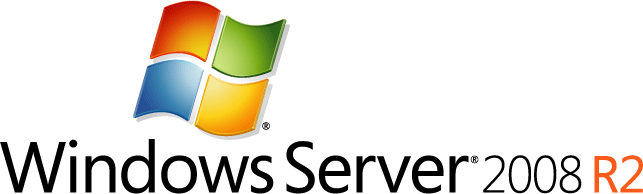
****

**  
  
볼륨 정품 인증 기술 참조 가이드**

**Windows 7 및 Windows Server 2008 R2**

Microsoft Corporation

게시일: 2009년 7월

요약

이 참조 가이드는 Windows® 7 및 Windows Server® 2008 R2 운영 체제의 정품 인증 버전을 배포하려는 조직의 IT(정보 기술) 구현 전문가를 위한 것입니다. 이 가이드는 *볼륨 정품 인증 계획 가이드*, *볼륨 정품 인증 배포 가이드* 및 *볼륨 정품 인증 운영 가이드*의 자매 안내서입니다.

이 문서와 여기에서 참조하는 모든 문서는 정보 제공만을 목적으로 하며 Microsoft는 이 문서에 있는 내용에 대해 어떠한 명시적 또는 암시적 보증도 하지 않습니다. URL 및 기타 인터넷 웹 사이트 참조를 포함하여 본 문서의 정보는 사전 통지 없이 변경될 수 있습니다. 이 문서를 사용하여 생기는 위험성이나 결과는 전적으로 사용자가 책임을 집니다. 특별한 언급이 없는 경우, 본 문서에서 예시하는 회사, 조직, 제품, 도메인 이름, 전자 메일 주소, 로고, 사람, 장소 및 이벤트는 가상으로 만들어진 것입니다. 실제 회사, 조직, 제품, 도메인 이름, 전자 메일 주소, 로고, 사람, 장소 또는 이벤트와 연관시키려는 어떠한 의도도 없으며 그렇게 해석되지 않아야 합니다. 해당하는 모든 저작권 법률을 준수하는 것은 사용자의 책임입니다. 저작권에 의해 주어지는 권리를 제한하지 않고 본 문서의 어떤 부분도 Microsoft Corporation의 명시적 서면 허가 없이는 어떠한 형태나 수단(전자, 기계, 복사, 기록 등) 또는 목적으로도 재생하거나 검색 시스템에 저장 또는 전송할 수 없습니다.

Microsoft는 본 문서에서 다루는 제품이나 서비스에 대해 특허, 특허 출원, 상표, 저작권 또는 기타 지적 재산권을 가지고 있을 수 있습니다. Microsoft와 체결한 서면 라이선스 계약서에 명시된 경우를 제외하면 본 문서를 제공한다고 해서 이러한 특허, 상표, 저작권 또는 기타 지적 재산권에 대한 라이선스가 부여되는 것은 아닙니다.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Hyper-V, Windows, Windows Server 및 Windows Vista는 Microsoft 그룹의 상표입니다.

본 문서에 언급된 실제 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

**목차**

[소개 1](#_Toc237188706)

[설치 환경 2](#_Toc237188707)

[Slmgr.vbs 옵션 5](#_Toc237188708)

[레지스트리 설정 11](#_Toc237188709)

[GPO(그룹 정책 개체) 설정 14](#_Toc237188710)

[KMS 정품 인증 시기 16](#_Toc237188711)

[KMS 검색 순서 17](#_Toc237188712)

[정품 인증 시나리오 18](#_Toc237188713)

[KMS 시나리오 18](#_Toc237188714)

[단일 사이트 네트워크에 대한 기본 KMS 구현 18](#_Toc237188715)

[복잡한 전역 네트워크에서 KMS 구현 19](#_Toc237188716)

[MAK 시나리오 22](#_Toc237188717)

[MAK 독립 정품 인증 23](#_Toc237188718)

[MAK 프록시 정품 인증 27](#_Toc237188719)

[KMS 정품 인증을 위한 VAMT 지원 33](#_Toc237188720)

[KMS를 MAK 정품 인증으로 변환 34](#_Toc237188721)

[제품에 대한 KMS 호스트 키 36](#_Toc237188722)

[정품 인증 정책 값 38](#_Toc237188723)

[KMS 클라이언트 설치 키 39](#_Toc237188724)

[정품 인증 오류 코드 41](#_Toc237188725)

[Windows 이벤트 로그 49](#_Toc237188726)

[WMI 속성 및 방법 53](#_Toc237188727)

[용어 61](#_Toc237188728)

[리소스 링크 62](#_Toc237188729)

# 소개

이 가이드는 [볼륨 정품 인증 계획 가이드](http://go.microsoft.com/fwlink/?LinkId=155926), [볼륨 정품 인증 배포 가이드](http://go.microsoft.com/fwlink/?LinkId=150083) 및 [볼륨 정품 인증 운영 가이드](http://go.microsoft.com/fwlink/?LinkId=150084) 에 대한 기술 참조 정보를 제공합니다. Microsoft® 볼륨 정품 인증 및 그 구성 요소의 개요에 대해서는 [볼륨 정품 인증 계획 가이드](http://go.microsoft.com/fwlink/?LinkId=155926)를 참조하십시오. 이 참조 가이드에는 다음 내용이 포함되어 있습니다.

* 설치 환경
* Slmgr.vbs 옵션
* 레지스트리 설정
* GPO(그룹 정책 개체) 설정
* KMS(키 관리 서비스) 정품 인증 시기
* KMS 검색 순서
* 정품 인증 시나리오
* 제품에 대한 KMS 호스트 키
* 정품 인증 정책 값
* KMS 클라이언트 설치 키
* 정품 인증 오류 코드
* Windows® 이벤트 로그
* WMI(Windows Management Instrumentation) 속성 및 메서드
* 용어
* 리소스

**참고**볼륨 정품 인증을 사용하는 다른 소프트웨어의 지원에 대해서는 이들 응용 프로그램을 위해 특별히 작성된 문서를 참조하십시오.

이 가이드는 다음과 같은 규칙을 사용합니다.

* 명령줄 및 명령줄 옵션은 굵게 표시합니다.
* 명령줄 옵션에서 자리 표시자는 그 주위에 꺽쇠 괄호(<>)를 사용합니다.
* 옵션으로 사용하는 명령줄 옵션은 그 주위에 대괄호([])를 사용합니다.
* 레지스트리 하위 키 및 값 이름은 굵게 표시합니다.

# 설치 환경

Windows® 7 및 Windows Server® 2008 R2는 특정 정품 인증 문제에 개별화된 알림 및 대화 상자를 표시합니다. 표 1은 이러한 알림 및 대화 상자가 각 문제에 어떻게 해당되는지 설명합니다.

**참고**   Windows Server 2008 core edition은 알림 사용자 환경을 제공하지 않습니다.

표 1. 알림 상태를 위한 풍선 및 대화 상자

| **문제** | **알림 풍선** | **해당 대화 상자** |
| --- | --- | --- |
| 새로 설치된 Windows 사본은 정품 인증 유예 기간 만료 때까지 정품 인증되지 않습니다. |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |
| 이전에 정품 인증된 Windows 사본은 Windows의 정품 재인증을 필요로 하는 컴퓨터 하드웨어 또는 BIOS(기본 입출력 시스템) 변경을 감지합니다. 또한, 정품 인증된 KMS 클라이언트는 180일 내에 스스로 정품 재인증하지 않습니다. |  | 37-HW OOT.jpg |
| Windows가 KMS를 사용하여 정품 인증되었으며 180일 및 30일간의 유예 기간 동안 정품 인증을 갱신하지 않았습니다. |  | 37-KMS OOT.jpg |
| 온라인 유효성 검사가 실패하거나 인증되지 않은 Windows 사본이 제품 정품 인증을 통과하도록 하는 정품 인증 악용 사례를 감지합니다. |  | 37-NG.jpg |
| Windows에서 Windows 라이선스 구성 요소의 변경 사항을 감지합니다. |  | 37 - No Key.jpg |
| Windows에서 Windows 라이선스 파일의 변경 사항을 감지합니다. |  | 37 - Reinstall.jpg |

# Slmgr.vbs 옵션

Windows 7 및 Windows Server 2008 R2에서 WMI가 변경되었으므 Slmgr.vbs 스크립트는 플랫폼에 따라 작동되지 않을 수도 있습니다. 따라서 Windows Vista® 운영 체제에서 Windows 7 또는 Windows Server 2008 R2 시스템을 관리하기 위해 Slmgr.vbs를 사용할 수 없습니다. Windows 7 또는 Windows Server 2008 R2에서 하위 수준 시스템을 관리하려고 하면 특정 버전의 불일치 오류가 발생합니다. 예를 들어, **cscript slmgr.vbs <vista\_machine\_name> /dlv**를 실행하면 다음과 같은 결과가 발생합니다.

Microsoft (R) Windows Script Host Version 5.8  
Copyright (C) Microsoft Corporation. All rights reserved.

The remote machine does not support this version of SLMgr.vbs

원격 클라이언트를 관리하려면 VAMT(볼륨 정품 인증 관리 도구) 버전 1.2 이상을 사용하거나 플랫폼 간 차이를 인식하는 사용자 지정 WMI 스크립트를 만듭니다. 볼륨 정품 인증의 WMI 속성 및 메서드에 대한 자세한 내용은 이 참조 가이드 뒷부분의 “” 단원을 참조하십시오.

다음은 Slmgr.vbs 스크립트의 구문이며 각 명령줄 옵션에 대해서는 표 2를 참조하십시오.

slmgr.vbs [MachineName [User Password]] [<Option>]

