Windows 10 IoT Enterprise 정품 인증 가이드

목 차

1. 소개 2
2. 정품인증 이란? 2
3. 정품인증 과정 소개 3
4. 정품인증 준비 5
4.1. 제품 키 5
4.2. OEM 이미지 완성 5
5. 정품인증 방법들 6
5.1. 인터넷 직접 연결 시나리오 6
5.2. 프록시 도구를 이용한 인터넷 연결 시나리오 6
5.3. 인터넷 미연결 시나리오 7
6. 정품인증 도구 7
6.1. Volume Activation Management Tool 3.1 (VAMT 3.1) 7
6.2. Windows Software Licensing Management Tool (slmgr.vbs) 8
6.3. Windows Activation UI (slui.exe) 8
7. 정품 재인증 8
7.1. 인터넷 직접 연결을 통한 Windows 10 IoT Enterprise 장치 활성화 9
7.2. VAMT 3.1 도구를 이용하여 인터넷을 통한 장치 활성화 12
7.3. 인터넷에 대한 프록시 연결을 이용하여 Windows 10 IoT Enterprise 장치 활성화 15
7.4. 전화를 이용하여 Windows 10 IoT Enterprise 장치 활성화 24

1. 소개

이 가이드는 공장 및 현장에서 Windows 10 IoT Enterprise 이미지를 활성화 (정품인증) 하고 다시 활성화 (정품 재인증) 하는 방법에 대한 개요 및 자세한 지침을 제공합니다.

모든 Windows 10 IoT Enterprise 장치는 반드시 활성화 (정품인증) 를 해야 합니다. 장치 활성화 (정품인증) 는 장치가 인터넷 연결을 통하여 직접 Microsoft AVS (Activation Verification Server) 에 연결되거나 프록시 도구를 통해 간접적으로 Microsoft AVS 에 연결하여 완료될 수 있습니다. 또는, Windows 10 IoT 부터 인터넷에 연결되지 않은 장치에 대해 지연된 활성화 (Deferred Activation) 상태로 유지될 수 있는 세 번째 옵션을 제공합니다. 이 세 번째 옵션은 Windows 10 IoT 에서 처음 제공하는 옵션입니다.

2. 정품인증 이란?

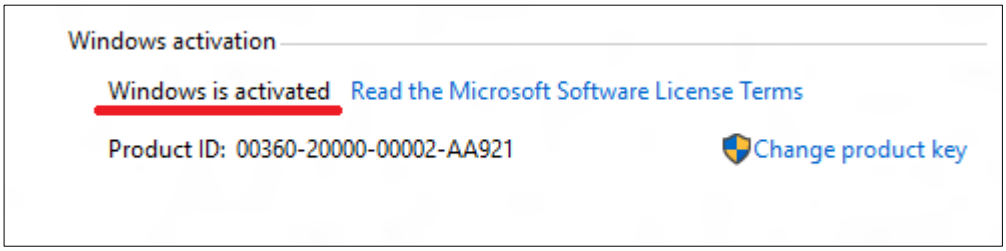
정품인증은 Windows 10 IoT Enterprise 를 Microsoft 에 등록하여 해당 제품이 정품인지 확인하는 프로세스입니다. 정품인증은 다음과 같은 목적으로 사용됩니다.

- 소프트웨어 불법 복제 및 사용 감소
- 소프트웨어 산업, 기업 지적 재산권, 소프트웨어 개발 투자 및 제품 품질 보호
- 고객이 기대하는 제품 품질을 받을 수 있도록 보증

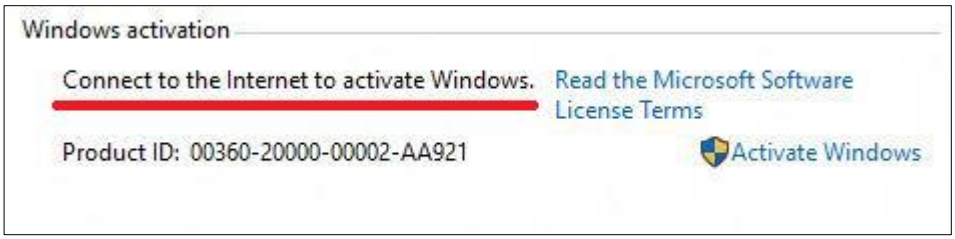
기본적으로는 각 장치를 활성화 (정품인증) 해야 합니다. 만약, 장치가 인터넷에 연결되어 있지 않다면, 그 장치는 지연된 활성화 (Deferred Activation) 상태로 남아 있게 됩니다. 만약, 장치가 인터넷에 연결된다면, 그 장치는 인터넷을 통해 자동적으로 활성화 (정품인증) 가 됩니다. 만약, 장치가 인터넷에 연결되었고 유효하지 않은 제품 키 또는 활성화 가능한 할당량을 초과한 제품 키 때문에 활성화 (정품인증) 이 실패한 다면, 그 장치는 활성화 (정품인증) 가 안된 상태가 됩니다.

다음과 같이 세 가지 경우의 장치 상태가 있습니다.

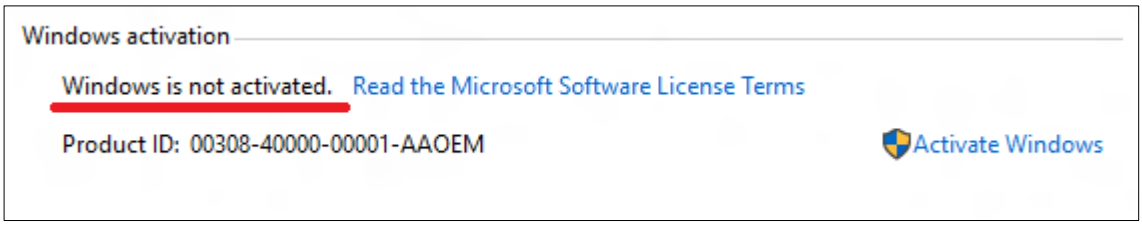
■ **활성화된 상태**



■ **지연된 활성화 상태**



■ **비 활성화된 상태**



장치가 활성화 (정품인증) 된 후에는, 메인보드 교체 또는 장치의 완전 재구성 같은 중요한 하드웨어 변경으로 인해 장치를 다시 활성화 (정품 재인증) 해야 하는 경우를 제외하고는, 장치가 활성화 (정품인증) 된 상태로 유지됩니다.

3. 정품인증 과정 소개

각 장치는 활성화 (정품인증) 를 하기 위해 유효한 제품 키를 가지고 있어야 합니다. 활성화 (정품인증) 과정은 다음과 같이 여러 단계를 거쳐 진행됩니다.

① 제품 키를 해당 장치에 적용합니다. (제품 키 입력)

② 장치로부터 라이선스 상태 정보를 가져옵니다. (정보 추출)

③ 장치를 활성화하기 위해 인터넷에 연결하거나, 지연된 활성화 상태로 남겨둡니다.

a. 장치를 지연된 활성화 상태로 남겨둡니다.

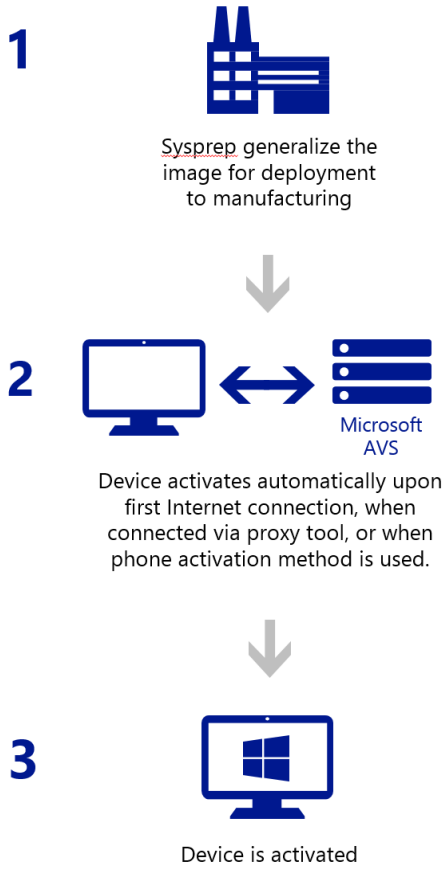
b. 활성화 (정품인증) 하려면: 장치를 인터넷에 직접 연결하거나, 프록시 활성화 도구를 사용하여 장치를 인터넷에 간접적으로 연결하거나, 인터넷에 연결할 수 없는 경우 전화를 사용하여 Microsoft 라이선스 서버를 통해 활성화합니다.

이 시점에 장치는 자동으로 라이선스 상태 정보를 보내거나, 혹은 전화를 사용하는 경우에는 사용자 입력을 통하여 상태 정보를 보냅니다. 그러면 장치는 자동적으로:

i. Microsoft 라이선스 서버로부터 Confirmation ID (CID) 를 가져옵니다.

ii. 해당 장치에 Confirmation ID 가 적용하면 바로 장치가 활성화됩니다.

④ OEM 은 라이선스 사용을 보고하기 위한 sales-out 보고 요구 사항을 가질 수 있습니다.



■ **활성화되지 않았을 때의 동작**

Windows 10 IoT Enterprise 장치 활성화 (정품인증) 시도가 유효하지 않은 제품 키 혹은 할당량을 초과한 제품 키로 인하여 실패했을 때, 해당 장치에 연결된 출력 화면 오른쪽 하단 위치에 아래와 같은 워터마크를 보여줍니다. 이 워터마크는 활성화가 실패한 후 3 시간 있다가 나타납니다. 또한, 활성화 (정품인증) 되지 않은 장치에서 사용자는 데스크톱 배경 혹은 잠금 화면 배경과 같은 윈도우 개인 설정을 변경할 수도 없습니다. 이 점들이 활성화된 장치 또는 지연된 활성화 상태의 장치와 비교하여 비활성화된 장치의 차이점입니다.

