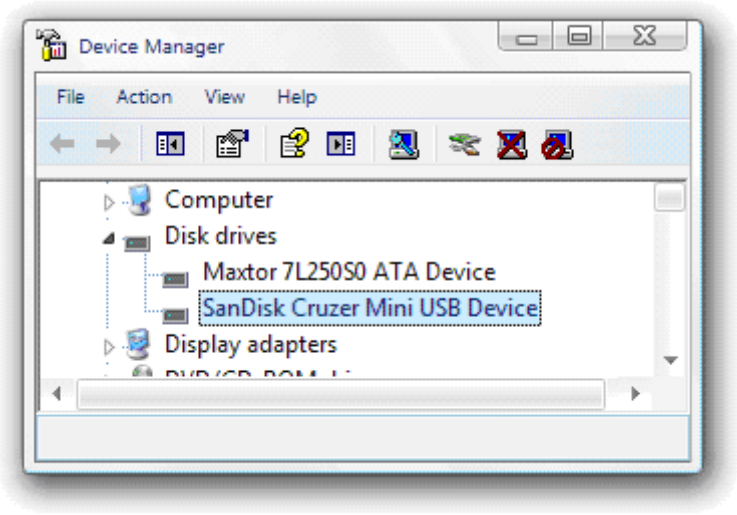

그림 18) 설치 완료 후 장치는 정상 작동하게 됨

7. 금지된 장치 설치 금지

이 시나리오는 장치 설치를 제어하는 다른 방법을 제시합니다. 처음 두 시나리오에서는 권한이 부여된 장치 목록에서 허용하는 장치를 제외한 모든 장치의 설치를 금지했습니다. 이 시나리오에서는 금지된 장치 목록에 있는 장치를 제외한 모든 장치의 설치를 허용합니다. 첫 번째 시나리오에서 작성한 관리자에 대한 예외 정책도 제거하여 관리자 조차도 이 정책의 영향을 받도록 설정합니다.

7.1. 금지된 장치의 설치를 방지하기 위한 선행 조건

"5. 모든 장치 설치 금지" 및 "6. 사용자가 승인된 장치만 설치하도록 허용" 의 모든 단계를 완료한 경우, 다음 단계를 진행하여 해당 정책들을 비활성화 해야 합니다.

모든 장치 설치 활성화

① DMI-Client1₩TestAdmin 으로 컴퓨터 로그인

② 그룹정책 편집기 실행 (시작 – 실행 – mmc gpedit.msc 입력 후 실행)

③ 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Device Installation – Device Installation Restrictions 으로 이동

④ 오른쪽 세부 정보 패널에서 Prevent installation of devices not described by other policy settings 우클릭 후 Properties 클릭

⑤ 현재 설정에 대한 정책 대화 상자가 실행

⑥ 정책 설정을 비활성화하기 위해 Disabled 클릭

⑦ 그룹 정책을 저장하기 위해 OK 클릭

다음 단계는 관리자 그룹의 구성원에게 예외를 부여한 정책을 제거하는 것입니다.

장치를 설치할 수 있도록 Administrators 그룹의 구성원에 대한 예외 처리 제거

① 그룹정책 편집기에서 Allow administrators to override device installation policy 우클릭 후 Properties 클릭

② 현재 설정에 대한 정책 대화 상자가 실행

③ Setting 탭에서 정책 설정을 비활성화하기 위해 Disabled 클릭

④ 그룹 정책을 저장하기 위해 OK 클릭

다음 단계는 승인된 장치 목록에서 하드웨어 ID 를 제거하는 것입니다.

승인된 장치 목록에서 하드웨어 ID 제거

① 그룹정책 편집기에서 Allow installation of devices that match any of these device IDs 우클릭 후 Properties 클릭

② 현재 설정에 대한 정책 대화 상자가 실행

③ Setting 탭에서 승인된 장치 목록을 보기 위해 Show 클릭

④ Show Contents 대화상자에서, USB 메모리 드라이브 선택하여 Remove 클릭하여 장치 목록에서 제거

⑤ OK 클릭하여 Show Contents 대화상자 종료

⑥ 정책 설정을 비활성화하기 위해 Disabled 클릭

⑦ 그룹 정책을 저장하기 위해 OK 클릭

7.2. 금지된 장치의 설치를 방지하기 위한 단계

사용자가 특정 장치를 설치하지 못하게 하려면, 금지된 장치 목록을 작성해야 합니다.