**참고**볼륨 정품 인증을 사용하는 다른 소프트웨어의 지원에 대해서는 이들 응용 프로그램을 위해 특별히 작성된 문서를 참조하십시오.

표 2. Slmgr.vbs 명령줄 옵션

| **옵션** | **설명** |
| --- | --- |
| **[MachineName]** | 원격 컴퓨터의 이름(기본값은 로컬 컴퓨터) |
| **[User]** | 원격 컴퓨터에 대한 필요한 권한을 갖고 있는 계정 |
| **[Password]** | 원격 컴퓨터에 대한 필요한 권한을 갖고 있는 계정의 암호 |
| **전역 옵션** | |
| **/ipk product\_key** | 5×5 제품 키를 설치합니다. 매개 변수로 제공되는 제품 키가 설치된 운영 체제에 대해 유효하며 사용 가능한지 확인됩니다. 그렇지 않으면 오류가 반환됩니다.  유효하고 사용 가능한 경우 키가 설치됩니다. 이미 키가 설치된 경우 자동으로 교체됩니다.  라이선스 서비스의 안정적으로 유지하기 위해 시스템을 다시 시작하거나 소프트웨어 보호 서비스를 다시 시작해야 합니다.  이 작업은 승격된 명령 프롬프트에서 실행하거나 권한이 없는 사용자도 추가로 소프트웨어 보호 서비스를 액세스할 수 있도록 **표준 사용자 작업** 레지스트리 값을 설정해야 합니다. |
| **/ato [Activation ID]** | KMS 호스트 키나 MAK(복수 정품 인증 키)가 설치된 소매 버전과 볼륨 시스템의 경우 **/ato**를 사용하면 Windows가 온라인 정품 인증을 시도합니다.  GVLK(일반 볼륨 라이선스 키)가 설치된 시스템의 경우에는 KMS 정품 인증 시 시도됩니다. 자동 KMS 정품 인증 시도가 일시 중단되도록 설정된 시스템(**/stao**)의 경우 **/ato**가 실행될 때 KMS 정품 인증이 시도됩니다.  **[Activation ID]** 매개 변수는 **/ato** 지원을 확장한 것으로 컴퓨터에 설치된 Windows 버전을 확인하기 위해 사용합니다. **[Activation ID]** 매개 변수를 지정하면 옵션이 해당 정품 인증 ID에 관련된 버전에만 적용됩니다. **Slmgr.vbs /dlv all**을 실행하면 설치된 Windows 버전의 정품 등록 ID를 얻을 수 있습니다. 다른 응용 프로그램을 지원해야 하는 경우 해당 응용 프로그램과 함께 제공된 설명서를 참조하십시오.  KMS 정품 인증에는 승격된 권한이 필요하지 않습니다. 그러나 온라인 정품 인증에는 승격이 필요하거나 권한이 없는 사용자도 추가로 소프트웨어 보호 서비스를 액세스할 수 있도록 **표준 사용자 작업** 레지스트리 값을 설정해야 합니다. |
| **/dli [Activation ID | All]** | 라이선스 정보를 표시합니다.  기본적으로 **/dli**는 정품 인증되어 설치된 Windows 버전의 라이선스 정보를 표시합니다. **[Activation ID]** 매개 변수를 지정하면 해당 정품 인증 ID와 관련된 특정 버전의 라이선스 정보가 표시됩니다. **[All]**을 매개 변수로 지정하면 사용할 수 있는 설치된 제품의 라이선스 정보가 모두 표시됩니다.  이 작업에는 승격된 권한이 필요하지 않습니다. |
| **/dlv [Activation ID | All]** | 자세한 라이선스 정보를 표시합니다.  기본적으로 **/dlv**는 설치된 운영 체제의 라이선스 정보를 표시합니다. **[Activation ID]** 매개 변수를 지정하면 해당 정품 인증 ID와 관련된 특정 버전의 라이선스 정보가 표시됩니다. **[All]** 매개 변수를 지정하면 사용할 수 있는 설치된 제품의 라이선스 정보가 모두 표시됩니다.  이 작업에는 승격된 권한이 필요하지 않습니다. |
| **/xpr [Activation ID]** | 해당 제품의 정품 인증 만료 날짜를 표시합니다. 기본적으로 이 날짜는 현재 Windows 버전을 참조하며 MAK와 소매 정품 인증이 영구적이므로 주로 KMS 클라이언트용으로 사용됩니다.  **[Activation ID]** 매개 변수를 지정하면 해당 정품 인증 ID와 관련된 특정 버전의 정품 인증 만료 날짜가 표시됩니다.  이 작업에는 승격된 권한이 필요하지 않습니다. |
| **고급 옵션** | |
| **/cpky** | 일부 서비스 작업의 경우 OOBE(Out-of-Box Experience) 작업 중 레지스트리에 제품 키를 사용할 수 있어야 합니다. **/cpky** 옵션은 레지스트리에서 제품 키를 삭제하므로 악성 코드에 의해 키가 유출되지 않습니다.  키를 배포하는 소매 설치의 경우 가장 좋은 방법은 이 옵션을 실행하는 것입니다. MAK와 KMS 호스트 키의 경우 이 옵션은 기본적인 작동이므로 필요하지 않습니다. 이 옵션은 기본적으로 레지스트리에서 키를 삭제하지 않는 다른 유형의 키에만 필요합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/ilc <license\_file>** | 이 옵션은 필요한 매개 변수로 지정된 라이선스 파일을 설치합니다. 이런 라이선스는 토큰 기반 정품 인증을 지원하기 위해 문제 해결의 수단으로 또는 보드상의 응용 프로그램을 수동으로 설치할 때 설치할 수 있습니다.  라이선스의 유효성이 이 프로세스 동안 검사되지 않았습니다. 라이선스 유효성 검사는 Slmgr의 범위를 벗어납니다. 대신 유효성 검사는 소프트웨어 보호 서비스에서 실행 중 처리합니다.  이 작업은 승격된 명령 프롬프트에서 실행하거나 권한이 없는 사용자도 추가로 소프트웨어 보호 서비스를 액세스할 수 있도록 **표준 사용자 작업** 레지스트리 값을 설정해야 합니다. |
| **/rilc** | 이 작업은 %SystemRoot%\system32\oem and %SystemRoot%\System32\spp\tokens에 저장된 모든 라이선스를 다시 설치합니다. 이런 모든 라이선스는 설치 중 저장된 “정상 작동이 확인된" 사본입니다.  신뢰된 저장소에 있는 모든 일치하는 라이선스는 교체됩니다. 다른 추가 라이선스(TA(트러스트된 권한) IL(발급 라이선스), 응용 프로그램용 라이선스 등)는 교체되지 않습니다.  이 작업은 승격된 명령 프롬프트에서 실행하거나 권한이 없는 사용자도 추가로 소프트웨어 보호 서비스를 액세스할 수 있도록 **표준 사용자 작업** 레지스트리 값을 설정해야 합니다. |
| **/rearm** | 이 작업은 정품 인증 타이머를 재설정합니다. **/rearm** 프로세스도 **sysprep /generalize**로 호출됩니다.  이 작업은 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm 레지스트리 하위 키가 **1**인 경우 아무런 작업도 수행하지 않습니다. 이 레지스트리 하위 키에 대한 자세한 내용은 이 가이드의 뒷부분에 있는 “” 단원을 참조하십시오.  이 작업은 승격된 명령 프롬프트에서 실행하거나 권한이 없는 사용자도 추가로 소프트웨어 보호 서비스를 액세스할 수 있도록 **표준 사용자 작업** 레지스트리 값을 설정해야 합니다. |
| **/upk [ActivationID]** | 이 옵션은 현재 Windows 버전의 제품 키를 제거합니다. 다시 시작하면 시스템은 새 제품 키를 설치하기 전까지는 라이선스가 없는 상태가 됩니다.  또는 **[Activation ID]** 매개 변수를 사용하여 설치된 다른 제품을 지정할 수 있습니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **볼륨 라이선스: KMS 클라이언트 옵션** | |
| **/skms Name[:Port] | : port [Activation ID] [Activation ID]** | 이 옵션은 접속할 KMS 호스트 컴퓨터의 이름과 경우에 따라 포트도 지정합니다. 이 값을 설정하면 KMS 호스트의 자동 감지 기능이 해제됩니다.  KMS 호스트에서 인터넷 프로토콜 버전 6(IPv6)만 사용하는 경우 주소는 [hostname]:port. 형식으로 지정해야 합니다. IPv6 주소에 포함된 콜론(:)은 Slmgr.vbs 스크립트에서 잘못 구문 분석됩니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/ckms [Activation ID]** | 이 옵션은 지정된 KMS 호스트 이름, 주소 및 포트 정보를 레지스트리에서 삭제하며 KMS 자동 검색 작동을 복원합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/skhc** | 이 옵션은 KMS 호스트 캐싱(기본값)을 사용하므로 동작 중인 KMS 호스트의 초기 검색 후 DNS(도메인 이름 시스템) **priority** 및 **weight**의 사용이 차단됩니다. 시스템에서 동작 중인 KMS 호스트에 더 이상 접속할 수 없는 경우 검색이 다시 시도됩니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/ckhc** | 이 옵션은 KMS 호스트 캐싱을 해제합니다. 이 설정을 사용하는 경우 클라이언트는 KMS 정품 인증을 시도할 때마다 DNS 자동 검색을 사용합니다(**priority** 및 **weight**를 사용할 때 권장됨).  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **KMS 호스트 구성** | |
| **/sai <interval>** | 이 옵션은 정품 인증이 되지 않은 클라이언트에서 KMS 연결을 시도하는 간격을 분 단위로 설정합니다. 정품 인증 간격은 15분에서 30일이어야 하지만 기본값인 2시간을 사용하는 것이 좋습니다.  KMS 클라이언트는 처음에 레지스트리로부터 이 간격을 채택하지만 첫 KMS 응답을 받은 후 KMS 설정으로 전환합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/sri <interval>** | 이 옵션은 정품 인증이 된 클라이언트에서 KMS 연결을 시도하는 갱신 간격을 분 단위로 설정합니다. 갱신 간격은 15분에서 30일이어야 합니다. 이 옵션은 KMS 서버와 클라이언트 쪽 모두에서 최초에 설정됩니다. 기본값은 10080분(7일)입니다.  KMS 클라이언트는 처음에 레지스트리로부터 이 간격을 채택하지만 첫 KMS 응답을 받은 후 KMS 설정으로 전환합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/sprt <port>** | 이 옵션은 KMS 호스트가 클라이언트 정품 인증 요청을 수신 대기하는 포트를 설정합니다. 기본 TCP 포트는 1688입니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/sdns** | KMS 호스트에 의한 DNS 게시를 설정합니다(기본값).  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/cdns** | KMS 호스트에 의한 DNS 게시를 설정합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/spri** | KMS 우선 순위를 기본으로 설정합니다(기본값).  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/cpri** | KMS 우선 순위를 낮음으로 설정합니다.  이 옵션을 사용하여 공동 호스팅 환경에서 KMS의 경합을 최소화할 수 있습니다. 이로 인해 활성 상태인 다른 응용 프로그램이나 서버 역할에 따라 KMS 부족 현상이 발생할 수 있습니다. 주의하여 사용하십시오.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **토큰 기반 정품 인증 구성** | |
| **/lil** | 설치된 토큰 기반 정품 인증 발급 라이선스를 목록으로 표시합니다. |
| **/ril <ILID> <ILvID>** | 설치된 토큰 기반 정품 인증 발급 라이선스를 제거합니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/stao** | **토큰 기반 정품 인증 전용** 플래그를 설정하므로 자동 KMS 정품 인증이 해제됩니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/ctao** | **토큰 기반 정품 인증만 전용** 플래그를 해제(기본값)하므로 자동 KMS 정품 인증이 설정됩니다.  이 작업은 승격된 명령 프롬프트에서 실행해야 합니다. |
| **/ltc** | 설치된 소프트웨어를 정품 인증할 수 있는 유효한 토큰 기반 정품 인증 인증서를 목록으로 표시합니다. |
| **/fta <Certificate Thumbprint> [PIN]** | 확인된 인증서를 사용하여 토큰 기반 정품 인증을 시도합니다. 옵션인 개인 ID 번호가 제공되므로 하드웨어(스마트 카드 등)로 보호되는 인증서를 사용할 때 개인 ID 번호 프롬프트 없이 개인 키의 잠금을 해제할 수 있습니다. |

# 레지스트리 설정

표 3은 볼륨 정품 인증이 지원하는 레지스트리 설정입니다.

표 3. 레지스트리 설정

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **레지스트리 하위 키: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **값** | **유형** | | **설명** | | **범위** |
| **Activation\AlternateURL** | **REG\_SZ** | | 관리자가 제공하는 URL이 포함될 수 있습니다. 이 키가 채워진 경우 일부 정품 인증 대화 상자에는 기본 브라우저에서 열리는 새 링크**온라인 정품 인증에 대한 자세한 정보**가 포함됩니다. | | 모두 |
| **DisableDnsPublishing** | **REG\_DWORD** | | 0 이외의 값으로 설정하면 KMS 호스트에 의해 자동 게시가 DNS로 차단됩니다. | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **형식:** domain\_name, <priority>, <weight>  KMS가 DNS 서비스(SRV) 레코드 자동 게시에 사용하는 정규화된 도메인 목록이 포함될 수 있습니다. KMS 홈 도메인이 항상 사용되므로 여기에 이를 포함시킬 필요는 없습니다. 이것은 **DisableDnsPublishing** 값에 따라 다릅니다.  **priority** 및 **weight** 매개 변수는 옵션입니다. 이들을 지정하지 않은 경우 SRV 레코드에서 **0**으로 설정됩니다. | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | 공동 호스팅 환경에서 KMS의 경합을 최소화하기 위해 이를 0 이외 값으로 설정합니다. 사용률 높은 시스템의 경우 이에 의해 KMS 호스트가 충분한 정품 인증 수를 관리하지 못할 수도 있습니다. | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | 이를 설정하면 KMS 호스트는 KMS가 지정된 TCP 포트를 수신 대기하도록 지정합니다. 이 값을 지정하지 않은 경우 이 호스트는 TCP 포트 1688을 사용합니다. | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | KMS 클라이언트가 강제로 특정 KMS 호스트를 사용하도록 이 값을 설정합니다. 기본 설정은 아닙니다.  App-ID 또는 SKU-ID를 지정하는 경우 다음은 값이 저장된 하위 키에 생성됩니다.  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName | | KMS 클라이언트 |
| **KeyManagementServicePort** | **REG\_SZ** | | KMS와 통신할 때 KMS 클라이언트가 강제로 특정 TCP 포트를 사용하도록 이 값을 설정합니다. 이 값을 지정하지 않은 경우 이 클라이언트는 포트 1688을 사용합니다.  App-ID 또는 SKU-ID를 지정하는 경우 다음은 값이 저장된 하위 키에 생성됩니다.  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort | | KMS 클라이언트 |
| **KeyManagementServiceVersion** | **REG\_SZ** | | KMS의 Microsoft Operations Manager (MOM) 2005 자동 검색을 사용하려면 이 값을 설정합니다. 컴퓨터에서 KMS가 더 이상 사용되지 않는 경우에는 이 값을 삭제하십시오. | | KMS |
| **UserOperations** | **REG\_DWORD** | | 이 값은 기본적으로 존재하지 않으며 기본값은 **0**이며 이에는 승격이 필요합니다. 이 값을 생성한 후 **1**로 설정하면 표준 사용자가 제품 키를 설치할 수 있으며 승격 없이 컴퓨터를 정품 인증하고 라이선스 초기화할 수 있습니다.  이 설정은 **\policies** 레지스트리 하위 키에 있는 GPO를 통해 구성할 수도 있습니다. | | 모두(KMS만이 아니라) |
| **VLActivationInterval** | **REG\_DWORD** | | KMS 서버와 클라이언트 쪽 모두에서 최초에 설정됩니다. 기본값은 120분(2시간)입니다. KMS 클라이언트는 처음에 레지스트리로부터 이 간격을 채택하지만 첫 KMS 응답을 받은 후 KMS 설정으로 전환합니다. 최소값은 15분, 최대값은 43,200분(30일)입니다. | | KMS 클라이언트 및 서버 |
| **VLRenewalInterval** | **REG\_DWORD** | | KMS 서버와 클라이언트 쪽 모두에서 최초에 설정됩니다. 기본값은 10,080분(7일)입니다. KMS 클라이언트는 처음에 레지스트리로부터 이 간격을 채택하지만 첫 KMS 응답을 받은 후 KMS 설정으로 전환합니다. 따라서 클라이언트 쪽 설정은 절대로 사용되지 않습니다. 최소값은 15분, 최대값은 43,200분(30일)입니다. | | KMS 클라이언트 및 서버 |
| **레지스트리 하위 키: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **값** | **유형** | **설명** | | **범위** | |
| **Manual** | **REG\_DWORD** | **0** = 자동 온라인 정품 인증 허용(기본값)  **1** = 자동 정품 인증 사용 안 함 | | MAK 및 KMS 호스트. KMS 클라이언트 아님. | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = 정품 인증 알림 및 풍선 표시(기본값)  **1** = Windows가 알림 또는 라이선스가 없는 상태가 아닌 경우 모든 정품 인증 관련 알림이 표시되지 않습니다. 권장하지 않음 | | 모두(KMS만이 아니라) | |

# GPO(그룹 정책 개체) 설정

표 4는 GPO(그룹 정책 개체)의 여러 설정입니다. 각 조직은 이를 사용하여 알림 상태에서 운영 체제의 바탕 화면이 검은 색으로 변경되지 않도록 만들 수 있습니다.