4. 정품인증 준비

4.1. 제품 키

Windows 10 IoT Enterprise 제품에 적용 가능한 제품 키들입니다.

- **Embedded Product Key Entry Activation (ePKEA)**

  ePKEA 키는 OEM 에 배포되고 지원됩니다. 이 유형의 제품 키는 여러 장치들을 키에 부과된 최대 한도까지 여러 번 활성화하는데 사용됩니다.

- **Product Key Entry Activation (PKEA) keys**

  PKEA 키는 OEM 에 배포되고 지원됩니다. 이 유형의 제품 키는 고유 키마다 하나의 단일 설치된 윈도우를 활성화하는데 사용됩니다.

- **OEM Activation 3.0 (OA 3.0) key**

  OA 3.0 키는 OEM Activation 3.0 시스템을 사용 시에만 단독으로 사용됩니다. 이 OA 3.0 시스템을 사용하려면 Microsoft 담당자에게 문의해야 합니다.

4.2. OEM 이미지 완성

다음 단계를 통해 Sysprep 실행 후 OOBE 초기 진행 과정에서 나타나는 라이선스 키 입력 대화 상자를 표시하지 않게 하고, 제품 키가 불법적으로 이미지로부터 추출되지 않도록 보호하고, 대량 배포를 위해 마스터 이미지를 준비할 수 있습니다. 이 명령들이 수행되는 순서는 매우 중요합니다.

*보안 업데이트 KB3074679 설치 필요

① 타겟 장치에 Windows 10 설치 미디어를 넣고 부팅

② OEM ePKEA 혹은 PKEA 제품 키 입력: 25자리 XXXXX- XXXXX- XXXXX- XXXXX- XXXXX

③ CMD 명령 창을 띄운 후, 'sysprep /audit /reboot' 입력, 실행

④ 재부팅 후, Sysprep 대화상자를 끄고, 설치 시 생성한 사용자 계정 제거, 그리고 OEM 이 제공하는 앱과 드라이버 설치 등의 기타 수정 사항을 반영

⑤ 보안 업데이트 KB3074679 설치 확인 및 미설치 시, 해당 KB 설치

⑥ CMD 명령 창을 띄운 후, 'slmgr /cpky' 입력, 실행

✓ 레지스트리에서 제품 키 지우기 및 공개 공격 방지 목적

⑦ 다음으로, 'sysprep /oobe /generalize /quit' 입력, 실행

⑧ 다음으로, 'reg add HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Setup₩OOBE /v SetupDisplayedProductKey /t REG_DWORD /d 1' 입력, 실행

⑨ CMD 명령 창을 종료하고, 타겟 장치 전원 끔

⑩ 옵션) 만약 대량 생산을 할 시, 해당 타겟 장치의 OS 이미지를 캡쳐 / 배포

OEM 의 고객이 장치를 부팅하면 (OEM 이 무인 설치 옵션으로 자동화 처리하지 않은 한) 그들은 OOBE 과정을 진행하게 됩니다. 참고로, OOBE 과정 중 제품 키 입력하는 단계는 표시되지 않습니다.

5. 정품인증 방법들

모든 Windows 10 IoT Enterprise 이미지는 정품인증을 위해 활성화되어야 합니다 (활성화 및 지연된 활성화 포함). 만약 장치가 인터넷에 절대로 연결되어 있지 않으면, 해당 장치는 지연된 활성화 (Deferred Activation) 상태로 남아 있습니다. 지연된 활성화 상태가 아닌, 이미지를 완전히 활성화하기로 결정한 경우, 이미지를 언제, 어떻게 활성화 할 것인지 결정하는 요소는 일반적으로 장치에서 사용할 수 있는 인터넷 연결의 종류와 최종 고객의 요구사항입니다.

Windows 10 IoT Enterprise 장치를 활성화 (정품인증) 하는 방법을 결정하는 첫 번째 요소는 장치에서 이용 가능한 인터넷 연결 유형을 확인하는 것입니다.

- 인터넷에 직접 연결할 것인지
- 프록시 도구를 이용하여 인터넷에 연결할 것인지
- 인터넷 연결을 하지 않을 것인지

5.1. 인터넷 직접 연결 시나리오

장치는 공용 네트워크에 접근할 수 있어서 Microsoft 정품인증 서버에 직접 연결하여 정품인증 프로세스를 완료할 수 있습니다. 해당 장치는 TCP 80 과 443 포트를 통해 정보를 주고받을 수 있어야 합니다.

5.2. 프록시 도구를 이용한 인터넷 연결 시나리오

장치는 개인 네트워크 (사설망) 에 접근할 수 있지만 인터넷에 직접 접근할 수는 없습니다.

이러한 경우에는 프록시 정품인증 도구를 사용하여 개인 네트워크 (사설망) 상의 장치와 공용 네트워크 상의 Microsoft 정품인증 서버 간의 정품인증 프로세스를 완료할 수 있습니다. 이 시나리오에서는 VAMT (Volume Activation Management Tool) 를 이용하여 장치를 활성화 할 수 있습니다. VAMT 기술 자료 링크

5.3. 인터넷 미연결 시나리오

장치에 네트워크 기능이 없거나, 공장이 인터넷에 연결되어 있지 않거나, 장치가 인터넷에 연결되어 있지 않은 개인 네트워크 (사설망) 에 연결되어 있거나, 혹은 보안상의 이유로 인터넷에 연결할 수 없는 경우 (프록시를 통한 간접적인 연결 조차도 안되는 경우) 와 같이 인터넷 연결을 할 수 없는 상황에서는 전화를 사용하여 장치를 활성화 할 수 있습니다. 이 시나리오에서는 Microsoft 제품 정품인증 센터에 전화 연결하여 장치를 활성화 할 수 있습니다. 또는, 장치를 지연된 활성화 상태로 두도록 선택할 수 있습니다. 전화 인증 센터 링크

■ **정품인증과 쓰기필터**

모든 활성화 진행 프로세스에는 장치의 쓰기필터가 비활성화되어 있어야 합니다. 만약 쓰기필터가 활성화되어 있으면 활성화가 성공된 것처럼 보이나, 장치를 재부팅하면 활성화 상태가 재설정되어 장치를 다시 활성화해야 합니다.

6. 정품인증 도구

6.1. Volume Activation Management Tool 3.1 (VAMT 3.1)

VAMT 3.1 를 사용하면 네트워크를 통해 Windows 10 IoT Enterprise 장치의 정품 인증 상태를 중앙에서 관리할 수 있습니다. 이 도구는 Windows ADK 안에 포함된 것으로 무료로 다운로드 받을 수 있습니다.

Windows ADK 다운로드 링크

VAMT 는 기본적으로 선택되어 있지 않아서, ADK 설치 시 수동으로 선택하여 설치해야 합니다. VAMT 를 사용하기 위해서는 Microsoft SQL Server 2008 또는 이후 버전의 데이터베이스가 필요합니다. VAMT 에 SQL Server 데이터베이스에 대한 연결이 필요하기 때문에 ADK 설치 시 SQL Server Express 2012 도 선택하여 설치해야 합니다. 그 외 다른 기능은 필요하지 않습니다.

VAMT 기술 자료 링크

6.2. Windows Software Licensing Management Tool (slmgr.vbs)

이 명령 줄 도구를 사용하면 Windows 10 IoT Enterprise 장치에서 제품 키 및 정품인증 상태를 관리할 수 있습니다. 이 도구는 모든 Windows 10 IoT Enterprise 운영체제에서 사용할 수 있습니다.

정품인증을 위한 slmgr.vbs 사용법

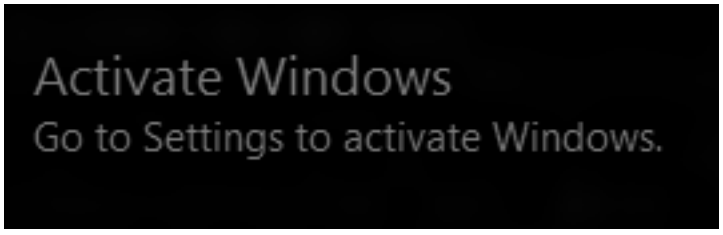
6.3. Windows Activation UI (slui.exe)

이 도구는 제품 키를 입력할 수 있는 윈도우 정품인증 UI 를 실행합니다. 이 도구는 모든 Windows 10 IoT Enterprise 운영체제에서 사용할 수 있습니다.

7. 정품 재인증

특정 사용 시나리오로 인해 장치를 다시 활성화 (정품 재인증) 해야하는 경우가 있습니다. 활성화된 장치가 변경될 시, 장치는 허용 오차 내 (in-tolerance) 또는 허용 오차 초과 (out-of-tolerance) 중 하나로 분류됩니다. 대부분의 경우, 장치를 다시 활성화하지 않고도 램을 추가하거나 하드디스크를 교체하는 등 하드웨어를 약간 변경할 수 있습니다. 하지만, 장치의 메인보드 변경과 같은 주요 하드웨어 변경으로 인해 장치가 허용 오차를 벗어난 것으로 간주되어 장치가 다시 활성화되지 않은 상태로 설정될 수 있습니다. 또한, 작은 하드웨어 변경을 한번에 많이 수행하면, 개별적인 하드웨어 변경 자체가 허용 오차 내에 속해 있을지라도 해당 장치가 허용 오차를 벗어날 수 있습니다. USB 장치 또는 기타 주변 장치들의 연결 및 분리는 장치의 허용 오차 상태에 영향을 미치지 않습니다.

Windows 10 IoT Enterprise 장치를 다시 활성화해야 하는 경우, 아래 그림과 같이 각 디스플레이 장치의 오른쪽 하단에 워터 마크가 표시되어 장치가 활성화되지 않았음을 표시합니다. 또한, 바탕 화면 배경 또는 잠금 화면 배경과 같은 Windows 개인 설정도 변경할 수 없습니다. 이 외 장치는 계속 정상 작동하며 장치 작동상 다른 변경 사항은 없습니다.