7.2.1. 금지된 장치 목록 생성

금지된 장치 목록을 작성하려면,

① 만약 현재 장치가 설치되어 있다면, "4.1.3. USB 메모리 드라이브 삭제하기" 절차를 참고하여 USB 메모리 드라이브를 삭제하고 제거

② DMI-Client1₩TestAdmin 으로 컴퓨터 로그인

③ 그룹정책 편집기 실행 (시작 – 실행 – mmc gpedit.msc 입력 후 실행)

④ 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Device Installation – Device Installation Restrictions 으로 이동

⑤ 오른쪽 세부 정보 패널에서 Prevent installation of devices that match these device IDs 우클릭 후 Properties 클릭

⑥ 현재 설정에 대한 정책 대화 상자가 실행

⑦ Settings 탭에서 정책 설정을 활성화하기 위해 Enabled 클릭

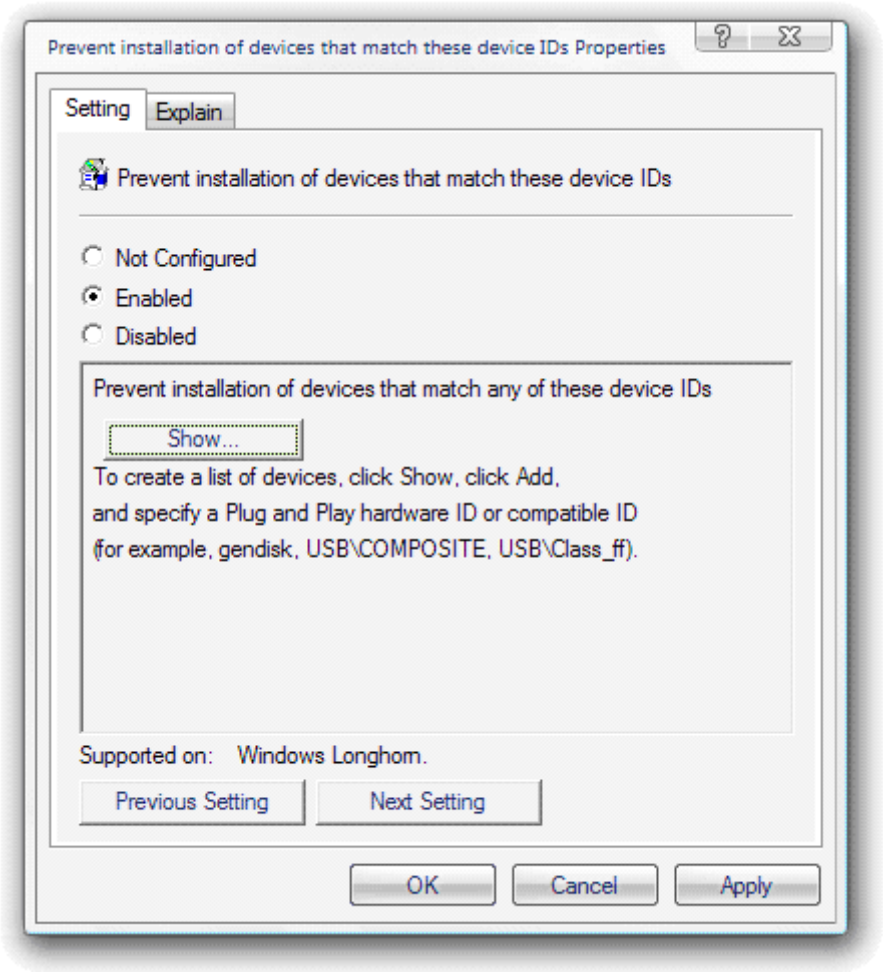

그림 19) 정책 활성화하기 위해 Enabled 클릭