표 4 GPO(그룹 정책 개체) 설정

| **정책 이름** | **설명** |
| --- | --- |
| **사용자 구성 -> 관리 템플릿 -> 제어판 -> 개인 설정 -> 바탕 화면 배경 변경 금지** | 사용자가 바탕 화면의 배경 모양을 추가하거나 변경하지 못하도록 만듭니다.  기본적으로 사용자는 개인 설정 또는 제어판 표시 항목의 **바탕 화면 배경** 페이지를 사용하여 배경 모양(배경 무늬)을 자신의 바탕 화면에 추가할 수 있습니다.  이 설정을 사용하도록 지정하면 사용자는 바탕 화면 배경 설정을 변경할 수 없습니다.  그룹의 배경 무늬를 지정하려면 **바탕 화면 배경 무늬** 설정을 사용합니다.  **참고**   사용자가 바탕 화면 배경 무늬를 변경하지 못하도록 하려면 **바탕 화면 배경 무늬** 설정도 사용으로 지정해야 합니다. 자세한 내용은 Microsoft 도움말 및 지원 문서, “관리자가 그룹 정책에서 &#x91;배경 무늬 변경 안 함' 옵션을 선택한 후에도 사용자가 바탕 화면 배경 무늬를 변경할 수 있다”(<http://support.microsoft.com/kb/Q327998>)을 참조하십시오.  또한 **비트맵 배경 무늬만 허용** 설정도 참조하십시오. |
| **사용자 구성 -> 관리 템플릿 -> 바탕 화면 -> 바탕 화면 -> 바탕 화면 배경 무늬** | 모든 사용자의 바탕 화면에 표시되는 바탕 화면 배경("배경 무늬")을 지정합니다.  이 설정을 사용하는 경우 사용자의 바탕 화면의 배경 무늬를 지정할 수 있으며 사용자가 이미지나 프레젠테이션을 변경하지 못하게 만들 수 있습니다. 지정하는 배경 무늬는 비트맵(\*.bmp) 또는 JPEG (\*.jpg) 파일로 저장할 수 있습니다.  이 설정을 사용하려면 배경 무늬 이미지의 정규화된 경로와 파일 이름을 입력합니다. C:\Windows\web\wallpaper\home.jpg와 같은 로컬 경로 또는 \\Server\Share\Corp.jpg와 같은 UNC(Universal Naming Convention) 경로를 입력할 수 있습니다. 지정한 파일을 사용자가 로그온할 때 사용할 수 없으면 배경 무늬가 표시되지 않습니다. 사용자는 다른 배경 무늬를 지정할 수 없습니다. 이 설정을 사용하여 배경 무늬를 가운데, 바둑판식 또는 늘이기 중 하나로 지정할 수도 있습니다. 사용자는 이렇게 지정된 사항을 변경할 수 없습니다.  이 설정을 해제하거나 구성하지 않은 경우 배경 무늬는 표시되지 않습니다. 그러나 사용자는 원하는 배경 무늬를 선택할 수 있습니다.  또한 같은 위치에 있는 **비트맵 배경 무늬만 허용** 설정 및 사용자 구성\관리 템플릿\제어판의 **배경 무늬 변경 안 함** 설정도 참조하십시오.  **참고**   이 설정은 원격 데스크톱 세션에는 적용되지 않습니다. |
| **사용자 구성 -> 관리 템플릿 -> 제어판 -> 개인 설정 -> 바탕 화면 아이콘 변경 금지** | 사용자가 바탕 화면 아이콘을 변경하지 못하도록 만듭니다.  기본적으로 사용자는 개인 설정 또는 제어판 표시 항목의 **바탕 화면 아이콘 설정** 대화 상자를 사용하여 바탕 화면 아이콘을 표시, 숨기기 또는 변경할 수 있습니다.  이 설정을 사용하도록 지정하면 사용자는 바탕 화면 아이콘을 변경할 수 없습니다.  Windows Vista 이전 운영 체제의 경우 이 설정을 사용하면 제어판 표시 항목에서 **바탕 화면** 탭도 표시되지 않습니다. |

# KMS 정품 인증 시기

KMS 정품 인증 시기는 다음 두 설정으로 제어합니다. 정품 인증 및 갱신 타이머:

* KMS 정품 인증 간격에 의해 유예 및 알림 기간 동안 정품 인증되기 전 KMS 클라이언트에서 정품 인증을 시도하는 빈도가 결정됩니다. 이 값은 **slmgr.vbs /sai *interval***을 실행하여 클라이언트에 설정됩니다. 간격은 분 단위로 표시되며 120분이 기본값입니다. 자세한 내용은 “” 및 “” 단원을 참조하십시오. 시스템이 KMS 호스트에 접속되면 로컬 클라이언트 설정 대신 KMS 호스트 설정이 사용됩니다.
* KMS 갱신 간격에 의해 KMS 클라이언트에서 정품 인증된 후 KMS를 통한 정품 재인증 시도 빈도가 결정됩니다. 이 값은 **slmgr /sri *interval***을 사용하여 설정할 수 있습니다. 간격은 분 단위로 설정합니다. 기본값은 10,080분(7일)입니다. 이 값은 클라이언트에 설정할 수 있지만 KMS 호스트에서 제공하는 값이 대신 사용됩니다.

작동하는 동안 KMS 클라이언트는 시작 시 KMS 호스트에 접속하려고 시도하며 실패 시 정품 인증 간격 시간(분)마다 다시 접속을 시도합니다. 기본적으로 이 과정은 2시간마다 반복됩니다. KMS 정품 인증이 성공하면 클라이언트는 KMS 호스트의 갱신 간격을 받아 저장하므로 Windows는 180일 동안 정품이 인증됩니다. 정품 인증 갱신은 슬라이딩 윈도우로 작동하며 DHCP(Dynamic Host Configuration Protocol) 임대와 유사합니다. 클라이언트는 180일 동안 정품이 인증되지만 갱신 간격 시간(기본값 7일)마다 정품 재인증이 시도됩니다. 인증에 성공하면 180일 기간이 재설정됩니다. 실패하면 시스템은 다른 시도를 발생시킬 네트워크 변경사항이나 다른 적격한 이벤트를 감시합니다. 15분 후 시스템은 적격한 이벤트의 감시를 중지하지만 정품 인증 간격 시간(분)마다 계속 시도합니다.

180일 동안 정품 재인증이 성공하지 못하면 클라이언트는 OOT(오차 허용 범위) 유예 기간으로 전환됩니다. OOT로 전환한 후 30일 이내에 정품 인증을 받지 못하면 알림 모드로 전환됩니다.

# KMS 검색 순서

KMS 자동 검색이 설정(기본값)되어 있고 KMS 호스트 캐싱이 해제된 경우 KMS 클라이언트는 다음 순서에 따라 사용할 KMS를 결정합니다(올바른 키가 있는 정품이 인증된 KMS 호스트가 응답할 때까지 각 단계가 수행됨).

* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ 레지스트리 값의 SKU-지정 값
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ 레지스트리 값의 AppID-지정 값
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ 레지스트리 값의 전역 값
* SKU-지정 캐시 KMS 호스트(최근 성공한 KMS 정품 인증에 사용된 호스트의 캐시된 ID).
* DNS 자동 검색(**weight** 및 **priority** 인식됨)

캐시된 KMS가 응답하지 않으면 검색이 수행됩니다.

# 정품 인증 시나리오

다음 단원에서는 KMS와 MAK 정품 인증의 주요 시나리오에 대해 설명합니다.

## KMS 시나리오

KMS는 간단한 단일 사이트 네트워크와 전역 네트워크를 지원할 수 있습니다. 다음 시나리오에서 설명하는 내용

* KMS의 기본 구현.
* 전역 네트워크를 지원하기 위해 확장되는 구현.

### 단일 사이트 네트워크에 대한 기본 KMS 구현

Contoso에는 100개의 Windows 7 Enterprise 클라이언트와 혼합된 형태의 Windows Vista, Windows Server 2008 및 Windows Server 2008 R2 시스템이 있습니다. Contoso는 평이한 도메인(Contoso.com)입니다(그림 1 참조). DNS 서버는 Microsoft DNS를 기본 구성을 실행합니다. 이 구성은 동적 DNS 등록과 DNS 레코드 청소를 지원하므로 부실한 레코드를 제거할 수 있습니다.



그림 1. 단일 사이트 네트워크에 대한 기본 KMS 구현

Contoso는 모든 시스템의 정품을 인증하는 KMS B 키를 제공하는 라이선스 계약서를 구입합니다. IT(정보 기술) 관리자는 승격된 명령 프롬프트에서 로컬로 실행되는 다음 명령을 사용하여 Windows Server 2008 R2가 실행되는 두 개의 KMS 호스트에 Contoso의 KMS 호스트 키(CSVLK)를 설치합니다.

Slmgr.vbs /ipk <KMS\_host\_key>

그런 다음 IT 관리자는 AD DS(Active Directory® 도메인 서비스) 내의 *KMS\_Hosts.*라는 보안 그룹을 생성합니다. 관리자는 서버 KMS\_1 및 KMS\_2를 KMS\_Hosts 구성원에 추가합니다.

호스트 KMS\_1은 인터넷에서 Microsoft을 통해 정품 인증됩니다. **Slmgr.vbs /ato**. KMS\_1은 자동으로 자신의 SRV RR(리소스 레코드)를 DNS로 게시합니다. IT 관리자는 DNS 서버에 액세스하여 \_vlmcs.\_tcp.contoso.com의 RR을 찾은 후 KMS\_Hosts에 레코드에 읽기, 쓰기, 삭제 권한을 부여하기 위해 권한을 변경합니다. 호스트 KMS\_2는 인터넷에서 Microsoft을 통해 정품 인증됩니다. **Slmgr.vbs /ato***.*

마지막으로 관리자는 KMS 호스트 제외가 Windows 방화벽에서 설정되었는지 확인합니다. KMS(키 관리 서비스) 방화벽 예외도 설정해야 합니다.

Contoso 네트워크의 KMS 클라이언트는 DNS를 쿼리한 후 두 KMS 호스트의 SRV 레코드를 받습니다. 클라이언트는 두 호스트 중 하나를 선택하고 정품 인증됩니다(KMS 정품 인증 수가 최소 한계를 넘는 순간). KMS 정품 인증 수 요구 사항에 대한 자세한 내용은 “” 단원을 참조하십시오.

### 복잡한 전역 네트워크에서 KMS 구현

Contoso는 두 개의 도메인인 east.contoso.com과 west.contoso.com으로 확장되었습니다(그림 2 참조). 네트워크 트래픽은 방화벽이 설정된 WAN(광역 네트워크) 링크를 통해 두 네트워크 간에 안전하게 통과할 수 있습니다. 이 링크의 대역폭은 제한되어 있으므로 리소스(DNS 포함)는 트래픽을 줄이기 위해 WAN 링크의 양쪽에서 가능한 복제됩니다.



그림 2. 복잡한 전역 네트워크에서 KMS 구현

Contoso는 이미지 기반 배포를 사용합니다. 해당 클라이언트 시스템은 Windows Vista에서 표준화되어 있지만 Windows Vista 시스템은 Windows 7 클라이언트로 대체되고 있습니다.

사용자는 지리적으로 정기적으로 이동하지만 이들의 네트워크 연결은 특정 도메인에서 다른 도메인으로 바뀝니다. 로컬 DNS 호스트, 로컬 게이트웨이 주소 등을 포함하여 클라이언트의 IP 주소 지정은 DHCP에서 동적으로 결정합니다.

기존 Windows Vista 클라이언트와 새 Windows 7 클라이언트에 정품 인증 지원을 제공하기 위해 Contoso은 네 개의 KMS 호스트를 설치합니다(KMS B 키 사용). 두 개의 KMS 호스트는 east.contoso.com에 다른 두 개는 west.contoso.com에 구성됩니다.

IT 관리자는 KMS 호스트를 구성하므로 DNS SRV 레코드는 east 도메인의 Windows 7 및 Windows Server 2008 R2 클라이언트를 KMS\_E1 또는 가능한 경우 KMS\_E2로 이동합니다. 둘 다 가능하지 않은 경우 클라이언트는 KMS\_W1과 최종적으로 KMS\_W2를 시도합니다. 마찬가지로 west의 DNS가 구성되므로 west 도메인의 Windows 7 클라이언트는 KMS\_W1, KMS\_W2 순으로 접속하고 이들이 실패하는 경우에만 WAN 링크의 먼 쪽에 있는 KMS\_E1 및 KMS\_E2로 정품 인증을 시도합니다.

IT 관리자는 이와 같은 작업을 다음과 같이 구성을 변경하여 수행합니다(표 5 참조).

* KMS\_E\* 호스트가 보안 그룹 KMS\_E에 추가됩니다 이 그룹에는 \_vlmcs.\_tcp.east.contoso.com 레코드에 대한 읽기, 쓰기, 삭제 권한이 부여됩니다.
* KMS\_W\* 호스트가 보안 그룹 KMS\_W에 추가됩니다 이 그룹에는 \_vlmcs.\_tcp.west.contoso.com 레코드에 대한 읽기, 쓰기, 삭제 권한이 부여됩니다.
* east.contoso.com 및 west.contoso.com을 모든 클라이언트의 DNS 접미사 검색 목록에 추가하기 위해 DHCP 서버가 구성됩니다.
* east와 west 도메인 간의 방화벽이 구성되어 1688 포트에서 KMS 호스트로 RPC 트래픽이 허용됩니다.