대부분의 경우, 이 가이드에서 설명한대로 새로운 장치를 활성화하는 것과 같은 방법으로 장치를 다시 활성화 할 수 있습니다. 사용한 제품 키 종류에 따라, 장치를 다시 활성화할 때의 제품 키 적용 의미가 다를 수 있습니다. ePKEA 키의 경우, 비록 장치의 하드웨어가 크게 변경되지 않는

경우, 동일한 장치를 여러 번 재활성화 하더라도 이미 활성화 된 키를 재사용해야 하지만, 이러한 경우라도 장치를 다시 활성화하면 사용 가능한 키 풀 중 하나가 사용될 수 있습니다.

7.1. 인터넷 직접 연결을 통한 Windows 10 IoT Enterprise 장치 활성화

대부분의 경우, 인터넷에 직접 연결된 Windows 10 IoT Enterprise 장치는 사용자 개입 없이 자동으로 활성화됩니다. 또한, 다음 절차를 사용하여 장치를 활성화 할 수도 있습니다.

- 인터넷에 직접 연결한 후 수동으로 장치 활성화
- VAMT 3.1 도구를 이용하여 인터넷을 통한 장치 활성화

7.1.1. 인터넷에 직접 연결한 후 수동으로 장치 활성화

만약 장치가 인터넷에 직접 연결되었다면, CMD 명령어 또는 윈도우 정품인증 UI 를 사용하여 수동으로 장치를 활성화 할 수 있습니다.

Windows 10 IoT Enterprise 는 정품인증 상태를 관리하기 위해 다음 두 가지 명령어 도구를 제공합니다.

- slmgr.vbs - Windows Software Licensing Management Tool 로 제품 키와 정품인증 상태 관리 가능
- slui.exe - 이 도구로 윈도우 정품인증 UI 를 실행 가능

7.1.2. 인터넷 직접 연결 및 CMD 명령어를 이용하여 수동으로 장치 활성화

✓ 준비사항

- ■ Windows 10 IoT Enterprise 가 설치된 장치
- ■ 해당 장치를 인터넷 직접 연결
- ■ 장치 사용 및 제어에 대한 관리자 권한 획득

✓ 정품인증 하려면

① 장치에서 관리자 권한으로 CMD 명령 창 실행

② <system drive>:₩Windows₩System32 폴더로 이동

③ cscript slmgr.vbs /ato 명령어 입력, 실행

④ cscript slmgr.vbs /dlv 명령어 입력, 실행

⑤ 'License Status' 항목에 '사용 허가됨 (Licensed)' 이라고 표시되는지 확인

7.1.3. 인터넷 직접 연결 및 윈도우 정품인증 UI를 이용하여 수동으로 장치 활성화

✓ 준비사항

- Windows 10 IoT Enterprise 가 설치된 장치
- 해당 장치를 인터넷 직접 연결
- 장치 사용 및 제어에 대한 관리자 권한 획득

✓ 정품인증 하려면

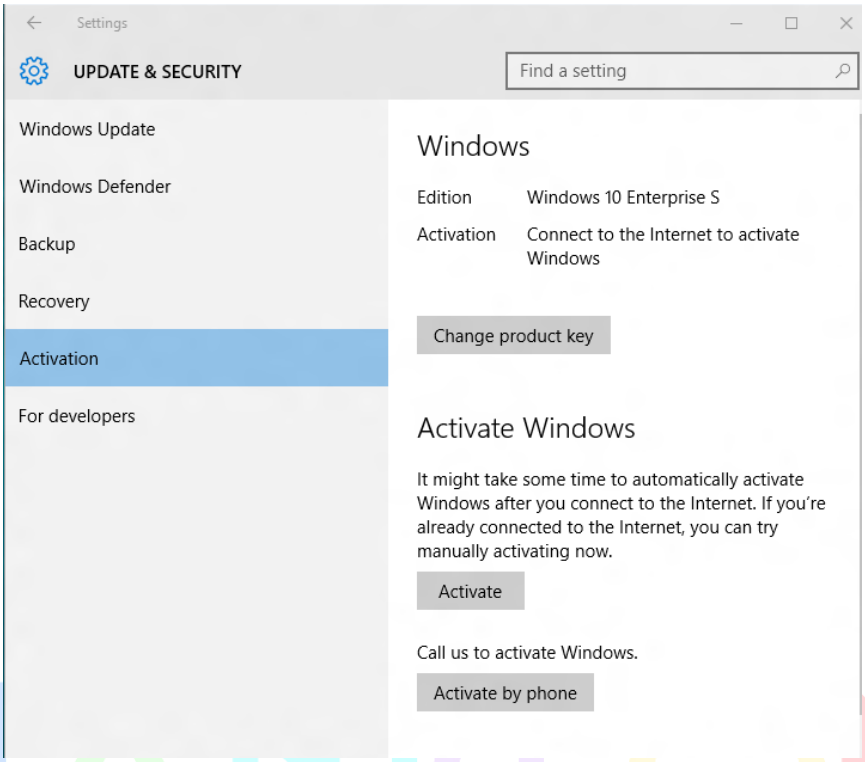
① 해당 장치에서, 다음 a, b 옵션 중 하나 실행

a. 관리자 권한으로 CMD 명령 창 실행한 다음, 윈도우즈 정품인증 UI 창을 실행하기 위해 'slui' 명령어 입력, 실행

b. Windows 10 의 'Setting' 메뉴 실행한 다음, 'Update & Security' 항목으로 이동, 'Activation' 항목 이동 후, 'Activate' 버튼 클릭

② 잠시 후, 해당 장치의 정품인증이 완료됨

HANCOM 한컴MDS



7.1.4. OS 설치 후 인터넷 직접 연결을 이용하여 자동으로 장치 활성화

기본적으로, Windows 10 IoT Enterprise 장치는 처음 인터넷에 연결될 때 자동으로 활성화 됩니다.

✓ 준비사항

- ■ 장치를 인터넷에 직접 연결
- ■ 유효한 제품 키가 적용된 마스터 OS 이미지
- ■ 마스터 및 참조 이미지에 대한 관리자 권한 획득

✓ 정품인증 하려면

장치는 인터넷에 연결될 때 자동으로 활성화가 됩니다. 그러나, 만약 특정한 시간에 정품인증이 진행되도록 하려면, 다음 방법들을 사용해야 합니다.

① 마스터 혹은 참조 장치에서, 관리자 권한으로 CMD 명령 창 실행

② 자동 정품인증을 활성화하기 위한 레지스트리 키 값 추가 명령어 입력, 실행

reg add HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Runonce₩ /v autoactivate /t REG_SZ /d "<system drive>:₩Windows₩System32₩slmgr.vbs /ato"

③ CMD 명령 창에서, '%systemdrive%₩Windows₩System32₩Sysprep' 폴더로 이동

한 다음, 'sysprep /generalize' 명령어를 입력, 실행하여 OS 이미지 일반화 작업을 진행

④ 생산 및 제조를 위해 '일반화된 (syspreped)' OS 이미지를 배포

참고로, 이 OS 이미지가 장치에 배포되고 장치가 처음으로 구동될 때, 인터넷 연결이 되어 있다면 그 장치는 자동으로 정품인증을 시도합니다.

7.2. VAMT 3.1 도구를 이용하여 인터넷을 통한 장치 활성화

장치에 디스플레이 장치나 사용자 입력 방법이 없을 경우, 혹은 네트워크 상에 많은 수의 장치가 있고 원격으로 그 장치들을 활성화 (정품인증) 하기를 원하는 경우, Volume Activation Management Tool 3.1 (VAMT 3.1) 도구를 사용하여 네트워크 상의 장치를 원격으로 활성화 할 수 있습니다. 이 도구는 Microsoft 에서 무료로 배포합니다.

7.2.1. VAMT 3.1 를 사용하여 인터넷을 통한 장치 활성화

✓ 준비사항

■ VAMT 3.1 호스트 준비

- VAMT 3.1 도구 설치
- VAMT 3.1 호스트를 인터넷에 연결
- VAMT 3.1 호스트를 개인 네트워크 (사설망) 에 연결

■ Windows PowerShell 4.0 설치

■ 활성화 (정품인증) 할 장치 준비

- WMI/PowerShell 원격 접근 설정

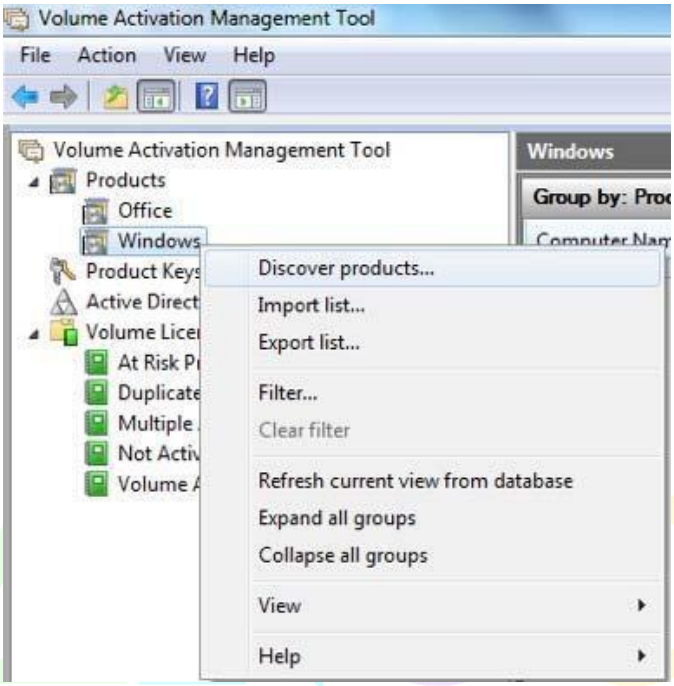
  https://msdn.microsoft.com/en-us/library/jj980508%28v=winembedded.81%29.aspx