⑧ 금지된 장치들 목록을 보기 위해 Show 클릭

⑨ Show Contents 대화상자에서 Add 클릭

⑩ Add Item 대화상자에서 금지할 장치에 대한 장치 ID 입력

⑪ OK 를 눌러 Show Contents 대화상자로 이동

⑫ 목록에서 등록한 장치 정보 확인

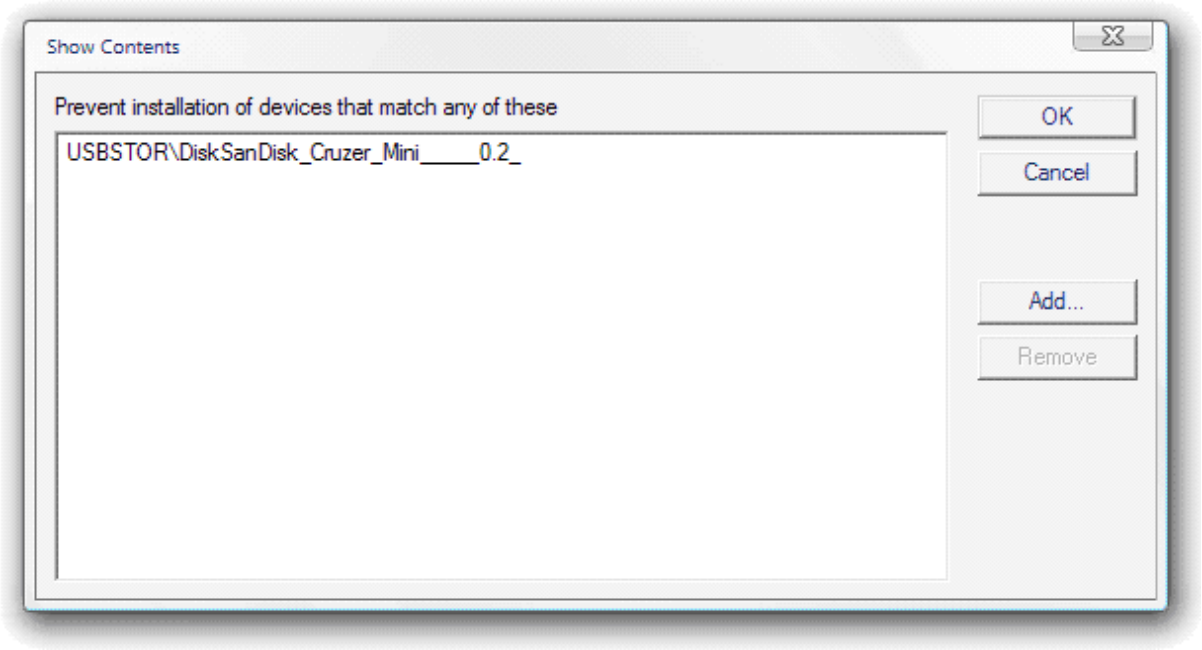

그림 20) 이 장치에 대한 설치가 이제 금지됨

⑬ 그룹 정책을 저장하기 위해 OK 클릭

7.2.2. 금지된 장치 목록 적용 테스트

이제 장치 설치를 시도할 수 있습니다. 정책은 더 이상 장치 설치를 막을 수 없기 때문에 다른 장치를 설치할 수 있습니다. 하지만 Administrators 그룹의 구성원으로 로그온 한 경우라도 이 특정 장치를 설치할 수는 없습니다.

금지된 장치 목록을 적용 테스트하려면,

① 그룹 정책을 강제로 다시 시작 (시작 – 실행 – gpupdate /force 입력 후 실행)

② 정책 업데이트 진행이 완료되면 명령 창 닫기

③ 장치 관리자 실행 (시작 – 실행 – mmc devmgmt.msc 입력 후 실행)