표 5. KMS 호스트 구성

| **설명** | **구성** | **호스트** |
| --- | --- | --- |
| 클라이언트가 KMS\_W\* 호스트에 접속을 시도하기 전에 가능한 경우 KMS\_E\* 호스트에 접속하도록 east.contoso.com SRV의 priority와 weight를 구성합니다. 트래픽이 75%는 KMS\_\*1 호스트로 25%는 KMS\_\*2 호스트로 분산됩니다. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_E1, 10, 75  KMS\_E2, 10, 25  KMS\_W1, 90, 75  KMS\_W2, 90, 25 | KMS\_E1  KMS\_E2 |
| 클라이언트가 KMS\_E\* 호스트에 접속을 시도하기 전에 가능한 경우 KMS\_W\* 호스트에 접속하도록 west.contoso.com SRV의 priority와 weight를 구성합니다. 트래픽이 75%는 KMS\_\*1 호스트로 25%는 KMS\_\*2 호스트로 분산됩니다. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_W1, 10, 75  KMS\_W2, 10, 25  KMS\_E1, 90, 75  KMS\_E2, 90, 25 | KMS\_W1  KMS\_W2 |

그런 다음 관리자는 표 6의 내용에 따라 KMS 클라이언트 트래픽을 허용하도록 Windows 방화벽 예외를 확인한 후 클라이언트 컴퓨터를 구성합니다

표 6. KMS 클라이언트 구성

| **설명** | **구성** |
| --- | --- |
| KMS 호스트 캐싱을 해제합니다. | **Slmgr /ckhc** |
| 정품 인증 문제가 있는 사용자가 Contoso 헬프 데스크에 직접 문의할 수 있도록 고객 URL이 설정됩니다. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  AlternateURL = http://contoso.com/help |

클라이언트 참조 컴퓨터의 KMS 정품 인증이 완료된 후 **sysprep /generalize**가 실행됩니다. 이 시스템은 종료된 후 Windows AIK(자동 설치 키트)의 ImageX를 사용하여 이미지화됩니다. Windows AIK는 <http://go.microsoft.com/fwlink/?LinkId=136976>에서 다운로드할 수 있습니다.

## MAK 시나리오

다음 단원에서는 MAK 정품 인증의 시나리오에 대해 설명합니다. 이들은 그림 3의 시나리오를 바탕으로 합니다. 그림 3은 대기업의 일반적인 네트워크와 작업 그룹 환경입니다.

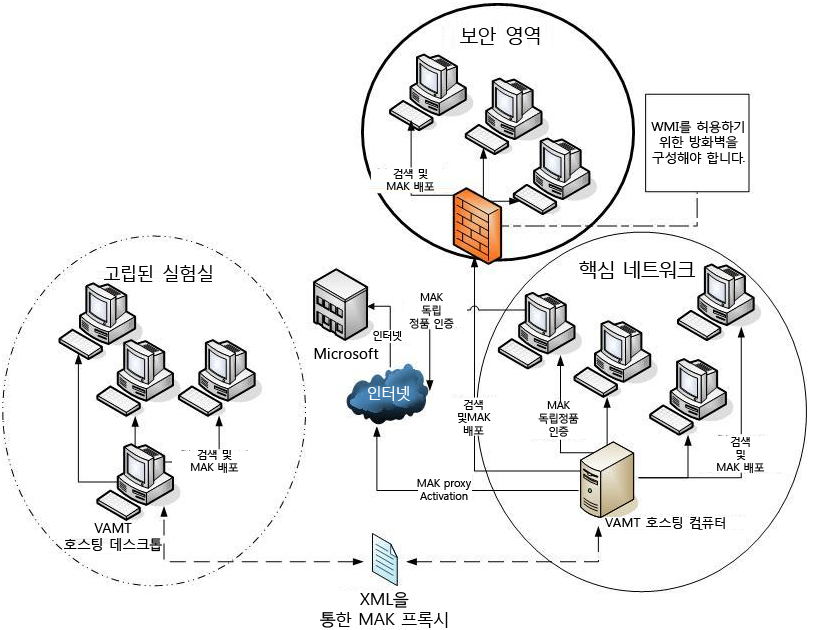


그림 3 기업 환경

핵심 네트워크 환경에서 모든 컴퓨터는 AD DS가 관리하는 공통 네트워크 내에 있습니다. 보안 영역은 방화벽 보호가 추가된 높은 수준의 보안 핵심 네트워크 컴퓨터를 나타냅니다.

고립된 실험실 환경은 핵심 네트워크와 물리적으로 떨어져 있고 포함된 컴퓨터에서 인터넷을 사용할 수 없는 작업 그룹입니다. 네트워크 보안 정책 상 특정 컴퓨터나 사용자를 식별할 수 있는 정보는 고립된 실험실 외부로 유출되어서는 안됩니다.

### MAK 독립 정품 인증

VAMT를 사용하면 그림 2와 같이 중앙 콘솔에서 MAK를 배포하여 네트워크를 통한 MAK 배포와 정품 인증을 자동으로 처리할 수 있습니다. VAMT는 주어진 MAK에 대해 남은 정품 인증 수를 Microsoft 정품 인증 서버에 쿼리한 다음 해당 환경에서 모든 MAK 정품 인증 시스템의 정품 인증 상태를 나열합니다. 이 수는 실시간이 아니라 특정 시점에서의 수입니다. VAMT 버전 1.2는 Windows AIK에 포함되어 있습니다.

이 시나리오에서 VAMT는 핵심 네트워크 환경에 배포됩니다(그림 3 참조). VAMT는 모든 클라이언트 컴퓨터에 네트워크 액세스가 가능한 중앙 컴퓨터에 설치됩니다. VAMT 호스트 및 클라이언트 컴퓨터에서는 인터넷 액세스가 가능합니다. 다음은 독립 정품 인증을 수행하는 방법입니다.

1. 네트워크로 연결된 호스트 컴퓨터에 VAMT를 설치하고 시작합니다.
   1. Windows AIK를 호스트 컴퓨터에 설치합니다.
   2. 시작을 클릭한 후 **VAMT**를 클릭하여 VAMT 콘솔을 엽니다.
2. WMI(Windows Management Instrumentation) 방화벽 예외를 대상 컴퓨터에 구성합니다. WMI 방화벽 예외가 모든 대상 컴퓨터에 대해 사용으로 설정되었는지 확인합니다(그림  4 참조).

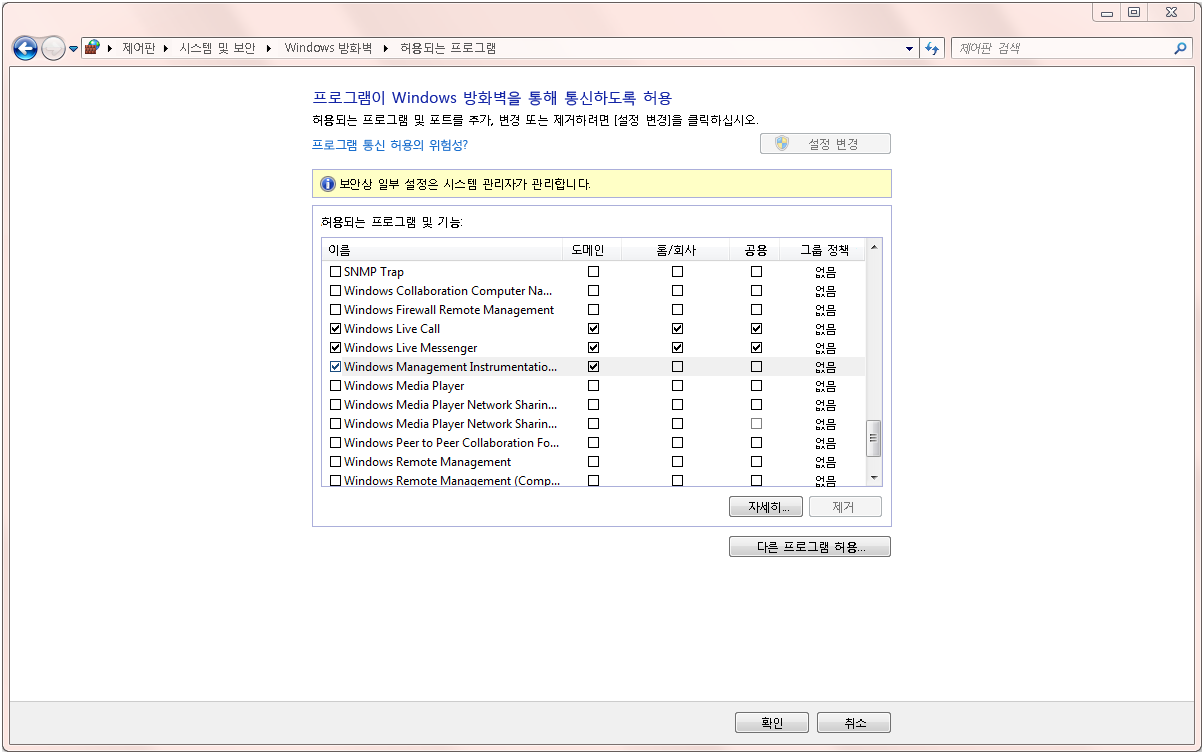


그림 4 WMI(Windows Management Instrumentation) 예외

1. 컴퓨터를 CIL(컴퓨터 정보 목록)에 추가합니다.
   1. VAMT 콘솔에서 **작업**을 클릭한 후 **컴퓨터 추가**를 클릭하여 **컴퓨터 추가** 대화 상자를 표시합니다.
   2. *핵심 네트워크 그룹*과 같이 정품 인증 중인 컴퓨터 그룹을 나타내는 컴퓨터 그룹 이름을 입력합니다.
   3. 드롭다운 목록을 클릭하여 검색 옵션을 선택합니다. 작업 그룹이나 AD DS 도메인 내의 또는 개별 컴퓨터 이름이나 IP 주소에 따라 컴퓨터를 검색할 수 있습니다.
   4. 개별 컴퓨터 이름 또는 IP 주소로 검색하는 경우 드롭다운 목록 밑의 입력란에 해당 정보를 입력합니다.
   5. 도메인 또는 작업 그룹을 검색하는 경우 해당 옵션에 따라 표시되는 추가 드롭다운 목록에서 도메인이나 작업 그룹을 선택합니다. **컴퓨터 이름별로 필터링** 필드를 사용하면 도메인 또는 작업 그룹 내의 특정 컴퓨터를 검색할 수 있습니다.
   6. **확인**을 클릭합니다.

VAMT는 LDAP(Lightweight Directory Access Protocol)를 통해 AD DS(Active Directory Directory Services)를 쿼리한 후 검색한 컴퓨터를 CIL에 추가합니다.

1. 검색한 컴퓨터에서 상태 정보 수집:
   1. VAMT의 경우 컴퓨터에서 작업을 수행하려면 해당 컴퓨터에 대한 현재 라이선스 상태 데이터가 있어야 합니다. 컴퓨터 목록 보기 창에서 하나 이상의 컴퓨터를 직접 선택하여 개별 컴퓨터의 상태를 수집합니다. 전체 그룹에 대해 작업을 수행하려면 보기 창에서 알 수 없는 상태 노드 또는 사용자 정의 그룹\핵심 네트워크 그룹 노드를 선택합니다.
   2. 그룹이나 원하는 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **컴퓨터 상태 새로 고침**을 클릭합니다.
   3. 현재 갖고 있는 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용**을 선택합니다.
   4. **확인**을 클릭합니다.
   5. 메시지가 표시되는 경우 도메인 관리자 계정(도메인 내의 모든 컴퓨터의 상태를 수집하기 위해)과 암호를 제공합니다.

VAMT는 선택한 모든 컴퓨터의 상태를 수집하는 동안 **컴퓨터 정보 수집 중**이라는 대화 상자를 표시합니다. 이 프로세스가 완료되면 새로 고친 각 컴퓨터의 상태가 VAMT 콘솔의 컴퓨터 목록 보기 창에 나타납니다.

**참고**   선택한 컴퓨터에서 라이선스 상태를 검색하기 위해 VAMT는 원격 컴퓨터에 대해 관리 권한이 있어야 하며 Windows 방화벽을 통해 WMI를 액세스할 수 있어야 합니다. 또한 작업 그룹 컴퓨터의 경우 레지스트리 키를 생성하여 UAC(사용자 계정 컨트롤)에서 원격 관리 작업이 가능하도록 만들어야 합니다. VAMT 원격 관리 구성에 대한 자세한 내용은 VAMT 도움말을 참조하십시오.

1. MAK를 추가한 후, 나머지 정품 인증 수를 확인합니다.
   1. **옵션**을 클릭한 후 **MAK 관리**를 클릭하여 **MAK 키 관리** 대화 상자를 엽니다.
   2. **추가**를 클릭하여 MAK를 입력합니다.
   3. MAK를 입력한 후 **유효성 검사**를 클릭합니다.

유효성이 검사되면 **버전** 필드가 자동으로 채워집니다.

* 1. 적절한 설명을 입력한 후,**추가**를 클릭합니다.

MAK가 **MAK 키 관리** 대화 상자에 표시됩니다.

* 1. **나머지 정품 인증 수 새로 고침**을 클릭하여 나열된 MAK에 대한 나머지 정품 인증 수를 Microsoft에서 가져옵니다. (이 단계에서 인터넷이 사용됩니다.)
  2. **종료**를 클릭하여 대화 상자를 닫습니다.

1. MAK를 설치한 후, 클라이언트 컴퓨터를 정품 인증합니다.
   1. 트리 보기 창에서 그룹을 클릭하거나 목록 보기 창에서 개별 컴퓨터를 선택하여 정품 인증할 컴퓨터를 선택합니다.
   2. 선택한 그룹이나 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **MAK 독립 정품 인증**을 클릭하여 **MAK 독립 정품 인증** 대화 상자를 표시합니다.
   3. **MAK 설치** 목록에서 적절한 MAK를 선택합니다.
   4. **MAK 설치(기존 덮어쓰기)** 및 **지금 정품 인증** 확인란을 선택하여 인터넷을 통해 Microsoft Windows Activation에 접속하여 선택한 컴퓨터를 즉시 정품 인증합니다.

별표(\*)가 이런 확인란 텍스트 옆에 나타나면 해당 작업은 가능한 컴퓨터에만 적용됩니다. 예를 들어, Windows Vista 소매 버전이 설치된 컴퓨터는 MAK를 사용하여 정품 인증할 수 없습니다.

* 1. 현재 갖고 있는 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용**을 선택합니다.
  2. **확인**을 클릭합니다.

VAMT는 **제품 키 할당** 대화 상자를 표시한 후 요청한 작업이 완료될 때까지 **컴퓨터 정품 인증 중** 대화 상자를 표시합니다. **다른 자격 증명 사용**을 선택한 경우 이런 대화 상자가 표시되기 전에 관련 자격 증명을 입력하라는 메시지가 표시됩니다.