- 개인 네트워크 (사설망) 에 연결
- 외부 인터넷 망에 직접 연결
- 암호 설정된 관리자 계정

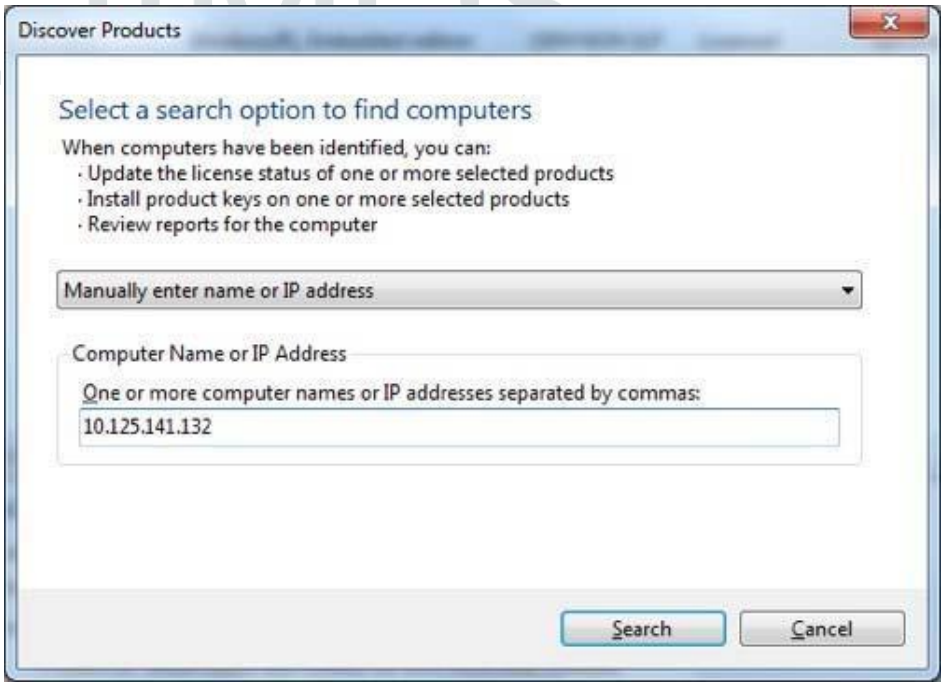
✓ 정품인증 하려면

① VAMT 3.1 호스트에서 VAMT 3.1 실행

② 왼쪽 패널에서 'Products' 노드 확장 후, 'Windows' 항목에서 마우스 우클릭한 메뉴에서 'Discover products' 항목 클릭

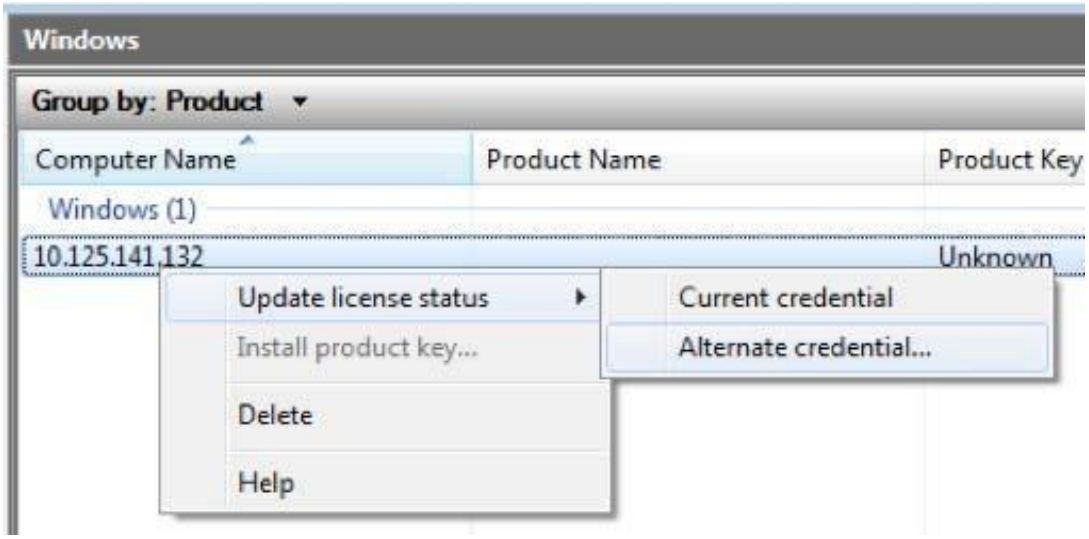


③ 실행된 'Discover Products' 창에서 'Manually enter name or IP address' 항목 선택한 다음, 활성화할 장치의 이름 혹은 IP 주소를 입력



④ VAMT 3.1 에서 성공적으로 해당 장치를 찾으면, 가운데 패널에 장치가 표시됨

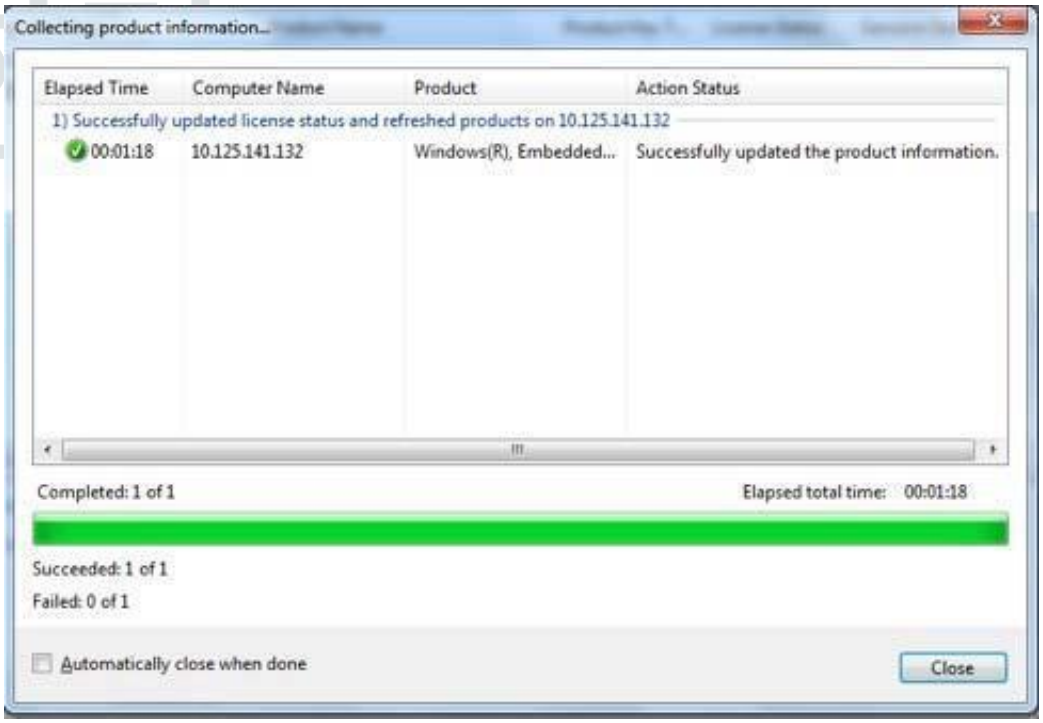
⑤ 찾은 장치에서 마우스 우클릭한 메뉴에서 'Update license status' 클릭한 다음, 'Alternate credential' 항목 클릭



⑥ 실행된 'Windows Security' 창에서 장치에 대한 관리자 권한을 가진 사용자 이름과 암호를 입력한 다음, 'OK' 클릭

※ 관리자 계정에는 반드시 암호가 설정되어 있어야 함

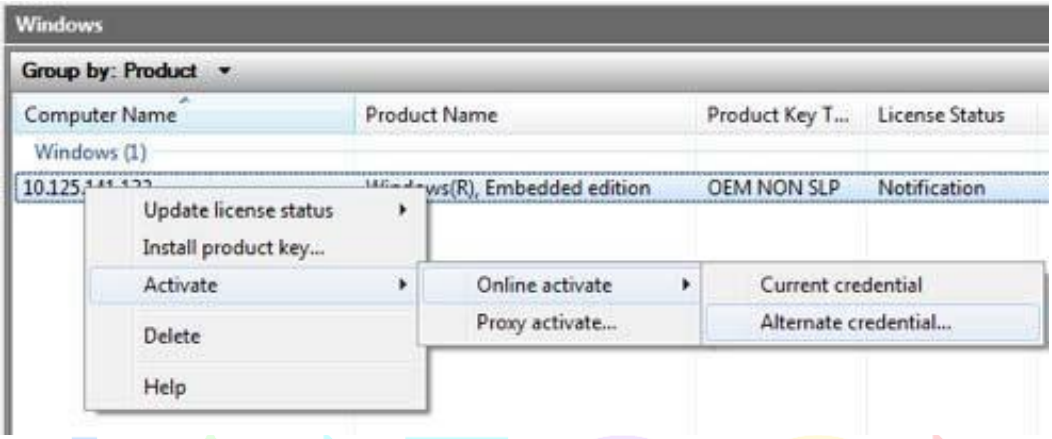
⑦ 장치 정보를 업데이트하는 진행 표시 창이 실행됨 (수분 소요)



⑧ 진행이 완료되면 'Close' 버튼 클릭

⑨ VAMT 3.1 의 가운데 패널에 해당 장치의 'License Status' 값이 'Notification' 으로 표시됨

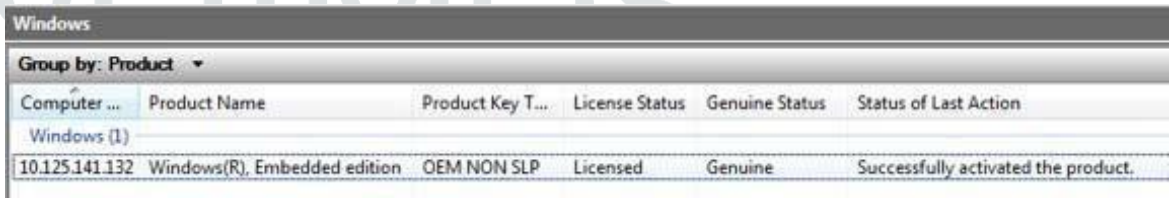
⑩ 가운데 패널의 검색된 장치에서 마우스 우클릭한 메뉴에서 'Activate', 'Online activate', 'Alternate credential' 를 차례대로 클릭



⑪ Windows Security 창에서, 장치에 대한 관리자 권한을 가진 사용자 이름과 암호를 입력한 다음, 'OK' 클릭

⑫ 인터넷을 통해 장치를 활성화하기 위한 VAMT 3.1 의 진행 상태가 표시되는 창이 실행됨

⑬ 몇 분 후 장치가 활성화되고 'License Status' 상태 값이 'Licensed' 로 변경됨



7.3. 인터넷에 대한 프록시 연결을 이용하여 Windows 10 IoT Enterprise 장치 활성화

만약 장치가 개인 네트워크 (사설망) 에 연결되어 있고, 인터넷망에 직접 접근할 수 없는 경우, 해당 장치와 인터넷 간의 중개자 역할을 하는 프록시 서버를 사용할 수 있습니다. 프록시 서버는 개인 네트워크 (사설망) 와 인터넷 망 사이의 다리 역할을 하며, 장치가 Microsoft 정품 인증 서버와 간접적으로 통신할 수 있게 합니다.