④ 시스템에 USB 메모리 드라이브 연결

⑤ 장치 관리자의 Other devices 노드에 해당 장치가 보임

⑥ 장치 설치가 완료되지 않아, 장치가 작동하지 않음

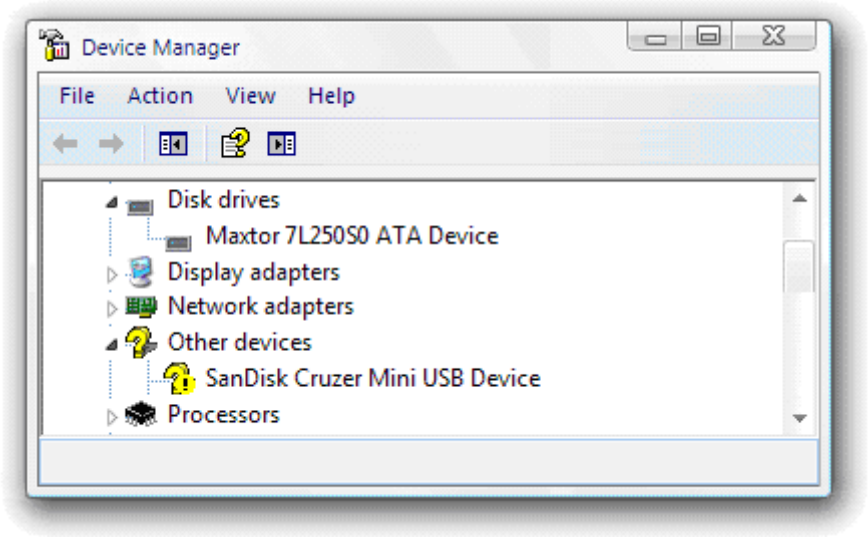

그림 21) 장치 설치가 완료되지 않아서 작동하지 않음

⑦ 윈도우는 시스템 알림 영역에 설치 실패 이유 메시지 표시

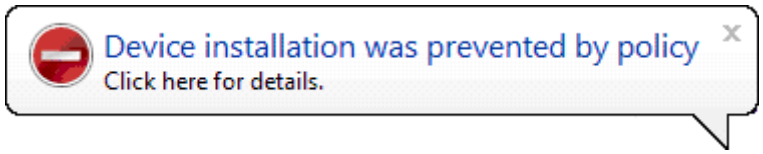

그림 22) 설치 실패 이유 관련 알림 메시지 출력

⑧ 장치 드라이버를 수동으로 설치하여 제한사항을 회피할 수 있습니다. 해당 장치에서 마우스 우클릭한 후 Update Driver Software 클릭