### MAK 프록시 정품 인증

이 시나리오에서는 VAMT를 사용하여 고립된 실험실 환경 내의 작업 그룹 컴퓨터를 정품 인증하였습니다(그림 3 참조). 이런 작업 그룹의 경우 대규모 네트워크에서 완전히 격리되었지만 고립된 작업 그룹 내의 컴퓨터에 두 번째 VAMT를 설치하고, 해당 컴퓨터와 인터넷 액세스가 가능한 다른 VAMT 호스트 간에 VAMT CIL을 전송하기 위해 이동 미디어를 사용하여 MAK 프록시 정품 인증을 수행할 수 있습니다. VAMT 원격 관리 구성에 대한 자세한 내용은 VAMT 도움말을 참조하십시오. 다음은 프록시 정품 인증을 수행하기 위해 VAMT 도구를 사용하는 방법입니다.

1. 고립된 실험실 내의 작업 그룹 컴퓨터에 VAMT를 설치합니다.
   1. Windows AIK를 고립된 실험실 작업 그룹의 호스트 컴퓨터에 설치합니다.

이 컴퓨터는 Windows XP with 서비스 팩 2(SP2), Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 또는 Windows Server 2008 R2이 실행되는 컴퓨터일 수 있습니다.

* 1. 시작을 클릭한 후 **VAMT**를 클릭하여 VAMT 콘솔을 엽니다.
  2. WMI(Windows Management Instrumentation) 방화벽 예외를 대상 컴퓨터에 구성합니다. WMI 방화벽 예외가 모든 대상 컴퓨터에 대해 사용으로 설정되었는지 확인합니다.

1. CIL에 컴퓨터를 추가합니다.
   1. VAMT 콘솔에서 **작업**을 클릭한 후 **컴퓨터 추가**를 클릭하여 **컴퓨터 추가** 대화 상자를 표시합니다.
   2. *고립된 실험실 그룹*과 같이 정품 인증 중인 컴퓨터 그룹을 나타내는 그룹 이름을 입력합니다.
   3. **작업 그룹** 옵션을 선택한 후 작업 그룹의 이름을 지정하고 **확인**을 클릭합니다.

VAMT는 컴퓨터의 작업 그룹을 검색합니다.

**참고**   VAMT의 경우 작업 그룹 내의 컴퓨터를 검색하려면 네트워크 검색 Windows 방화벽 예외를 설정해야 합니다.

1. 검색한 컴퓨터에서 상태를 수집합니다.
   1. VAMT의 경우 컴퓨터에서 작업을 수행하려면 해당 컴퓨터에 대한 현재 라이선스 상태 데이터가 있어야 합니다. 컴퓨터 목록 보기 창에서 하나 이상의 컴퓨터를 직접 선택하여 개별 컴퓨터의 상태를 수집합니다. 전체 그룹에 대해 작업을 수행하려면 보기 창에서 알 수 없는 상태 노드 또는 사용자 정의 그룹\핵심 네트워크 그룹 노드를 선택합니다.
   2. 그룹이나 원하는 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **컴퓨터 상태 새로 고침**을 클릭합니다.
   3. 현재 갖고 있는 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용**을 선택합니다.
   4. **확인**을 클릭합니다. 메시지가 표시되면 선택한 작업 그룹 컴퓨터에 로컬 관리 권한이 있는 계정에 자격 증명을 제공합니다.

VAMT는 선택한 모든 컴퓨터의 상태를 수집하는 동안 **컴퓨터 정보 수집 중**이라는 대화 상자를 표시합니다. 이 프로세스가 완료되면 새로고친 각 컴퓨터의 상태가 VAMT 콘솔의 컴퓨터 목록 보기 창에 나타납니다.

**참고**   선택한 컴퓨터에서 라이선스 상태를 검색하기 위해 VAMT는 원격 컴퓨터에 대해 관리 권한이 있어야 하며 Windows 방화벽을 통해 WMI를 액세스할 수 있어야 합니다. 또한 작업 그룹 컴퓨터의 경우 레지스트리 키를 생성하여 UAC에서 원격 관리 작업이 가능하도록 만들어야 합니다.

1. MAK를 추가합니다.
   1. **옵션**을 클릭한 후 **MAK 관리**를 클릭하여 **MAK 키 관리** 대화 상자를 엽니다.
   2. **추가**를 클릭하여 MAK를 입력합니다.
   3. MAK를 입력한 후 **유효성 검사**를 클릭합니다.

유효성이 검사되면 **버전** 필드가 자동으로 채워집니다.

* 1. 적절한 설명을 입력한 후,**추가**를 클릭합니다.

MAK가 **MAK 키 관리** 대화 상자에 표시됩니다.

* 1. **종료**를 클릭하여 대화 상자를 닫습니다.

**참고**   VAMT가 인터넷이 연결되는 컴퓨터에 설치되지 않았으므로 **나머지 정품 인증 수 새로고침** 옵션은 작동하지 않습니다. 이 기능을 사용하려면 인터넷이 필요합니다.

1. 고립된 실험실 컴퓨터에 MAK를 설치합니다.
   1. 트리 보기 창에서 고립된 실험실 그룹을 선택합니다.
   2. 선택한 그룹이나 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **MAK 독립 정품 인증**을 클릭하여 **MAK 독립 정품 인증** 대화 상자를 표시합니다.
   3. **MAK 설치** 목록에서 적절한 MAK를 선택합니다.
   4. **MAK 설치(기존 덮어쓰기)**를 선택합니다.

별표(\*)가 이런 확인란 텍스트 옆에 나타나면 해당 작업은 가능한 컴퓨터에만 적용됩니다. 예를 들어, Windows Vista 소매 버전이 설치된 컴퓨터는 MAK를 사용하여 정품 인증할 수 없습니다.

* 1. 이 컴퓨터에서 인터넷에 액세스할 수 없으므로 **Microsoft에서 확인 ID 가져오기** 확인란 선택을 취소합니다.
  2. CID(확인 ID)가 아직 요청되지 않았으므로 **확인 ID 적용 후 정품 인증** 확인란 선택을 취소합니다.
  3. 현재 사용 중인 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용**을 선택한 후 **확인**을 클릭합니다.

VAMT는 요청한 작업이 완료될 때까지 **제품 키 할당** 대화 상자를 표시합니다. **다른 자격 증명 사용**을 선택한 경우 이런 대화 상자가 표시되기 전에 관련 자격 증명을 입력하라는 메시지가 표시됩니다.

**참고**   **MAK 설치(기존 덮어쓰기)** 확인란을 선택하면 MAK가 클라이언트 컴퓨터에 강제로 설치됩니다. 따라서 이런 경우에는 주의해야 합니다. Windows Vista SP1 이전 버전이 30일 이상 컴퓨터에 설치되어 있고 초기 유예 기간이 만료된 경우 다음 로그온 전에 정품 인증이 성공적으로 완료되지 않으면 컴퓨터가 RFM(기능 제한 모드)으로 전환됩니다. 그러나 올바르게 구성된 컴퓨터에서 VAMT 호스트를 액세스할 수 있는 경우에는 MAK 프록시 정품 인증을 사용하여 RFM로부터 이들 컴퓨터를 복원할 수 있습니다. RFM은 Windows Vista의 SP1 이전 버전에만 적용됩니다. Windows Vista(SP1 이상), Windows 7, Windows Server 2008 또는 Windows Server 2008 R2는 RFM으로 전환되지 않습니다.

1. CIL을 저장합니다.

이 단계에서는 전체 CIL을 로컬(작업 그룹) VAMT 호스트에 저장합니다. MAK 프록시 정품 인증에서는 VAMT가 이 파일을 사용하여 CID를 해당 컴퓨터에 적용하므로 이 파일을 보관해야 합니다.

* 1. VAMT 트리 보기 또는 목록 보기 창에서 MAK를 성공적으로 수신한 그룹 또는 개별 컴퓨터를 선택합니다.
  2. **파일** 메뉴에서 **저장**을 클릭하여 **컴퓨터 정보 목록 저장** 대화 상자를 표시합니다.
  3. 디렉터리를 선택한 후, *IsolatedLabGroup.CIL.*과 같이 CIL 파일 이름을 입력합니다.
  4. **저장**을 클릭합니다.

1. CIL을 내보냅니다.

이미 설명한 바와 같이 기업의 보안 정책 상 특정 컴퓨터나 사용자를 식별할 수 있는 정보는 고립된 실험실 외부로 유출되어서는 안됩니다. 따라서 이런 유형의 데이터는 핵심 네트워크 VAMT 호스트로 전송할 CIL 파일에서는 제외해야 합니다.

* 1. VAMT 트리 보기 또는 목록 보기 창에서 MAK를 성공적으로 수신한 그룹 또는 개별 컴퓨터를 선택합니다.
  2. 선택한 그룹이나 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **컴퓨터 내보내기**를 클릭하여 **컴퓨터 정보 목록 저장** 대화 상자를 표시합니다.
  3. **민감한 환경 데이터 제외**를 선택합니다.
  4. **찾아보기**를 클릭하여 **다른 이름으로 저장** 대화 상자를 표시합니다.
  5. 디렉터리를 선택한 후, *IsolatedLabGroupSecureExport.CIL.*과 같이 CIL 파일 이름을 입력합니다.
  6. **저장**을 클릭합니다.
  7. IsolatedLabGroupSecureExport.CIL 파일을 이동식 미디어(디스크 드라이브, CD/DVD 또는 USB 플래시 드라이브[UFD])에 복사합니다.

**참고**   **민감한 환경 데이터 제외**확인란을 선택하면 PII(개인 식별이 가능한 정보)가 CIL에 저장되지 않습니다. 따라서 CIL을 이 VAMT 호스트와 전체가 저장된 CIL 파일로 다시 가져와야 Microsoft에 요청한 CID를 고립된 실험실 그룹 내의 컴퓨터에 올바르게 할당할 수 있습니다.

1. 인터넷을 액세스할 수 있는 VAMT 호스트에서 CIL을 가져오기
   1. 이동식 미디어에서 IsolatedLabGroupSecureExport.CIL을 인터넷을 사용할 수 있는 VAMT 호스트의 드라이브로 복사합니다.
   2. VAMT 콘솔을 엽니다.
   3. **파일** 메뉴에서 **가져오기**를 클릭하여 **컴퓨터 정보 목록 열기** 대화 상자를 엽니다.
   4. **IsolatedLabGroupSecureExport.CIL**을 찾아 선택한 후 **열기**를 클릭하여 CIL을 VAMT로 로드합니다.
   5. 컴퓨터, 그룹, 작업 그룹 이름이 표시되지 않음을 확인합니다.
2. Microsoft에 CDI를 요청합니다.
   1. 가져온 컴퓨터를 마우스 오른쪽 단추로 클릭한 후 **MAK 프록시 정품 인증**을 클릭하여 **MAK 프록시 정품 인증** 대화 상자를 엽니다.
   2. **MAK 설치(기존 덮어쓰기)**확인란 선택을 취소합니다.
   3. **Microsoft에서 확인 ID 가져오기** 확인란 선택을 취소합니다.
   4. 이 VAMT 호스트가 선택한 컴퓨터와 같은 네트워크에 있지 않으므로 **확인 ID 적용 후 정품 인증** 확인란 선택을 취소합니다.
   5. **확인**을 클릭합니다.

VAMT는 Microsoft에 접속하여 CID를 수집하는 동안 **확인 ID 온라인 획득 중**이라는 대화 상자를 표시합니다.

1. 인터넷이 연결된 VAMT 호스트에서 CIL을 내보냅니다.
   1. 모든 컴퓨터에 대한 CID를 가져온 후 CIL 파일을 저장합니다. VAMT 콘솔에서 오른쪽으로 스크롤한 후 **PendingCID** 열에 값이 있는지 확인합니다.
   2. **파일** 메뉴에서 **다른 이름으로 저장**을 클릭한 후*IsolatedLabGroupSecureExportwithCID.CIL.*과 같이 파일의 새 이름을 입력합니다.
   3. 업데이트된 IsolatedLabGroupSecureExportwithCID.CIL 파일을 이동식 미디어(디스크 드라이브, CD/DVD 또는 UFD)에 복사합니다.
2. 고립된 실험실 내의 원래 VAMT 호스트로 CIL을 가져옵니다.
   1. 이동식 미디어에서 IsolatedLabGroupSecureExportwithCID.CIL을 고립된 실험실에 있는 VAMT 호스트의 드라이브로 복사합니다.
   2. VAMT 콘솔을 엽니다.
   3. **파일** 메뉴에서 **열기**를 클릭하여 **컴퓨터 정보 목록 열기** 대화 상자를 표시합니다.
   4. IsolatedLabGroup.CIL을 찾아 선택한 후 **열기**를 클릭하여 CIL을 VAMT로 로드합니다.

이렇게 하면 이전에 검색한 컴퓨터와 해당 라이선스 상태가 컴퓨터 목록 보기 창에 표시됩니다.

* 1. **파일** 메뉴에서 **가져오기** 를 클릭한 후 CID((IsolatedLabGroupSecureExportwithCID.CIL)가 포함된 파일을 찾습니다.

이렇게 하면 CID를 컴퓨터의 IID에 일치시키는 병합 프로세스가 시작됩니다.

* 1. **파일** 메뉴에서 **저장**을 클릭한 후 해당 CID와 IID를 연결하는 이 파일을 저장할 파일 이름을 *IsolatedLabGroupwithCID.CIL*와 같이 입력합니다.