프록시 서버를 사용하여 네트워크를 통해 Windows 10 IoT Enterprise 장치를 활성화 (정품 인증) 할 수 있는 도구는 VAMT 3.1 (Volume Activation Management Tool 3.1) 입니다. 이 도구는 Microsoft 에서 무료로 배포합니다.

7.3.1. 프록시 컴퓨터에서 VAMT 3.1 를 사용하여 개인 네트워크 (사설망) 를 통해 장치 활성화

✓ 장치 활성화 진행 프로세스

① VAMT 3.1 이 설치되어 있고 인터넷에 연결된 프록시 컴퓨터를 Windows 10 IoT Enterprise 장치가 있는 개인 네트워크 (사설망) 에 연결

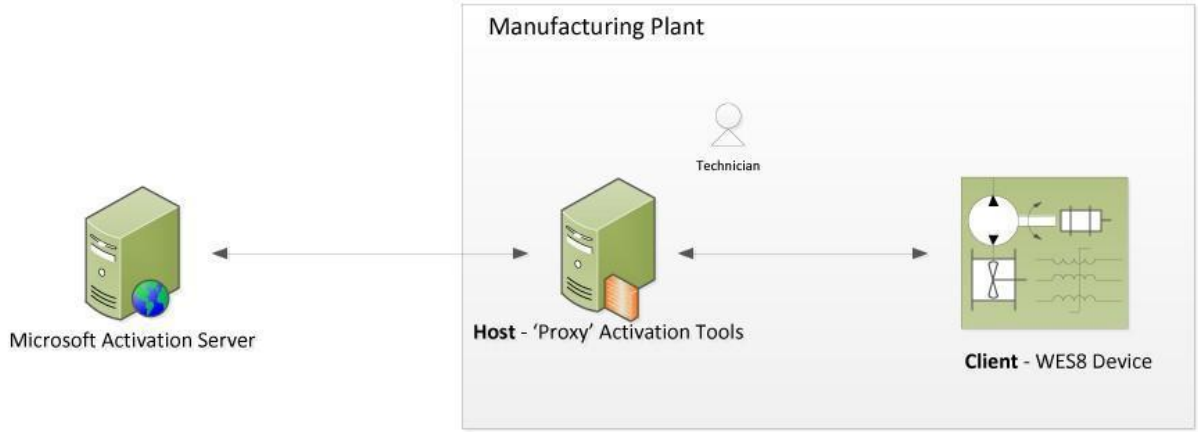
② VAMT 3.1 을 사용하여 장치를 검색하고 장치 정보를 VAMT 3.1 호스트의 데이터베이스에 추가

③ VAMT 3.1 호스트는 인터넷을 통해 Microsoft 정품 인증 서버에 연결하고 장치의 라이선스 정보를 전송

④ Microsoft 정품 인증 서버는 VAMT 3.1 호스트로 장치의 'Confirmation ID (CID)' 값을 반환

⑤ VAMT 3.1 호스트는 장치에 해당 'Confirmation ID (CID)' 를 적용하여 장치를 활성화

위 프로세스는 하나의 장치 단위로 수행할 수 있지만, 자동화 또는 다수의 장치에서의 활성화가 가능하도록 스크립트 처리도 가능합니다.



7.3.2. VAMT 3.1을 사용하여 개인 네트워크 (사설망) 를 통해 개별 장치 활성화

✓ 준비사항

■ VAMT 3.1 호스트 준비

• VAMT 3.1 도구 설치

- SQL Server 데이터베이스 설치
- VAMT 3.1 호스트를 인터넷에 연결
- VAMT 3.1 호스트를 개인 네트워크 (사설망) 에 연결
- TCP 80 과 443 포트 접근 허용

■ 활성화 (정품인증) 할 장치 준비

- WMI/PowerShell 원격 접근 설정

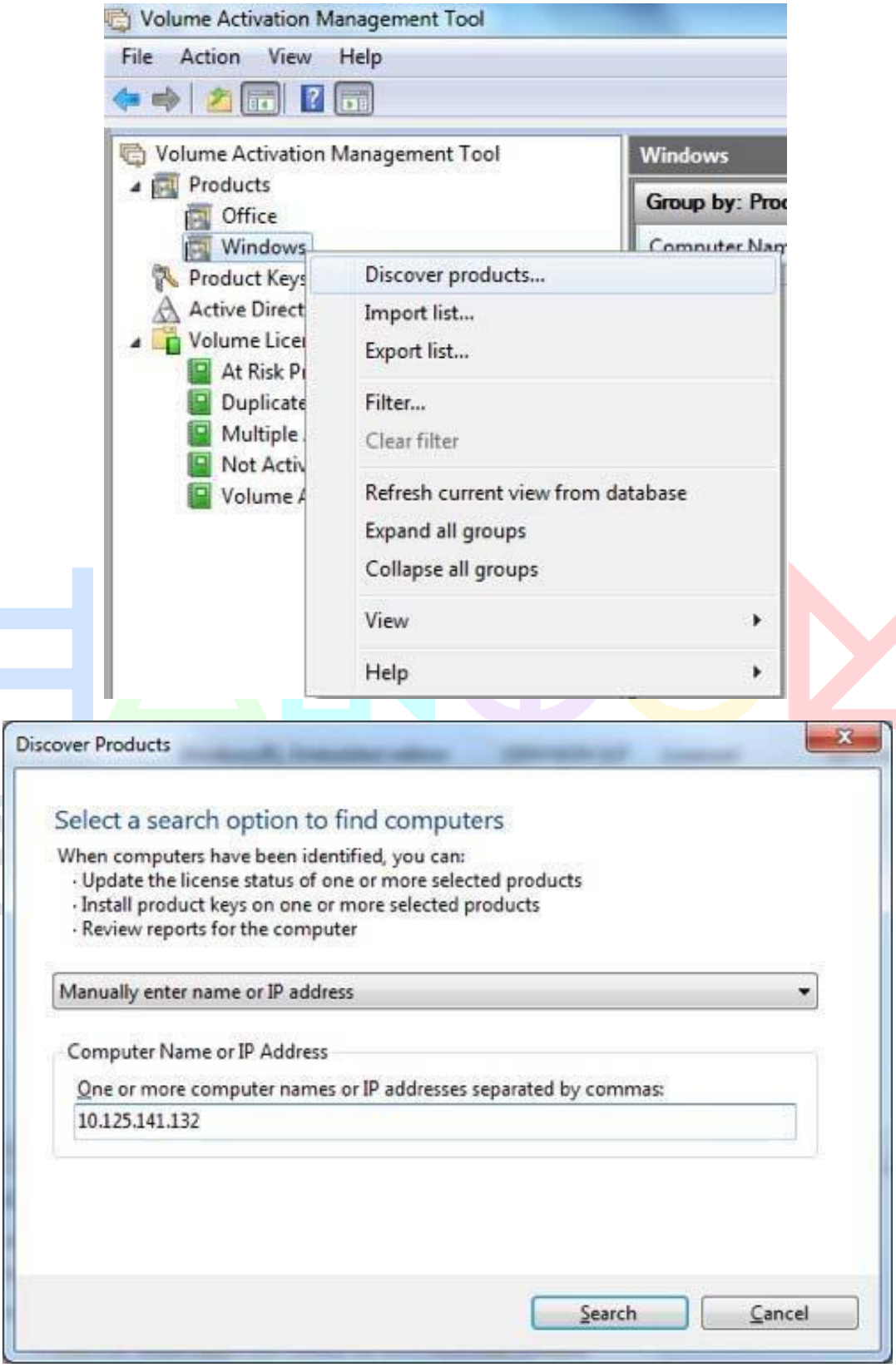
  https://msdn.microsoft.com/en-us/library/jj980508%28v=winembedded.81%29.aspx
- 개인 네트워크 (사설망) 에 연결
- 암호 설정된 관리자 계정