⑨ 시스템에서 장치에 대한 장치 드라이버를 제공하라는 메시지를 표시

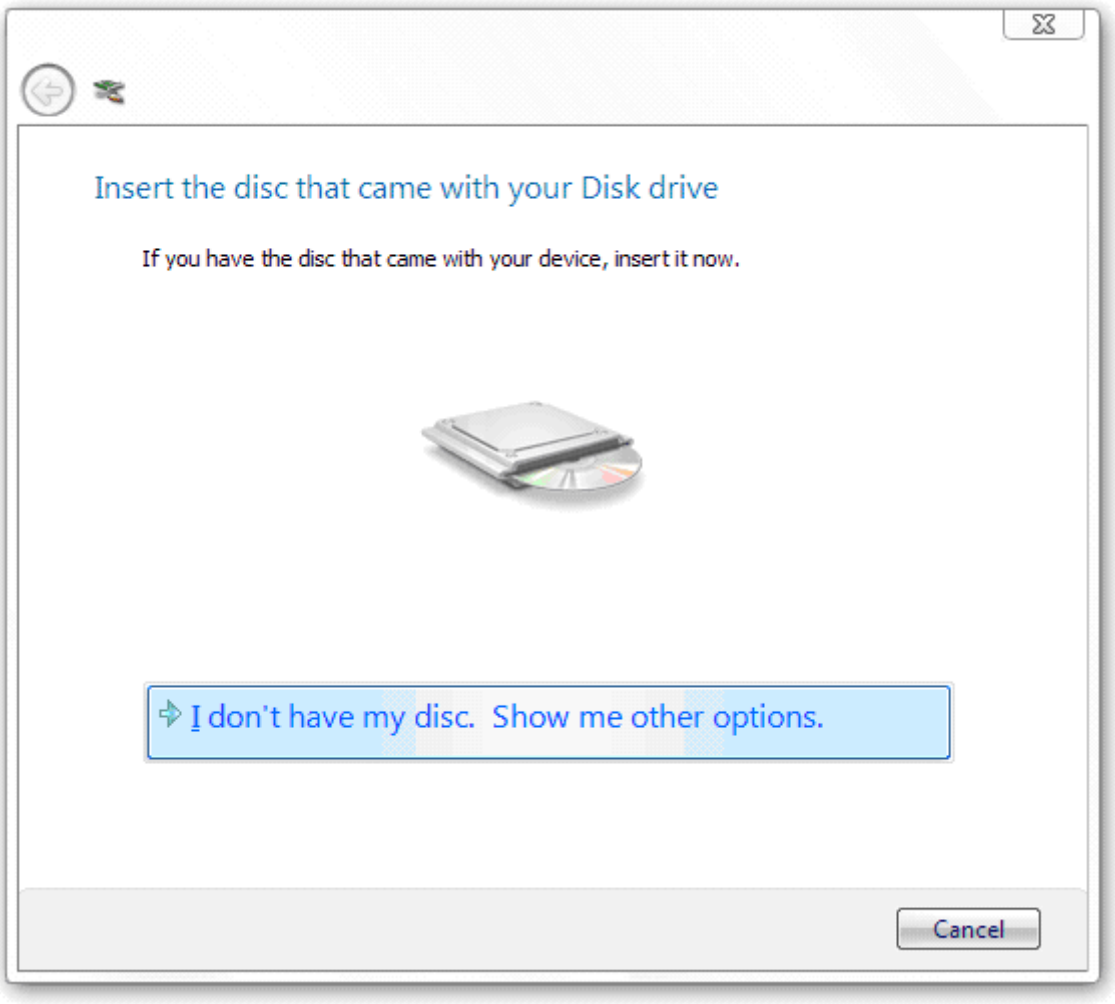

그림 23) 장치 드라이버 요구 메시지

⑩ 사용자가 무엇을 시도할지 시뮬레이션 하려면, Search automatically for updated driver software 클릭

⑪ 윈도우가 검색했지만 드라이버를 설치할 수 없다라는 메시지 출력

⑫ 마지막 문장은 설정한 시스템 정책으로 인해 설치 시도가 실패했다고 설명함

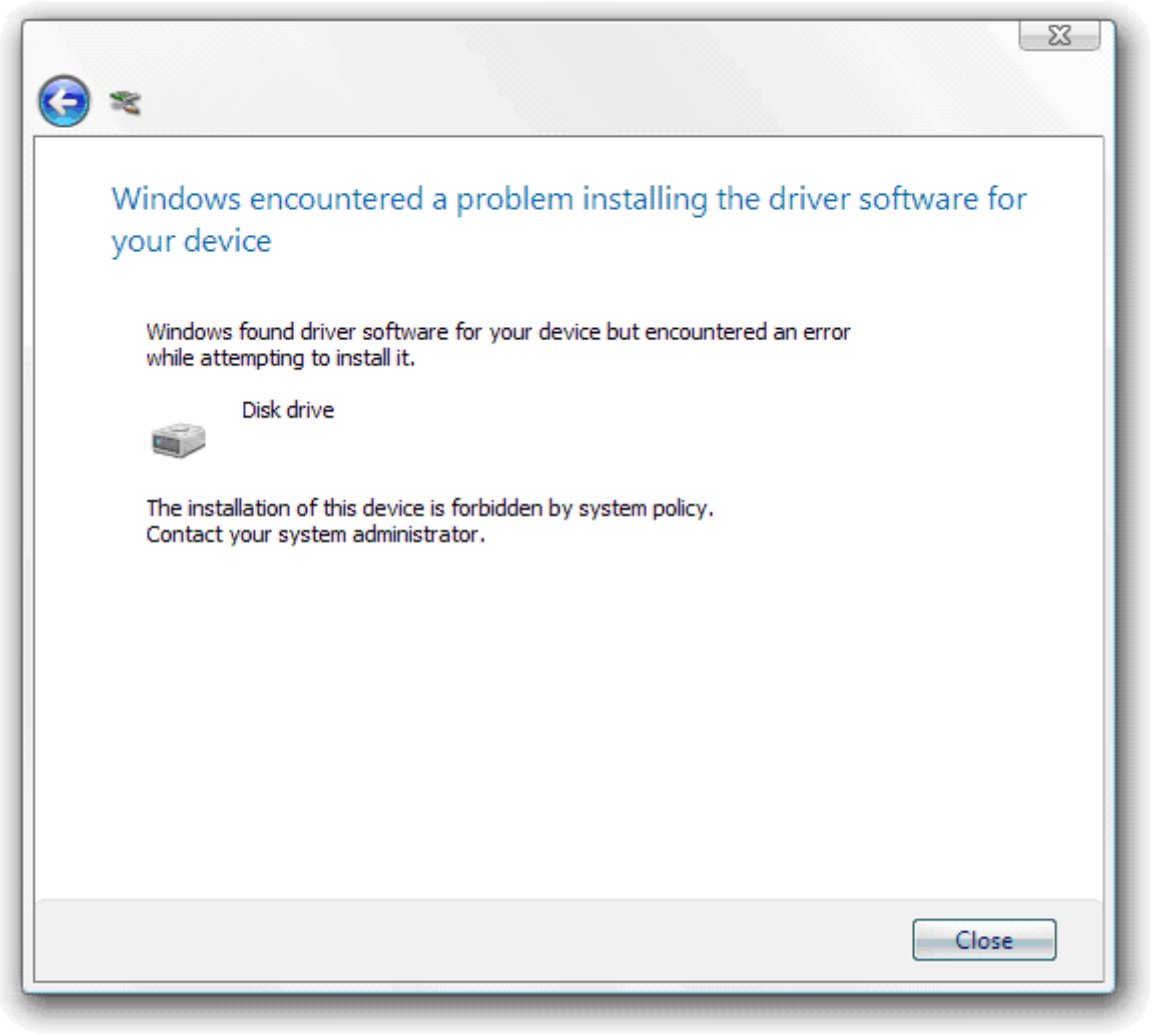

그림 24) 설치 실패 이유를 설명하는 대화상자

8. 이동식 미디어에 대한 읽기 및 쓰기 권한 제어

이 시나리오에서는 컴퓨터에서 이동식 장치 또는 이동식 미디어를 사용하는 장치에 대한 읽기 또는 쓰기 액세스를 제어하는 방법을 보여줍니다. 이 시나리오에서는 USB 메모리 드라이브를 읽기 전용으로 설정하기 위해 컴퓨터 정책을 설정합니다. 또한 컴퓨터에 연결된 모든 CD 또는 DVD 레코더를 읽기 전용으로 설정하기 위해 컴퓨터 정책을 설정합니다. 그러면, 레코딩 기능을 비활성화할 수 있습니다.

8.1. 이동식 미디어에 대한 읽기 및 쓰기 권한을 제어하기 위한 선행 조건

이 섹션의 절차를 수행하기 전에 USB 메모리 드라이브 설치를 막는 정책을 비활성화해야 합니다

USB 메모리 드라이브 설치를 막는 정책을 비활성화하려면,

① 만약 현재 장치가 설치되어 있다면, "4.1.3. USB 메모리 드라이브 삭제하기" 절차를 참고하여 해당 장치를 제거하고 삭제