**중요**   이 파일은 재이미징 시나리오에서 매우 중요하게 사용되므로 저장해야 합니다. 이 파일을 백업하고 덮어 쓰이지 않도록 해야 합니다.

1. CID를 적용한 후 고립된 실험실 컴퓨터를 정품 인증합니다.
   1. 트리 보기 창에서 고립된 실험실 그룹을 마우스 오른쪽 단추로 클릭한 후 **MAK 프록시 정품 인증** 을 클릭하여 **MAK 프록시 정품 인증** 대화 상자를 엽니다.
   2. 선택한 컴퓨터에 이미 MAK가 설치되어 있으므로 **MAK 설치(기존 덮어쓰기)** 확인란 선택을 취소합니다.
   3. **Microsoft에서 확인 ID 가져오기** 확인란 선택을 취소합니다.
   4. **확인 ID 적용 후 정품 인증** 확인란을 선택한 VAMT가 해당 CID를 설치하여 선택한 컴퓨터를 정품 인증하도록 만듭니다.
   5. **확인**을 클릭합니다.

VAMT는 선택한 컴퓨터의 CID를 설치하는 동안 **확인 ID 할당 중**이라는 대화 상자를 표시합니다.

1. 또는 고립된 실험실의 재이미징 컴퓨터를 정품 인증합니다.

고립된 실험실의 컴퓨터가 재이미징되어 있지만 기본 하드웨어가 변경되지 않은 경우 VAMT는 IsolatedLabGroupwithCID.CIL 파일을 사용하여 컴퓨터를 정품 인증할 수 있습니다.

* 1. 이전과 같은 컴퓨터 이름으로 각 컴퓨터에 Windows를 재배포합니다.
  2. 로컬(작업 그룹) VAMT 호스트에서 VAMT 콘솔을 엽니다.
  3. **파일** 메뉴에서 **열기**를 클릭한 후 IsolatedLabGroupwithCID.CIL 파일을 선택합니다.
  4. 트리 보기 창에서 **고립된 실험실** 그룹을 마우스 오른쪽 단추로 클릭한 후 **확인 ID 재적용**을 클릭하여 **MAK 프록시 정품 재인증** 대화 상자를 표시합니다.
  5. **MAK 설치(기존 덮어쓰기)** 확인란이 선택된 상태에서, 이전에 사용한 MAK가 목록에서 선택된 상태인지 확인합니다.
  6. IsolatedLabGroupwithCID.CIL 파일의 저장된 CID를 재적용하려면 **확인 ID 재적용 후 재인증** 확인란이 선택된 상태를 그대로 유지합니다.
  7. 최초 MAK 프록시 정품 인증 이후 하드웨어가 변경되지 않았고 컴퓨터를 재인증하기 위해 같은 MAK를 사용하고 있는 경우 **정확한 IID 일치 요구** 확인란을 선택한 상태 그대로 유지합니다.

하드웨어는 변경되었지만 이전에 저장한 CID를 사용하여 정품 재인증을 시도하기 위해 계속 VAMT를 사용하려는 경우 이 확인란 선택을 취소합니다. 이런 시나리오의 경우 Windows가 제대로 정품 인증되지 않을 수 있습니다.

* 1. 현재 사용 중인 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용** 확인란을 선택합니다.
  2. **확인**을 클릭합니다.

VAMT는 MAK를 고립된 실험실 그룹에 적용하는 동안 **제품 키 할당 중**이라는 대화 상자를 표시합니다.

VAMT는 선택한 컴퓨터의 CID를 설치하는 동안 **확인 ID 할당 중**이라는 대화 상자를 표시합니다.

**참고** **MAK 설치(기존 덮어쓰기)** 확인란을 선택하면 MAK가 강제로 설치됩니다. 따라서 이런 경우에는 주의해야 합니다. Windows Vista SP1 이전 버전이 30일 이상 설치되어 있고 초기 유예 기간이 만료된 경우 다음 로그온 전에 정품 인증이 성공적으로 완료되지 않으면 컴퓨터가 RFM으로 전환됩니다. 그러나 올바르게 구성된 원격 컴퓨터에서 네트워크에 액세스할 수 있는 경우에는 VAMT를 사용하여 RFM로부터 이들 컴퓨터를 복원할 수 있습니다. RFM은 Windows Vista의 SP1 이전 버전에만 적용됩니다. Windows Vista(SP1 이상), Windows 7, Windows Server 2008 및 Windows Server 2008 R2는 RFM으로 전환되지 않습니다.

### KMS 정품 인증을 위한 VAMT 지원

이 시나리오에서 VAMT는 핵심 네트워크 또는 고립된 실험실 컴퓨터에서 KMS 클라이언트 키를 설치하고 정품 인증하기 위해 사용됩니다. 아래 설명된 절차에서는 VAMT가 설치되었고 CIL에 컴퓨터가 추가되었다고 가정합니다. 이 작업들은 시나리오1(핵심 네트워크용)과 시나리오2(독립된 실험실 작업 그룹용)에서 모두 단계1–4로 설명됩니다.

1. VAMT 콘솔을 엽니다.
2. 트리 보기 창에서 그룹을 클릭하거나 목록 보기 창에서 개별 컴퓨터를 선택하여 정품 인증할 컴퓨터를 선택합니다.
3. 선택한 그룹 또는 컴퓨터를 마우스 오른쪽 단추로 클린한 후 **KMS 정품 인증 구성**을 클릭하여 **KMS 구성** 대화 상자를 표시합니다.
4. **KMS 클라이언트 키 설치(기존 키 덮어쓰기)**를 선택하여 VAMT가 KMS 클라이언트 키를 클라이언트 컴퓨터에 설치하도록 지시합니다.
5. 다음 중 적합한 정품 인증 옵션을 선택합니다.

* **DNS를 사용하여 KMS 호스트를 자동 검색합니다.** VAMT는 우선 대상 컴퓨터에서 이전에 구성된 모든 KMS 호스트를 삭제한 다음 컴퓨터가 DNS를 쿼리하여 KMS 호스트를 찾고 정품 인증을 시도하도록 지시합니다.
* **특정 KMS 호스트 및 포트를 사용합니다.** VAMT는 대상 컴퓨터에 지정된 KMS 호스트 이름과 포트를 설정한 다음 컴퓨터가 그 특정 KMS 호스트를 사용하여 정품 인증을 시도하도록 지시합니다.

1. 현재 사용 중인 것과 다른 관리자 자격 증명이 있어야 컴퓨터 정품 인증이 가능한 경우 **다른 자격 증명 사용**을 선택한 후 **확인**을 클릭합니다.

VAMT는 **제품 키 할당** 대화 상자를 표시한 후 요청한 작업이 완료될 때까지 **컴퓨터 정품 인증 중** 대화 상자를 표시합니다. **대체 자격 증명 사용** 확인란을 선택한 경우 이러한 대화 상자가 나타나기 전에 자격 증명을 입력하라는 메시지가 표시됩니다.

### KMS를 MAK 정품 인증으로 변환

Windows 7 및 Windows Server 2008 R2는 KMS 클라이언트로 자동 설치됩니다. KMS 클라이언트를 MAK 정품 인증으로 변환하려면 MAK를 설치하십시오. MAK는 운영 체제 설치 중이나 설치 후 언제든지 설치할 수 있습니다.

MAK 키는 Windows 7 및 Windows Server 2008 R2의 참조 이미지에 설치하여 이 이미지로부터의 모든 설치가 기본 KMS 정품 인증 대신 MAK 정품 인증을 사용하도록 할 수 있습니다. 그러면 자동 설치 파일에서 MAK를 지정하는 불편함이 해소됩니다.

#### 운영 체제 설치 중 MAK 설치

관리자는 Windows 7 또는 Windows Server 2008 R2를 처음 설치할 때 무인 설치(Unattend.xml) 파일에 MAK를 포함시켜 KMS 클라이언트를 MAK 클라이언트로 변환할 수 있습니다. Unattend.xml 파일을 Setup.exe 또는 WDS(Windows 배포 서비스)와 함께 사용할 수 있습니다. 자세한 내용은 <http://go.microsoft.com/fwlink/?LinkId=136976>에서 Windows AIK의 Windows 무인 설치 참조 도움말 파일을 참조하십시오.

**참고**   MAK는 Unattend.xml 파일에 암호화되지 않은 텍스트로 저장됩니다. 무인 설치 중 Unattend.xml 또는 Autounattend.xml 파일이 대상 컴퓨터의 %SystemRoot%\Panther 폴더에 복사됩니다. 그러나, 설치 과정이 끝나면 설치 프로그램이 이를 “SENSITIVE\*DATA\*DELETEDD”로 대체합니다.

#### 운영 체제 설치 후 MAK 설치

제어창 시스템 항목을 사용하거나 Slmgr.vbs 스크립트를 실행하여 MAK 정품 인증을 사용하도록 Windows 7 또는 Windows Server 2008 R2 볼륨 버전을 구성할 수 있습니다.

* 시스템 응용 프로그램을 이용하여 MAK를 설치하려면 **제품 키 변경** 링크를 클릭한 다음 **정품 인증을 받으려면 제품 키를 변경하십시오.** 대화 상자에 MAK를 입력합니다.
* Slmgr.vbs를 사용하여 MAK를 설치하려면 명령 프롬프트에서 다음 명령을 실행하십시오.

slmgr.vbs /ipk <MultipleActivationKey>

여기서 MultipleActivationKey는 MAK입니다.

사용자가 UI(사용자 인터페이스)를 사용하여 MAK를 설치하는 경우, MAK 클라이언트는 인터넷을 통해 한 번만 자체 정품 인증을 시도합니다. 사용자가 Slmgr.vbs 스크립트를 사용하여 MAK 키를 설치하는 경우, MAK 클라이언트는 자동으로 정품 인증을 시도하지 않습니다. 사용자는 **Slmgr.vbs /ato**를 사용하여 인터넷을 통해 MAK를 직접 정품 인증할 수 있습니다.

# 제품에 대한 KMS 호스트 키

표 7에서는 각 KMS가 정품 인증할 수 있는 제품을 표시합니다.

표 7. KMS 호스트 키와 그들이 정품 인증하는 제품

| **볼륨 제품 그룹** | **Windows 제품** | **키 유형** | **키 유형에 의해 정품 인증되는 제품** |
| --- | --- | --- | --- |
| Windows Vista | Windows Vista Business  Windows Vista Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise |
| Windows 7 | Windows 7 Professional  Windows 7 Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise  Windows 7 Professional  Windows 7 Enterprise |
| Windows Server 2008 R2  서버 그룹 A | Windows Web Server® 2008 R2  Windows Server 2008 R2 HPC Edition  Windows HPC Server 2008 R2 | KMS\_A | Windows Server 2008 R2 그룹 A  Windows Server 2008 그룹 A  Windows Vista 볼륨 버전  Windows 7 볼륨 버전 |
| Windows Server 2008 R2  서버 그룹 B | Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise | KMS\_B | Windows Server 2008 R2 그룹 A  Windows Server 2008 그룹 A  Windows Server 2008 R2 그룹 B  Windows Server 2008 그룹 B  Windows Vista 볼륨 버전  Windows 7 볼륨 버전 |
| Windows Server 2008 R2  서버 그룹 C | Windows Server 2008 R2 Datacenter  Itanium 기반 시스템용 Windows Server 2008 R2 | KMS\_C | Windows Server 2008 R2 그룹 A  Windows Server 2008 그룹 A  Windows Server 2008 R2 그룹 B  Windows Server 2008 그룹 B  Windows Server 2008 R2 그룹 C  Windows Server 2008 그룹 C  Windows Vista 볼륨 버전  Windows 7 볼륨 버전 |
| Windows Server 2008 R2 KMS 키는 Windows Server 2008과 동일한 계층(그룹 A, B, C)을 따르며 Windows Server 2008 데이터센터(Hyper-V™ 제외), Windows Server 2008 Enterprise(Hyper-V 제외) 및 Windows Server 2008 Standard(Hyper-V 제외)를 추가합니다. 가장 유의해야 할 차이점은 Windows Server 2008 R2 KMS 키가 KMS 호스트를 정품 인증하는 데 사용될 수 있고 이 호스트는 다시 Windows Server 2008, Windows 7 및 Windows Vista를 정품 인증한다는 점입니다.  Windows Server 2008 및 Windows Vista 키는 Windows 7 또는 Windows Server 2008 R2 시스템을 정품 인증할 수 없습니다. | | | |

# 정품 인증 정책 값

표 8은 Windows 7 및 Windows Server 2008 R2에 대한 정책 값을 나열합니다.

표 8. Windows 7 및 Windows Server 2008 R2 정책 값

| **요소** | **클라이언트 값** | **서버 값** | **범위** |
| --- | --- | --- | --- |
| 라이선스 초기화 한계 | 3 | 3 | 구성 불가 |
| KMS 클라이언트 최소 임계 값 | 25 | 5 | 구성 불가 |
| KMS 정품 인증 기간 | 180일 | 180일 | 구성 불가 |
| KMS 호스트 수신 포트 | 1688 | 1688 | 열린 모든 TCP 포트 |
| OOB 유예 | 30일 | 30일 | 구성 불가 |
| OOT 유예 | 30일 | 30일 | 구성 불가 |
| KMS 클라이언트 정품 재인증(분 단위) | 10,080분  (7일—기본) | 10,080분  (7일—기본) | 15–43,200분  (30일—기본) |
| 자동 KMS 재시도 간격—KMS 정품 인증 실패 시 발생 | 120분 | 120분 | 15–43,200분  (120분—기본) |

# KMS 클라이언트 설치 키

기본적으로, Windows 7 및 Windows Server 2008 R2 운영 체제는 정품 인증에 KMS를 사용합니다. 볼륨 설치에서는 시스템을 KMS 클라이언트로 만들어주는 설치 키가 기본적으로 설치됩니다. 컴퓨터를 KMS 호스트, MAK 또는 Windows의 소매 버전에서 KMS 클라이언트로 변환하는 경우 **slmgr /ipk<설치 키>**를 사용하여 표 9에서 해당 설치 키(GVLK)를 설치합니다.