✓ 정품인증 하려면

① VAMT 3.1 호스트에서 VAMT 3.1 실행

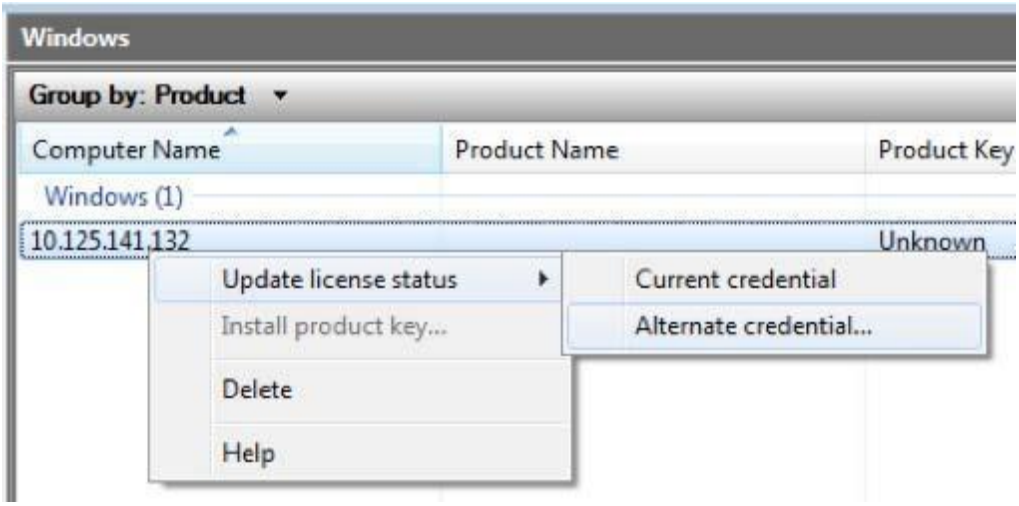
② 왼쪽 패널에서 'Products' 노드 확장, 'Windows' 항목에서 마우스 우클릭한 메뉴에서 'Discover Products' 항목 클릭

③ 'Discover Product' 창에서, 'Manually enter name or IP Address' 항목 선택하고, 활성화 (정품인증) 할 장치의 컴퓨터 이름 혹은 IP 주소 입력



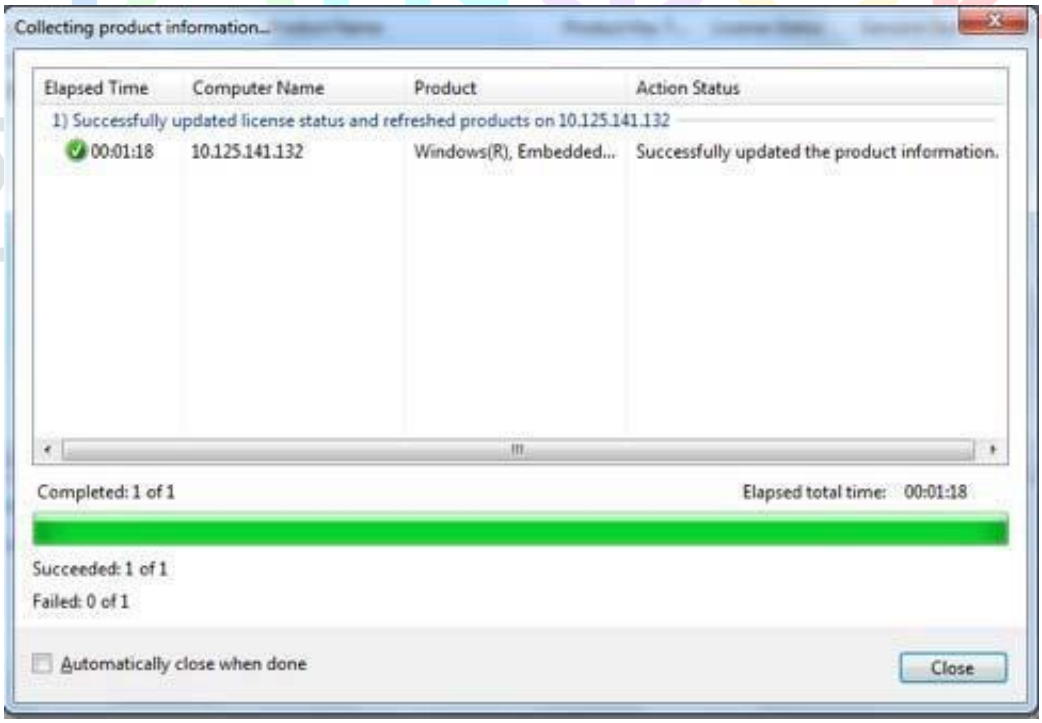
④ VAMT 3.1 에서 성공적으로 해당 장치를 찾으면, 가운데 패널에 장치가 표시됨

⑤ 가운데 패널의 검색된 장치에서 마우스 우클릭한 메뉴에서 'Update license status', 'Alternate credential' 를 차례대로 클릭



⑥ Windows Security 창에서, 장치에 대한 관리자 권한을 가진 사용자 이름과 암호를 입력한 다음, 'OK' 클릭

⑦ 장치 정보를 업데이트하는 진행 표시 창이 실행됨 (수분 소요)



⑧ 정보 업데이트 진행이 완료되면, 'Close' 클릭. 해당 장치에 대한 'License Status' 항목에 'Notification' 값이 표시

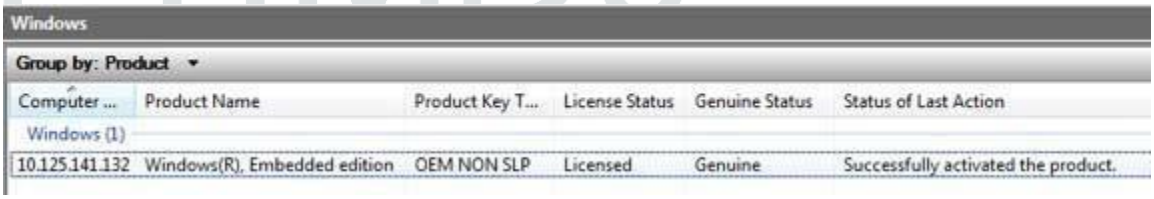
⑨ 가운데 패널의 장치에서 마우스 우클릭한 메뉴에서 'Activate', 'Proxy Activate' 를 차례

대로 클릭

⑩ 'Proxy Activate' 창에서, 'Acquire confirmation ID, apply to selected machine(s) and activate' 항목 선택, 'Use Alternate Credentials when applying confirmation ID' 항목 체크 후, 'OK' 클릭

⑪ Windows Security 창에서, 장치에 대한 관리자 권한을 가진 사용자 이름과 암호를 입력한 다음, 'OK' 클릭

⑫ 인터넷을 통해 장치를 활성화하기 위한 VAMT 3.1 의 진행 상태가 표시되는 창이 실행됨. 몇 분 후 장치가 활성화되고 'License Status' 상태 값이 'Licensed' 라고 변경됨



7.3.3. VAMT 3.1을 사용하여 개인 네트워크 (사설망) 를 통해 배치 파일로 다수의 장치 활성화

Windows 10 IoT Enterprise 는 다수의 활성화 (정품인증) 작업을 자동화하는 데 사용할 수 있는 Windows PowerShell 명령줄 인터페이스 스크립트와 두 개의 관련 파일을 제공합니다. 이 스크립트를 사용하면 주기적으로 활성화 스크립트를 실행하고 장치를 활성화하는 예약된 작업을 만들 수 있습니다.

이 파일들은 %systemdrive%₩Windows Embedded Standard 8₩Toolset₩Activation 폴더에 저장되어 있습니다.

- activationHelper.ps1 : Windows PowerShell 스크립트 파일
- Config.xml : 구성 파일
- Config.xsd : 구성 스키마 파일

✓ activationHelper.ps1 스크립트 실행 과정

① Windows PowerShell 로 VAMT 모듈 가져오기

② 장치의 IP 주소/이름 정보를 가져오기 위해 Config.xml 파일 구문 분석 후 장치 목록 생성

③ 장치 이름과 IP 주소를 지정하여 장치를 VAMT DB 에 장치 추가 (백그라운드 작업으로 진행됨)

④ Microsoft AVS 로 장치의 라이선스 정보 전달 (백그라운드 작업으로 진행됨)

⑤ AVS 로부터 장치에 대한 configuration ID 부여 받음 (백그라운드 작업으로 진행됨)

⑥ 장치에 configuration ID 적용 (백그라운드 작업으로 진행됨)

⑦ 구성 파일에 플래그가 설정된 경우, UWF (Unified Write Filter) 활성화

⑧ 구성 파일에 플래그가 설정된 경우, 장치 전원 종료

✓ 준비사항

■ VAMT 3.1 호스트 준비

- VAMT 3.1 도구 설치
- SQL Server 데이터베이스 설치
- VAMT 3.1 호스트를 인터넷에 연결
- VAMT 3.1 호스트를 개인 네트워크 (사설망) 에 연결
- Standard 8 Toolkit 에서 활성화 (정품인증) 스크립트 파일을 VAMT 3.1 호스트에 복사하고 사용자 환경에 맞게 구성
- Windows PowerShell 4.0 설치
- TCP 80 과 443 포트 접근 허용

■ 활성화 (정품인증) 할 장치 준비

- WMI/PowerShell 원격 접근 설정

  https://msdn.microsoft.com/en-us/library/jj980508%28v=winembedded.81%29.aspx

■ 개인 네트워크 (사설망) 에 연결

■ 암호 설정된 관리자 계정

✓ 정품인증 하려면

주기적인 활성화 프로세스를 설정하기 전에, 사용자 환경에 대한 활성화 스크립트의 구성 파일을 수정해야 합니다. 다음은 Config.xml 구성 스크립트의 샘플입니다.