② 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Device Installation – Device Installation Restrictions 으로 이동

③ 오른쪽 세부 정보 패널에서 Prevent installation of devices that match these device IDs 우클릭 후 Properties 클릭

④ 현재 설정에 대한 정책 대화 상자가 실행

⑤ Settings 탭에서 금지된 장치 목록을 보기 위해 Show 클릭

⑥ Show Contents 대화상자에서, USB memory drive 선택 후 Remove 클릭, 그런 다음 OK 클릭

⑦ Settings 탭에서 정책 설정을 비활성화하기 위해 Disabled 클릭

⑧ 변경한 정책을 저장하기 위해 OK 클릭

8.2. 이동식 미디어에 대한 읽기 및 쓰기 권한을 제어하기 위한 단계

- 특정 이동식 장치 클래스에 대한 쓰기 권한을 거부하도록 컴퓨터 정책 설정
- 컴퓨터 정책 설정 테스트

8.2.1. 특정 이동식 장치 클래스에 대한 쓰기 권한을 거부하도록 컴퓨터 정책 설정

이번 과정에서 설정한 정책은 많은 이동식 저장 장치에 대한 쓰기 액세스를 차단합니다. 그러나 장치에 대한 쓰기 액세스를 차단하는 정확한 컴퓨터 정책은 특정 제조업체 및 장치 모델에 따라 다를 수 있습니다. Custom Classes 정책을 사용할 수도 있지만, 특정 장치에 대한 장치 설치 클래스 GUID 를 식별해야 합니다.