표 9. KMS 클라이언트 설치 키

| **플랫폼** | **운영 체제 버전** | **제품 키** |
| --- | --- | --- |
| **Windows 7 및 Windows Server 2008 R2** | | |
| 클라이언트 | Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| 클라이언트 | Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| 클라이언트 | Windows 7 Professional E | W82YF-2Q76Y-63HXB-FGJG9-GF7QX |
| 클라이언트 | Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| 클라이언트 | Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| 클라이언트 | Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| 서버 | Windows Server 2008 R2 Web | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |
| 서버 | Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| 서버 | Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| 서버 | Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| 서버 | Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| 서버 | Itanium 기반 시스템용 Windows Server 2008 R2 | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| **Windows Vista 및 Windows Server 2008** | | |
| 클라이언트 | Windows Vista Business | YFKBB-PQJJV-G996G-VWGXY-2V3X8 |
| 클라이언트 | Windows Vista Business N | HMBQG-8H2RH-C77VX-27R82-VMQBT |
| 클라이언트 | Windows Vista Enterprise | VKK3X-68KWM-X2YGT-QR4M6-4BWMV |
| 클라이언트 | Windows Vista Enterprise N | VTC42-BM838-43QHV-84HX6-XJXKV |
| 서버 | Windows Web Server 2008 | WYR28-R7TFJ-3X2YQ-YCY4H-M249D |
| 서버 | Windows Server 2008 Standard | TM24T-X9RMF-VWXK6-X8JC9-BFGM2 |
| 서버 | Windows Server 2008 Standard(Hyper-V 제외) | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ |
| 서버 | Windows Server 2008 Enterprise | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V |
| 서버 | Windows Server 2008 Enterprise(Hyper-V 제외) | 39BXF-X8Q23-P2WWT-38T2F-G3FPG |
| 서버 | Windows Server 2008 Datacenter | 7M67G-PC374-GR742-YH8V4-TCBY3 |
| 서버 | Windows Server 2008 Datacenter(Hyper-V 제외) | 22XQ2-VRXRG-P8D42-K34TD-G3QQC |
| 서버 | Itanium 기반 시스템용 Windows Server 2008 | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK |

# 정품 인증 오류 코드

표 10에서는 Windows 7 및 Windows Server 2008 R2 운영 체제의 볼륨 버전을 정품 인증할 때 발생하는 문제를 해결할 때 유용하게 이용할 수 있습니다.

표 10. 오류 코드 및 설명

| **오류 코드** | **오류 메시지** | **정품 인증 유형** | **가능한 원인** | **문제 해결 단계** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | 정품 인증 서버에서 지정한 제품 키가 잘못되었다고 확인했습니다. | MAK | 입력된 MAK가 유효하지 않습니다. | 키가 Microsoft에서 제공한 MAK인지 확인하십시오.  MAK의 유효성을 확인하려면 [Microsoft 정품 인증 콜 센터](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)로 문의하십시오. |
| 0xC004C003 | 정품 인증 서버에서 지정한 제품 키가 차단되었다고 확인했습니다. | MAK | 정품 인증 서버에서 MAK가 차단되었습니다. | [Microsoft 정품 인증 콜 센터](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)로 연락하여 새 MAK를 받고 시스템을 설치/정품 인증하십시오. |
| 0xC004C008 | 정품 인증 서버에서 지정한 제품 키를 사용할 수 없다고 확인했습니다. | KMS | KMS 키가 정품 인증 한계를 초과했습니다. | KMS 호스트 키는 6대의 컴퓨터에서 최대 10회 정품 인증합니다. 추가 정품 인증이 필요하면 [Microsoft 정품 인증 콜 센터](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)로 문의하십시오. |
| 0xC004C020 | 정품 인증 서버에서 MAK(복수 정품 인증 키)가 제한을 초과했다고 보고되었습니다. | MAK | MAK가 정품 인증 한계를 초과했습니다. | 기본적으로 MAK는 정해진 수까지만 정품 인증합니다. [Microsoft 정품 인증 콜 센터](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)에 문의하십시오. |
| 0xC004C021 | 정품 인증 서버에서 MAK(복수 정품 인증) 연장 제한이 초과했다고 보고되었습니다. | MAK | MAK가 정품 인증 한계를 초과했습니다. | 기본적으로 MAK는 정해진 수까지만 정품 인증합니다. [Microsoft 정품 인증 콜 센터](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)에 문의하십시오. |
| 0xC004F009 | 소프트웨어 보호 서비스에서 유예 기간이 만료했다고 보고되었습니다. | MAK | 시스템이 정품 인증되기 전에 유예 기간이 만료되었습니다. 시스템은 이제 알림 상태에 있습니다. | “” 단원을 참조하십시오. |
| 0xC004F00F | 소프트웨어 라이선스 서버에서 하드웨어 ID 바인딩이 허용 수준을 벗어났다고 보고했습니다. | MAK/KMS 클라이언트/KMS 호스트 | 시스템에서 하드웨어가 변경되었거나 드라이버가 업데이트되었습니다. | **MAK:**온라인 또는 전화 정품 인증을 사용하여 OOT 유예 기간 동안 시스템을 정품 재인증하십시오.  **KMS:**재시작하거나 **slmgr.vbs /ato**를 실행하십시오. |
| 0xC004F014 | 소프트웨어 보호 서비스에서 제품 키를 사용할 수 없다고 보고했습니다. | MAK/KMS 클라이언트 | 시스템에 설치된 제품 키가 없습니다. | MAK 제품 키를 설치하거나 설치 미디어의 \sources\pid.txt에 있는 KMS 설치 키를 설치하십시오. |
| 0xC004F02C | 소프트웨어 보호 서비스에서 오프라인 정품 인증 데이터 형식이 잘못되었다고 보고했습니다. | MAK/KMS 클라이언트 | 시스템이 전화 정품 인증 기간 중 입력된 데이터가 유효하지 않은 것으로 확인했습니다. | CID가 정확하게 입력되었는지 확인하십시오. |
| 0xC004F035 | 이 오류 코드는 "소프트웨어 보호 서비스에서 볼륨 라이선스 제품 키를 사용하여 컴퓨터의 정품을 인증할 수 없다고 보고했습니다."와 동일합니다. 이 오류 텍스트는 정확하지만 모호합니다.  이 오류는 컴퓨터에 BIOS의 Windows 마커가 없음을 나타냅니다 – OEM 시스템에 제공되어 유효한 Windows 버전의 컴퓨터임을 나타내며 이것은 KMS 클라이언트 정품 인증을 위한 요구 사항입니다.  오류: 잘못된 볼륨 라이선스 키입니다.  정품 인증을 위해서는 제품 키를 유효한 MAK(복수 정품 인증 키) 또는 소매 키로 변경해야 합니다.  적격한 운영 체제 라이선스와 함께 볼륨 라이선스 Windows 7 업그레이드 라이선스 또는 소매 소스로부터 Windows 7에 대한 완전한 라이선스를 가지고 있어야 합니다.  ANY OTHER INSTALLATION OF THIS SOFTWARE IS IN VIOLATION OF YOUR AGREEMENT AND APPLICABLE COPYRIGHT LAW. | KMS 클라이언트/KMS 호스트 | Windows 7 볼륨 버전이 업그레이드 전용으로 라이선스 체결되었습니다. 자격이 있는 OS가 설치되지 않은 컴퓨터에는 볼륨 OS를 설치할 수 없습니다. | 자격이 있는 Microsoft 운영 체제 버전을 설치한 다음 MAK를 사용하여 정품 인증하십시오. |
| 0xC004F038 | 소프트웨어 보호 서비스에서 컴퓨터를 정품 인증할 수 없다고 보고되었습니다. KMS(키 관리 서비스)에서 보고된 개수가 부족합니다. 시스템 관리자에게 문의하십시오. | KMS 클라이언트 | KMS 호스트에서 정품 인증 수가 충분하지 않습니다. KMS 정품 인증 수는 Windows Server의 경우 5개 이상, Windows 클라이언트의 경우 25개 이상이어야 합니다. | KMS 클라이언트를 정품 인증하기 위해서는 KMS 풀에 더 많은 컴퓨터가 필요합니다. KMS 호스트에서 현재 정품 인증 수를 확인하려면 **Slmgr.vbs /dli**를 실행하십시오. |
| 0xC004F039 | 소프트웨어 보호 서비스에서 컴퓨터를 정품 인증할 수 없다고 보고되었습니다. KMS(키 관리 서비스)를 사용하고 있지 않습니다. | KMS 클라이언트 | 이 오류는 KMS 요청에 응답이 없는 경우에 발생합니다. | KMS 호스트와 클라이언트 사이의 네트워크 연결 문제를 해결하십시오. TCP포트 1688(기본 설정)이 방화벽에 의해 차단되거나 다른 식으로 필터링되지 않았는지 확인하십시오. |
| 0xC004F041 | 소프트웨어 보호 서비스에서 KMS(키 관리 서버)가 정품 인증되지 않았음을 확인했습니다. KMS를 활성화해야 합니다. | KMS 클라이언트 | KMS 호스트가 정품 인증되지 않았습니다. | 온라인이나 전화 정품 인증을 이용하여 KMS 호스트를 정품 인증하십시오. |
| 0xC004F042 | 소프트웨어 보호 서비스에서 지정된 KMS(키 관리 서비스)를 사용할 수 없음이 확인되었습니다. | KMS 클라이언트 | KMS 클라이언트와 KMS 호스트 불일치 | 이 오류는 KMS 클라이언트가 클라이언트 소프트웨어를 정품 인증할 수 없는 KMS 호스트에 연결할 때 발생합니다. 이 오류는 예를 들어 응용 프로그램과 운영 체제별 KMS 호스트를 포함하는 혼합 환경에서 흔히 발생할 수 있습니다. |
| 0xC004F050 | 소프트웨어 보호 서비스에서 제품 키가 잘못되었다고 보고했습니다. | KMS, KMS 클라이언트, MAK | KMS 키를 잘못 입력하거나 배포된 OS 버전에 베타 키를 입력하는 경우에 발생할 수 있습니다. | 해당 Windows 버전에 적합한 KMS 키를 설치하십시오. 철자가 맞는지 확인하십시오. 키를 복사하여 붙여 넣은 경우라면 키의 대시가 em- 대시로 대체되지 않았는지 확인하십시오. |
| 0xC004F051 | 소프트웨어 보호 서비스에서 제품 키가 차단되었다고 보고했습니다. | MAK/KMS | 정품 인증 서버에서 제품 키가 Microsoft에 의해 차단되었습니다. | 새 MAK/KMS 키를 얻어 시스템에 설치하고 정품 인증하십시오. |
| 0xC004F064 | 소프트웨어 보호 서비스에서 비정품 유예 기간이 만료되었다고 보고했습니다. | MAK | Windows 정품 인증 도구(WAT)에서 시스템이 정품이 아니라고 확인했습니다. | 볼륨 정품 인증 운영 가이드를 참조하십시오. |
| 0xC004F065 | 소프트웨어 보호 서비스에서 응용 프로그램이 유효한 비정품 기간 내에 실행되고 있다고 보고했습니다. | MAK/KMS 클라이언트 | Windows 정품 인증 도구에서 시스템이 정품이 아니라고 확인했습니다. 시스템은 비정품 유예 기간 동안 계속해서 실행됩니다. | 정품 키를 얻어 설치하고 유예 기간 중 시스템을 정품 인증하십시오. 그렇지 않으면 시스템은 유예 기간이 끝나면 알림 상태로 들어갑니다. |
| 0xC004F06C | 소프트웨어 보호 서비스에서 컴퓨터를 정품 인증할 수 없다고 보고되었습니다. KMS(키 관리 서비스)는 요청 타임스탬프가 잘못되었음을 확인했습니다. | KMS 클라이언트 | 클라이언트 컴퓨터의 시스템 시간이 KMS 호스트의 시간과 크게 다릅니다. | 여러 가지 이유로 시스템과 네트워크 보안을 위해 시간 동기화가 중요합니다. KMS와 동기화되도록 클라이언트의 시스템 시간을 변경하여 이 문제를 해결하십시오. 시간 동기화를 위해 네트워크 시간 프로토콜(NTP) 시간 소스 또는 Active Directory 도메인 서비스를 사용하는 것이 좋습니다. 이 문제는 UTP 시간을 사용하고 시간대 선택과 무관합니다. |
| 0x80070005 | 액세스가 거부되었습니다. 요청된 작업을 수행하려면 높은 권한이 필요합니다. | KMS 클라이언트/MAK/KMS 호스트 | UAC(사용자 계정 제어)는 승격되지 않은 명령 프롬프트에서 정품 인증 프로세스가 실행되지 않도록 합니다. | 승격된 명령 프롬프트에서 slmgr.vbs를 실행하십시오. cmd.exe를 마우스 오른쪽 단추로 클릭하고 관리자 권한으로 실행을 클릭하십시오. |
| 0x8007232A | DNS 서버 오류입니다. | KMS 호스트 | 시스템에 네트워크 또는 DNS 문제가 있습니다. | 네트워크 및 DNS 문제를 해결하십시오. |
| 0x8007232B | DNS 이름이 없습니다. | KMS 클라이언트 | KMS 클라이언트가 DNS에서 KMS SRV RR를 찾을 수 없습니다.  KMS 호스트가 네트워크에 없는 경우 MAK를 설치해야 합니다. | KMS 호스트가 설치되었고 DNS 게시를 사용할 수 있는지(기본 설정) 확인하십시오.  DNS를 사용할 수 없는 경우 **slmgr.vbs /skms <*kms\_host\_name>***를 사용하여 KMS 클라이언트를 KMS 호스트에 지정시키십시오.  선택적으로 MAK를 얻어 설치한 다음 시스템을 정품 인증하십시오.  마지막으로 DNS 문제를 해결하십시오. |
| 0x800706BA | RPC 서버를 사용할 수 없습니다. | KMS 클라이언트 | KMS 호스트에 방화벽 설정이 구성되지 않았거나 DNS SRV 레코드가 부실합니다. | KMS 호스트 시스템에서 키 관리 서비스 방화벽 예외를 사용할 수 있는지 확인하십시오.  SRV 레코드가 유효한 KMS 호스트를 가리키고 있는지 확인하십시오.  네트워크 연결 문제를 해결하십시오. |
| 0x8007251D | DNS 쿼리에 대한 레코드가 없습니다. | KMS 클라이언트 | KMS 클라이언트가 DNS에서 KMS SRV RR를 찾을 수 없습니다. | 네트워크 연결과 DNS 문제를 해결하십시오. |
| 0xC004F074 | 소프트웨어 보호 서비스에서 컴퓨터를 정품 인증할 수 없다고 보고되었습니다. 키 관리 서비스(KMS)를 연결할 수 없습니다. 추가 정보를 보시려면 응용 프로그램 이벤트 로그를 참조하십시오. | KMS 클라이언트 | 모든 KMS 호스트 시스템이 오류를 반환합니다. | 정품 인증 시도와 관련된 각 이벤트 ID 12288에서 오류 문제를 해결하십시오. |

# Windows 이벤트 로그

표 11은 KMS가 Windows 이벤트 로그에 기록하는 이벤트를 나열합니다. 다음은 각 이벤트에 대한 공통 데이터를 설명합니다.