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
    <Vamt
        InstallLocation="C:\Program Files (x86)\Windows Kits\8.0\Assessment and
Deployment Kit\VAMT 3.0"
        maxThreads="3"
        checkConnectivity="false"
    />
   <Machineidentity
        Prefix="192.168.0."
        Start="100"
        End="105"
    />
    <UserAccount
        UseAlternateCredential="true"
        Username="john"
        Password="1234"
    />
    <PostActivationTasks
        EnableUWF="false"
        ShutDownMachine="Shutdown"
    />
    <LogInfo
         Level="ErrorOnly"
         Logfile="script.log"
    />
</Configurations>
```

주기적인 활성화 프로세스에서 사용되는 설정 사항은 다음 표에 자세하게 설명되어 있습니다. ※ 각 요소와 속성 이름은 대, 소문자를 구분합니다.

Element/Attribute	Description	Schema
VAMT	설치 경로, 최대 스레드 수, 연결 플레그 확인 등이 포함된 VAMT 3.1 관련 정보 지정	<xs:complexType name="vamtInfo"> <xs:annotation> <xs:documentation>VAMT infomation</xs:documentation> </xs:annotation> <xs:attributename="InstallLocation"use="required"type="xs:string"/> </xs:complexType>
maxthreads	백그라운드로 구동되는 최대 스레드 지정	<xs:simpleType name="smallInteger"> <xs:restriction base="xs:nonNegativeInteger"> <xs:maxInclusive value="100"/> <xs:minInclusive value="1"/> </xs:restriction> </xs:simpleType>
checkConnectivity	전체 목록을 직접 VAMT로 전달하는 것 대신에, 먼저 연결을 확인하기 위해 컴퓨터를 toping 할지 여부를 지정. 클라이언트 장치	<xs:attributename="checkConnectivity"use="optional"type="xs:boolean" default="false"/>

	는 Ping 동작을 위해 네트워크 검색 활성화 필요	
machineIdentity	장치 ID를 생성하는데 사용할 요소를 지정. 규칙은 Prefix + index [index 는 Start 에서 End]. 이 샘플에서는 IP 주소를 Prefix 문자열로 사용; "MS-machine"과 같은 컴퓨터 이름으로 쉽게 변경 가능	<xs:complexType name="MachineIdentityInfo"> <xs:annotation> <xs:documentation>Machine discovery phase to generate machine list, MachineNameis{Prefix+[Start..End]}</xs:documentation> </xs:annotation> <xs:attributename="Prefix"use="required"type="xs:string"/> <xs:attributename="Start"use="required"type="xs:int"/> <xs:attributename="End"use="required"type="xs:int"/> </xs:complexType>
UserAccount	대체 자격 증명이 필요한지 여부를 지정: 만약 그렇다면, 사용자이름과 암호를 지정; 만약 그렇지 않다면, 스크립트 내부의 모든 작업은 현재 자격 증명을 사용	<xs:complexType name="useraccountInfo"> <xs:annotation> <xs:documentation>Needed to perform remote operation</xs:documentation> </xs:annotation> <xs:attributename="UseAlternateCredential"use="required" type="xs:boolean"/> <xs:attributename="Username"type="xs:string"/> <xs:attribute name="Password" type="xs:string"/> </xs:complexType>
EnableUWF	정품인증을 완료한 후에 타깃 장비에서 UWF 기능을 활성화 할지 여부 지정	<xs:attributename="EnableUWF"use="optional"type="xs:boolean" default="false"/>
Shutdowntype	정품인증 후의 작업 지정. Reboot / Shut down / Log off / Power off / Do nothing	<xs:simpleType name="shutdownType"> <xs:annotation> <xs:documentation>Post-activationphasetoperformshudown operation</xs:documentation> </xs:annotation> <xs:restriction base="xs:string"> <xs:enumerationvalue="NO"/> <xs:enumerationvalue="LogOff"/> <xs:enumerationvalue="Shutdown"/> <xs:enumerationvalue="Reboot"/> <xs:enumerationvalue="PowerOff"/> </xs:restriction> </xs:simpleType>
LogInfo	로그 레벨과 파일 저장위치 지정	<xs:simpletype name="loglevelType"> <xs:annotation> <xs:documentation>Tospecifytheloglevel</xs:documentation> </xs:annotation> <xs:restriction base="xs:string"> <xs:enumerationvalue="NoLog"/> <xs:enumerationvalue="ErrorOnly"/> <xs:enumeration value="Info" /> </xs:restriction> </xs:simpleType>

구성 파일을 설정하고 Config.xml 로 저장 한 후, 다음 절차에 따라 예약된 작업을 설정할 수 있습니다.

✓ VAMT 3.1 호스트에서 %path% 시스템 변수에 스크립트 파일의 위치를 추가

① VAMT 3.1 호스트에서 'Task Scheduler' 실행

- Windows 10 에서 'Control Panel' - 'System and Security' - 'Administrator Tools' - 'Task Scheduler' 를 실행

② 'Task Scheduler' 에서 'Action' 클릭 후, 'Create a basic task' 클릭

③ 'Create a basic task wizard' 에서, 작업 이름과 설명 기입 후, 'Next' 클릭

④ 'Task Trigger' 페이지에서 'Next' 클릭

⑤ 'Daily' 페이지에서 'Next' 클릭

⑥ 'Action' 페이지에서 'Start a Program' 선택 후 'Next' 클릭