특정 이동식 장치 클래스에 대한 쓰기 권한을 거부하려면,

① 그룹정책 편집기에서 Computer Configuration – Administrative Templates – System – Removable Storage Access 로 이동

② CD and DVD: Deny write access 항목에서 우클릭 후 Properties 클릭

③ Properties 대화상자에서, 제한 기능을 켜기 위해 Enabled 클릭 후 OK 클릭

④ 다음 컴퓨터 정책들에 대해서도 ②, ③ 단계 반복 설정

- ✓ Removable Disks: Deny write access
- ✓ Floppy Drives: Deny write access
- ✓ WPD Devices: Deny write access

⑤ 그룹 정책 편집기 종료

8.2.2. 컴퓨터 정책 설정 테스트

만약 장치가 사용 중이라면, 쓰기 액세스 제한 정책을 바로 적용할 수가 없습니다. 컴퓨터 정책을 적용하려면, 컴퓨터를 재시작해야 합니다.

컴퓨터 정책 설정을 테스트하려면,

① 그룹정책 강제 업데이트 (시작 – 실행 – gpupdate /force 입력 후 실행)

② 그룹정책 업데이트가 완료되면 컴퓨터를 재시작

③ DMI-Client1₩TestAdmin 계정으로 로그온

④ 시스템에 USB 메모리 드라이브를 연결한 후, 윈도우가 작동 중임을 알려줄 때까지 대기

⑤ 윈도우 탐색기를 실행한 다음, USB 메모리 드라이브를 더블 클릭하여 실행

⑥ 실행된 USB 메모리 드라이브 탐색기에서 마우스 우클릭하여 New – Folder 항목 클릭하여 새로운 폴더를 하나 생성

⑦ 윈도우에서 폴더 생성 실패 이유에 대한 에러 메시지를 출력

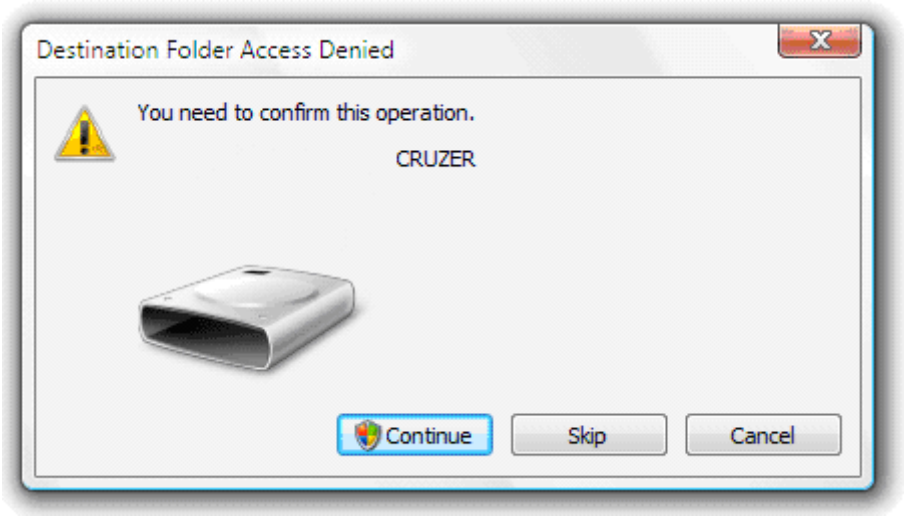

그림 25) 폴더 생성 시도 실패 이유에 대한 에러 메시지

⑧ 해당 창에서 Continue 를 눌러 제한 사항을 해결

⑨ 만약 User Account Control 대화상자가 표시되면, 표시되는 동작이 무엇인지 확인한 다음, Continue 클릭

⑩ 윈도우는 폴더에 쓸 수 없는 이유를 나타내는 두 번째 메시지를 표시

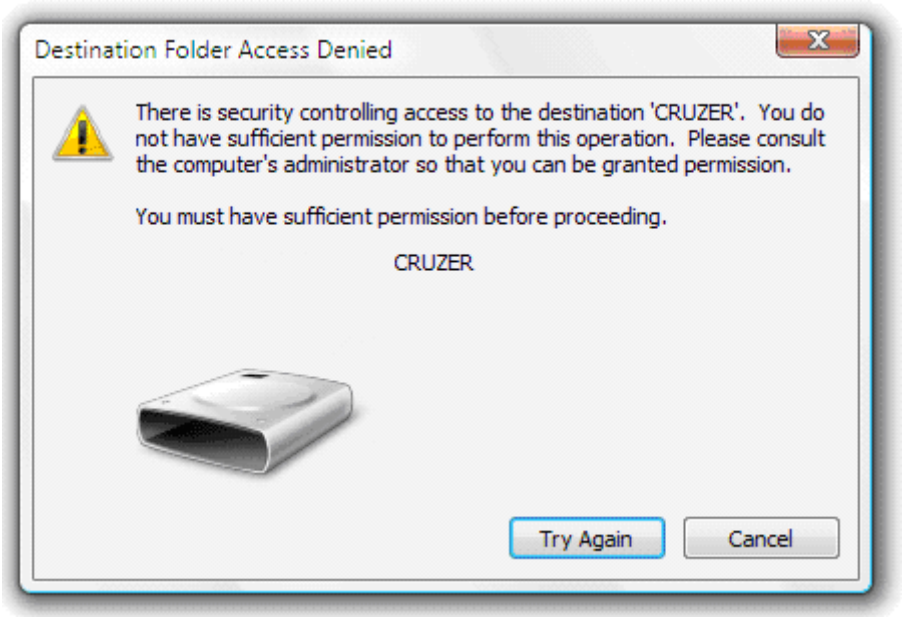

그림 26) 쓰기 권한이 허용되지 않음을 나타내는 두 번째 에러 메시지

9. 결론

이 가이드에서 샘플 장치를 사용하여 사용자가 장치를 설치할 수 있는지 여부를 제어하는 방법에 대해 학습했습니다. 또한 이동식 저장 장치나 이동식 미디어를 사용하는 장치에 대한 액세스를 제한하는 방법을 배웠습니다. 이 방법으로 설치 및 장치 사용을 제어하면 사용자가 설치할 수 있는 장치를 조직에서 승인하고 지원하는 장치로 제한하여 보안을 향상시키고 Help Desk 의 효율성을 높일 수 있습니다. 이러한 구성을 보여주기 위해 사용된 시나리오는 다음과 같습니다.

- **모든 장치 설치 금지**

  이 시나리오에서는, 일반 사용자가 모든 장치를 설치하지 못하게 금지했지만 관리자는 장치를 설치하거나 업데이트 할 수 있도록 허용했습니다.

- **사용자가 인증된 장치만 설치할 수 있도록 허용**

  이 시나리오에서는, 일반 사용자가 인증된 장치 목록에 포함된 장치만 설치할 수 있도록 허용했습니다.

- **금지된 장치만 설치 금지**

  이 시나리오에서는, 일반 사용자가 대부분의 장치를 설치할 수는 있지만 금지된 장치 목록에 포함된 장치를 설치하지 못하게 금지했습니다.

- **이동식 미디어 저장 장치의 사용 제어**

  이 시나리오에서는, 일반 사용자가 이동식 저장 장치 또는 USB 메모리 드라이브나 CD 또는 DVD 버너와 같은 이동식 미디어가 있는 장치에 데이터를 쓰는 것을 금지했습니다.

참고사이트

Step-By-Step Guide to Controlling Device Installation Using Group Policy

https://msdn.microsoft.com/en-us/library/bb530324.aspx#grouppolicydeviceinstall_topic4ac

끝.