⑦ 'Start a Program' 페이지에서 'Program/script box' 항목에 'powershell.exe' 파일의 전체 경로 입력

※ VAMT 3.1 요구 사항으로, x86 버전의 Windows PowerShell 에서 이 스크립트를 실행해야 함. 만약 x64 기반 시스템에서 이 스크립트를 실행하는 경우, x86 버전의 Windows PowerShell 응용 프로그램의 기본 경로는 다음과 같습니다.

%SystemRoot%₩syswow64₩WindowsPowerShell₩v1.0₩powershell.exe

⑧ 'Add Arguments' 상자에서 '–File parameter' 를 사용하는 스크립트 위치와 'activationHelper.ps1' 파일의 전체 경로를 입력 후 'Next' 클릭

⑨ 'Summary' 페이지에서, 'Open the properties dialog for this task when I click finish' 선택 후, 'Finish' 클릭

⑩ 'Properties' 창에서

a. 'General' 탭에서 'Run with highest privileges' 항목 선택

b. 'Conditions' 탭에서 'Start the task only if the computer is idle' 항목 선택 해제

c. 'Conditions' 탭에서 'Start the task only if the computer is on AC power' 항목 선택 해제

⑪ 'OK' 클릭하여 작업 예약을 완료

7.4. 전화를 이용하여 Windows 10 IoT Enterprise 장치 활성화

Windows 10 IoT Enterprise 장치가 인터넷에 연결되어 있지 않거나 해당 장치를 직접 또는 개인 네트워크 (사설망) 의 프록시 연결을 통해 인터넷에 연결할 수 없는 경우, 장치를 활성화 (정품인증) 하기 위해 전화 연결 및 Software Licensing Management Tool (SLMGR) 명령줄 도구를 사용해야 합니다. 또는 장치를 지연된 활성화 (Deferred Activation) 상태로 놔둘 수 있습니다.

만약 장치가 인터넷에 연결되어 있지만, 전화 정품 인증을 계속 사용하고 싶은 경우, SLMGR 또는 윈도우 정품 인증 UI (SLUI)를 사용할 수 있습니다.

7.4.1. 전화 연결을 통한 장치 정품 인증

Microsoft 정품 인증 센터로 전화를 걸어 장치를 활성화 (정품인증) 할 수 있습니다. 사용자 정보와 63자리 설치 ID를 제공하면 Microsoft 정품 인증 센터로부터 48자리 Confirmation ID (CID) 를 받게 됩니다.

그런 다음 해당 장치에 Confirmation ID (CID) 를 입력한 다음 SLMGR 또는 SLUI 를 사용하여 장치를 활성화 (정품인증) 해야 합니다. SLUI 를 사용하려면 반드시 장치가 인터넷에 연결되어 있어야 합니다.

- 전화 및 SLMGR 를 사용하여 장치 활성화
- 전화 및 SLUI 를 사용하여 장치 활성화

7.4.1.1. 전화 및 slmgr 를 사용하여 장치 활성화

✓ 준비사항

■ 전화

■ Windows 10 IoT Enterprise 가 설치된 장치

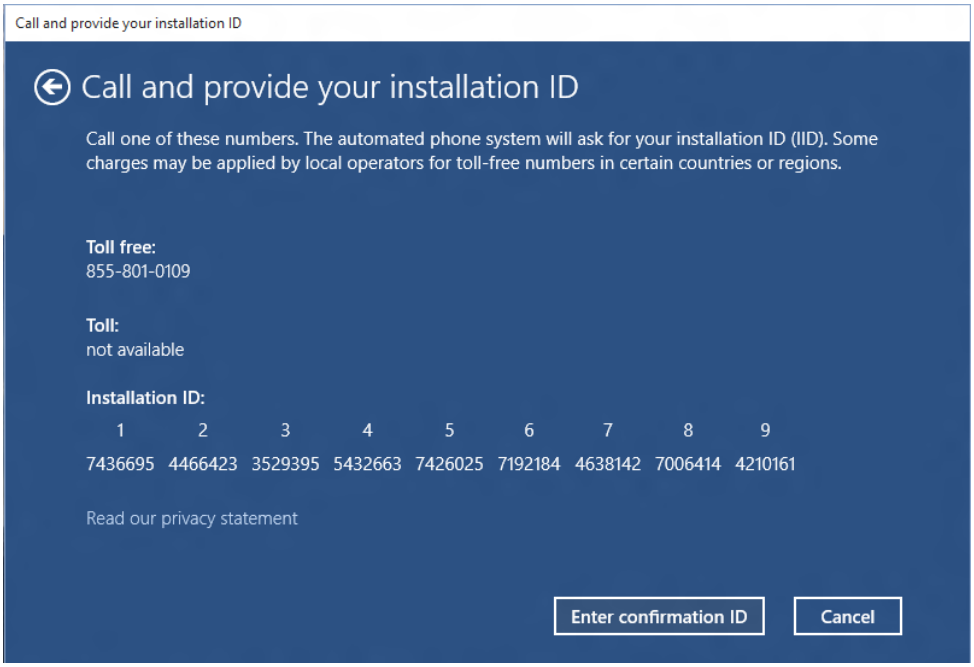
■ 장치에 대한 관리자 권한 획득

✓ 정품인증 하려면

① 해당 장치에서 관리자 권한으로 CMD 명령어 창 실행

② '<system drive>:₩Windows₩System32' 폴더로 이동 후, 'cscript slmgr.vbs /dti' 입력, 실행

③ 63자리 'Installation ID' 별도 기록



④ 소속된 국가의 Microsoft 정품 인증 센터로 전화

- 국가별 정품인증 센터 전화 번호

  https://www.microsoft.com/en-us/licensing/existing-customer/activation-centers.aspx

⑤ 자동 지침을 따라서 이전에 기록한 63자리 'Installation ID' 를 입력

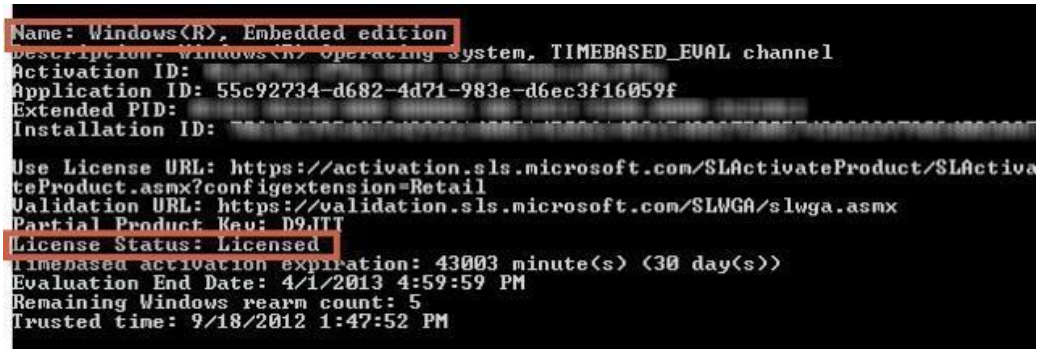
⑥ 전화 정품인증 시스템에서 제공하는 'confirmation ID (CID)' 기록

⑦ 장치에서 CMD 명령 창을 실행한 다음, 다음 명령어 입력, 실행

여기서 <confirmation ID> 는 전화 정품인증 시스템으로부터 제공받은 CID 임

- cscript slmgr.vbs /atp <confirmation ID>

⑧ 'cscript slmgr.vbs /dlv' 입력 후, 'License Status' 항목에 'Licensed' 라고 표시되어 있는지 확인



※ 각 장치는 별도로 활성화해야 합니다. 일괄 배치 활성화는 지원되지 않습니다.

7.4.1.2. 전화 및 SLUI 를 사용하여 장치 활성화

✓ 준비사항

- 전화
- Windows 10 IoT Enterprise 가 설치된 장치
- Windows Security Center 모듈 (Features > Security)
- Telephony API Client (Features > Application Development Frameworks > Legacy Support)
- 장치에 대한 관리자 권한 획득

✓ 정품인증 하려면

① 해당 장치에서 관리자 권한으로 CMD 명령어 창 실행한 다음, 'SLUI 4' 명령어 실행

※ 4 옵션은 전화 정품인증 UI 를 실행시키는 SLUI 서브 옵션

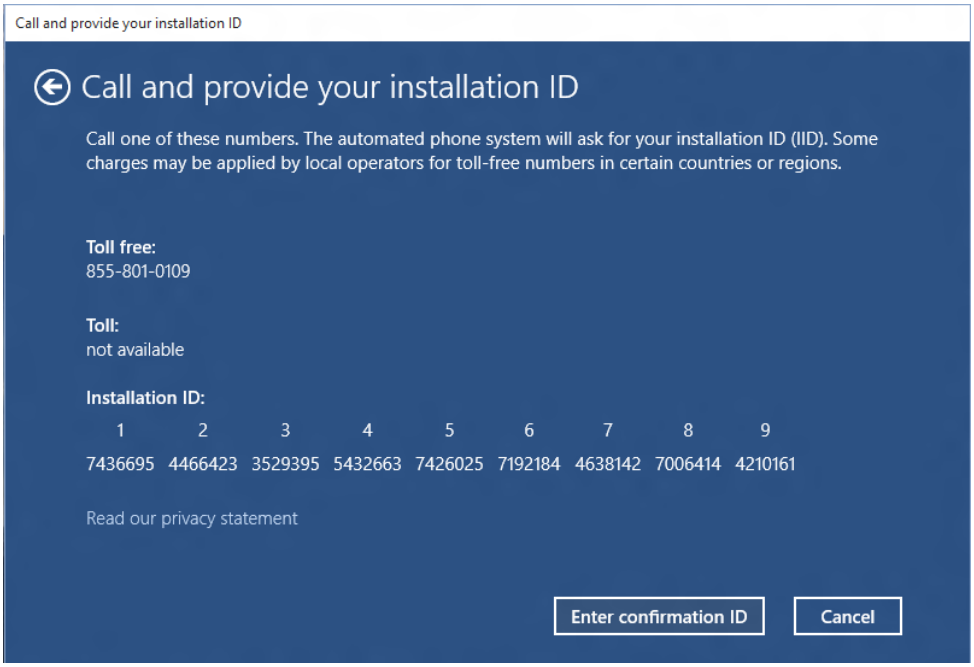
② Windows Activation 도구의 'Click the nearest location' 페이지에서 'Next' 를 클릭

③ 소속된 국가의 Microsoft 정품 인증 센터로 전화

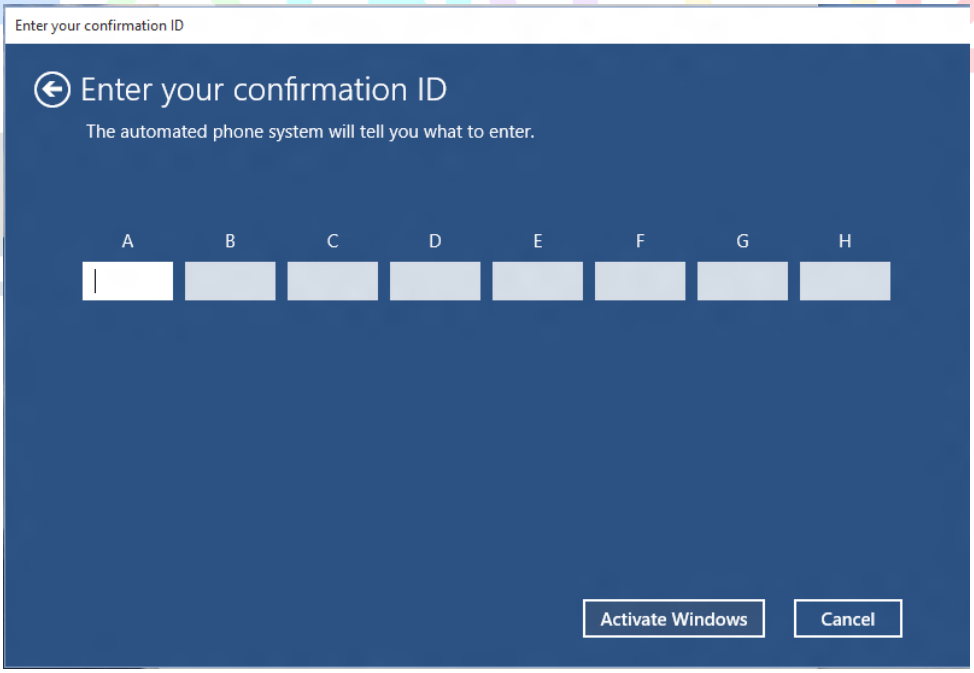
- 국가별 정품 인증 센터 전화 번호

  https://www.microsoft.com/en-us/licensing/existing-customer/activation-centers.aspx

④ 자동 지침을 따라서 63자리 'Installation ID' 를 입력

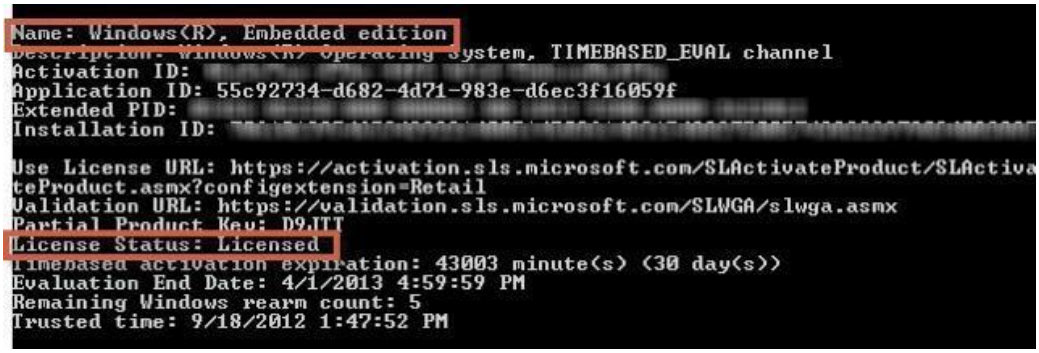


⑤ 전화 정품인증 시스템에서 제공하는 'confirmation ID (CID)' 입력 후, 'Activate Windows' 클릭



⑥ 라이선스 상태를 확인하기 위해, 해당 장치에서 관리자 권한으로 CMD 명령 창 실행

⑦ '<system drive:>₩Windows₩System32' 폴더로 이동 후, 'cscript slmgr.vbs /dlv' 입력 후, 'License Status' 항목이 'Licensed' 라고 표시되어 있는지 확인



끝.

한컴 MDS

Windows IoT 총판 | https://www.hancommds.com/windowsiot

영업 문의: essales@hancommds.com

기술 지원 문의: essupport@hancommds.com

© 2015 Microsoft Corporation. 판권 소유.

이 문서는 Microsoft 로부터 제공받은 영문 문서를 번역한 것으로, 문서 출처 및 판권은 Microsoft 에 있습니다. 문서에 나와 있는 URL 및 기타 인터넷 웹 사이트 주소, 정보와 견해는 참조용으로 예고 없이 변경 될 수 있습니다. 또한, 일부 예제는 설명용으로 실제와 상이할 수 있습니다.

이 문서는 Microsoft 제품의 지적 재산권에 대한 법적 권리를 제공하지 않습니다. 내부 참조용으로 이 문서를 복사하여 사용할 수 있으며, 이 문서는 Microsoft 의 기밀이며 독점권이 있습니다.