* **모든 로그 파일 이름(12290 제외):** Windows 로그\응용 프로그램
* **로그 파일 이름 12290:** 응용 프로그램 및 서비스 로그/키 관리 서비스
* **이벤트 공급자 이름:** Microsoft-Windows-Security-Licensing-SLC
* **소스 이름:**소프트웨어 보호 서비스

표 11. Windows 이벤트 로그에 기록되는 KMS 이벤트

| **이벤트 ID** | **Logged by** | **설명** | | **메시지** | **매개 변수**  **쉼표로 구분된 문자열에 포함된 필드** | | **예** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  | **이름** | **설명** |  |
| 12288 | 클라이언트 | 요청 생성 실패 또는 RPC 제출 후(클라이언트) | | 클라이언트가 정품 인증 요청을 키 관리 서비스 컴퓨터로 보냈습니다. %nInfo:%n%1 | HRESULT | 반환 코드 | 0x0 |
|  | | | | | Status | 플래그(참고 1) | 0x8 |
| Server:Port | 이름:포트 | kms01.contoso.com:1688 |
| CMID | 클라이언트 컴퓨터 ID | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be, |
| Client Time | 요청 타임스탬프 | 2006/1/14 2:30, |
| VM Info | Unused | 1 |
| Licensing Status | 라이선스 상태  0 – 라이선스 없음  1 – 라이선스 취득(정품 인증됨)  2 - OOB 유예 기간  3 - OOT 유예 기간  4 – 비정품 유예 기간  5 – 알림 기간  6 – 유예 연장 기간 | 2 |
|  | | | | | Time to Expiration | 남은 시간(분) | 40123 |
| ActID | 정품 인증 ID – 라이선스 확인 | cf67834d-db4a-402c-ab1f-2c134f02b700, |
| N-Policy | 최소 클라이언트 수 정품 인증 필요 | 25 |
| 12289 | 클라이언트 | | KMS 응답 정품 확인 후(클라이언트) | 클라이언트가 키 관리 서비스 컴퓨터로부터 정품 인증 응답을 처리했습니다. %nInfo:%n%1 | HRESULT | 반환 코드 | 0x0 |
|  | | | | | Status | 플래그(참고 1) | 0x4000008 |
| fBound | 정품 인증된 플래그 | 0 |
| Unused | 사용 안 함 – 무시 | 0 |
| Count | 현재 KMS 정품 인증 수 | 4 |
| Activation Interval | 정품 인증되지 않은 경우 요청 간격(분) | 120 |
| Renewal Interval | 정품 인증된 경우 요청 간격(분) | 10080 |
| Client Time | 요청 타임스탬프 | 1/14/2006 2:30 |
| 12290 | KMS | 각 요청에 대한 KMS 서버 쪽 로그 | | 정품 인증 요청이 처리되었습니다.%nInfo:%n%1 | HRESULT | 반환 코드 | 0x0 |
|  | | | | | N-Policy | 최소 수의 클라이언트 제품을 정품 인증해야 함 | 25 |
| Machine | 클라이언트 컴퓨터 이름 | kms03.site5.contoso.com |
| CMID | 클라이언트 컴퓨터 ID | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | | Client Time | 요청 타임스탬프 | 2006/1/14 22:36 |
| VM Info | 클라이언트 OS가 가상 컴퓨터에서 실행 중 | 1 |
| Licensing Status | 라이선스 상태  0 – 라이선스 없음  1 – 라이선스 취득(정품 인증됨)  2 - OOB 유예 기간  3 - OOT 유예 기간  4 – 비정품 유예 기간  5 – 알림 기간  6 – 유예 연장 기간 | 2 |
| Time to Expiration | 남은 시간(분) | 40123 |
| ActID | 정품 인증 ID – 라이선스 확인 | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | KMS 초기화 실패 | | 볼륨 라이선스 클라이언트가 키 관리 서비스 갱신 타이머를 초기화하지 못했습니다.%nInfo:%n%1 | HRESULT | 반환 코드 |  |
| 12292 | KMS | 갱신 타이머 초기화 실패 | | KMS(키 관리 서비스)가 갱신 타이머를 초기화하지 못했습니다.%nInfo:%n%1 | HRESULT | 반환 코드 |  |
| 12293 | KMS | DNS RR 게시 실패 | | '%2' 도메인의 DNS로 KMS(키 관리 서비스)를 게시하지 못했습니다.%nInfo:%n%1 | P1: HRESULT  P2: DNS 도메인 | P1: 반환 코드  P2: DNS 도메인 이름 | |
| 12294 | KMS | DNS RR 게시 성공 | | '%1' 도메인의 DNS로 KMS(키 관리 서비스)를 성공적으로 게시했습니다.%n | DNS 도메인 | DNS 도메인 이름 |  |

# WMI 속성 및 방법

표 12에서는 소프트웨어 보호 플랫폼을 위한 WMI 속성과 방법을 나열합니다. 소프트웨어 보호 플랫폼 속성은 %WinDir%\System32\wbem\sppwmi.mof 파일에 정의되어 있습니다.

표 12. 소프트웨어 보호 플랫폼 WMI 속성 및 방법

|  |  |  |  |
| --- | --- | --- | --- |
| **//속성 SoftwareLicensingService 클래스** | | | |
| **Version** | 소프트웨어 보호 서비스의 버전 | | |
| **KeyManagementServiceMachine** | KMS 호스트 이름 **SetKeyManagementServiceMachine**이 호출되지 않은 경우, Null을 반환합니다. | | |
| **KeyManagementServicePort** | KMS 정품 인증 요청을 보내기 위해 클라이언트에서 사용된 TCP 포트 **SetKeyManagementServicePort**가 호출되지 않은 경우, **0**을 반환합니다. | | |
| **IsKeyManagementServiceMachine** | 컴퓨터에서 KMS를 사용할 수 있는지 여부를 표시합니다. 거짓이면 **0**, 참이면 **1**. | | |
| **VLActivationInterval** | 클라이언트가 사용 허가되기 전 클라이언트가 KMS 호스트에 연결하는 분 단위 빈도 | | |
| **VLRenewalInterval** | 클라이언트가 사용 허가된 후 클라이언트가 KMS 호스트에 연결하는 분 단위 빈도 | | |
| **KeyManagementServiceCurrentCount** | KMS 호스트에서 현재 정품 인증된 KMS 클라이언트 수 **-1**은 호스트가 KMS로 사용되지 않았거나 어떠한 클라이언트 라이선스 요청도 받지 않았음을 나타냅니다. | | |
| **RequiredClientCount** | 볼륨 라이선스 사용을 위해 KMS 호스트에 연결하는 데 필요한 최소 클라이언트 수. | | |
| **PolicyCacheRefreshRequired** | 라이선스 정책 캐시를 업데이트해야 하는지 여부를 표시합니다. **0**=필요하지 않음, **1**=갱신 필요함. | | |
| **ClientMachineID** | KMS 호스트가 KMS 클라이언트를 식별할 수 있게 해주는 GUID(Globally Unique Identifier) 클라이언트는 KMS에 보내는 요청에 이것을 포함시킵니다. | | |
| **RemainingWindowsReArmCount** | 클라이언트를 성공적으로 다시 설치할 수 있는 남은 횟수 | | |
| **KeyManagementServiceListeningPort** | 정품 인증 요청을 수신하기 위해 KMS 호스트에서 사용하는 TCP 포트 | | |
| **KeyManagementServiceDnsPublishing** | KMS 호스트의 DNS 게시 상태를 표시합니다. **0**=해제, **1**=자동 게시 사용(기본 설정). | | |
| **KeyManagementServiceLowPriority** | KMS 서비스의 스레드 우선 순위 상태를 표시합니다. **0**=정상 우선 순위(기본 설정), **1**=낮은 우선 순위. | | |
| **KeyManagementServiceHostCaching** | KMS 호스트 이름 및 포트의 캐시 상태를 표시합니다. **0**=캐시 해제, **1**=캐시 사용(기본 설정). | | |
| **KeyManagementServiceUnlicensedRequests** | 라이선스 상태가 0(라이선스 미취득)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceLicensedRequests** | 라이선스 상태가 1(라이선스 취득)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceOOBGraceRequests** | 라이선스 상태가 2(OOB유예)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceOOTGraceRequests** | 라이선스 상태가 3(OOT유예)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceNonGenuineGraceRequests** | 라이선스 상태가 4(비정품유예)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceNotificationRequests** | 라이선스 상태가 5(알림)인 클라이언트로부터 받은 KMS 요청 수 | | |
| **KeyManagementServiceTotalRequests** | 유효한 총 KMS 요청 수 | | |
| **KeyManagementServiceFailedRequests** | 유효하지 않은 KMS 요청 수 | | |
| **KeyManagementServiceActivationDisabled** | KMS를 통한 볼륨 정품 인증을 사용할 수 없는지 여부를 표시합니다. | | |
| **//방법 SoftwareLicensingProduct 클래스** | | | |
| **InstallProductKey** | | 제품 키를 설치합니다. | |
| **InstallLicense** | | 라이선스를 설치합니다. | |
| **InstallLicensePackage** | | 현재 제품에 대한 라이선스 패키지를 설치합니다. | |
| **SetKeyManagementServiceMachine** | | 볼륨 정품 인증에 사용할 KMS 호스트 이름을 지정합니다. | |
| **ClearKeyManagementServiceMachine** | | 이전에 구성된 KMS 호스트 이름을 삭제합니다. | |
| **SetKeyManagementServicePort** | | 클라이언트가 KMS 호스트 요청을 하기 위해 사용하는 TCP 포트 지정하지 않는 경우 포트 1688이 사용됩니다. | |
| **ClearKeyManagementServicePort** | | 이전에 지정된 모든 포트 번호를 삭제합니다. | |
| **SetVLActivationInterval** | | 클라이언트가 사용 허가되기 전 KMS 클라이언트가 KMS 호스트에 연결하는 분 단위 정품 인증 빈도. 빈도는 15이상 43,200이하이어야 합니다. 방법이 호출되고 컴퓨터가 KMS가 아닌 경우 오류가 반환됩니다. | |
| **SetVLRenewalInterval** | | 클라이언트가 사용 허가되기 전 KMS 클라이언트가 KMS 호스트에 연결하는 분 단위 갱신 빈도. 빈도는 15이상 43,200이하이어야 합니다. 방법이 호출되고 컴퓨터가 KMS가 아닌 경우 오류가 반환됩니다. | |
| **ClearProductKeyFromRegistry** | | 레지스트리에서 제품 키를 지웁니다. | |
| **AcquireGenuineTicket** | | 온라인 정품 인증을 수행합니다. 이 방법을 호출하면 컴퓨터의 정품 상태가 변경될 수 있습니다. | |
| **ReArmWindows** | | 컴퓨터의 라이선스 상태를 OOB 유예로 초기화합니다  (**LicenseStatus** 참조).  **참고**   변경 사항을 적용하려면 클라이언트를 다시 시작해야 합니다. | |
| **RefreshLicenseStatus** | | 응용 프로그램이 현재 라이선스 정보에 액세스할 수 있도록 Windows의 라이선스 상태를 업데이트합니다. | |
| **SetKeyManagementServiceListeningPort** | | 정품 인증 요청을 수신하기 위해 KMS 호스트에서 사용하는 TCP 포트를 지정합니다. KMS 호스트에만 적용됩니다. 지정하지 않는 경우 포트 1688이 사용됩니다. | |
| **ClearKeyManagementServiceListeningPort** | | 이전에 지정된 모든 수신 포트를 삭제합니다. KMS 호스트에만 적용됩니다. | |
| **DisableKeyManagementServiceDnsPublishing** | | KMS 호스트 컴퓨터에서 DNS 게시를 사용/사용 해제합니다. **0**=사용, **1**=해제. | |
| **EnableKey ManagementServiceLowPriority** | | 낮은 우선 순위로 실행되는 KMS 서비스를 사용/사용 해제합니다. **0**=해제, **1**=사용. | |
| **DisableKeyManagementServiceHostCaching** | | 볼륨 정품 인증 클라이언트 컴퓨터에서 KMS 호스트 이름 및 포트의 캐시를 사용/사용 해제합니다. **0**=사용, **1**=해제. | |
| **DisableKeyManagementServiceActivation** | | KMS 시스템을 통한 볼륨 정품 인증을 사용/사용 해제합니다. **0**=사용, **1**=해제. | |
| **DiscoveredKeyManagementServiceMachineName** | | DNS를 통해 마지막으로 발견된 KMS 호스트 이름. | |
| **DiscoveredKeyManagementServiceMachinePort** | | DNS를 통해 마지막으로 발견된 KMS 호스트 포트 | |
| **//속성 SoftwareLicensingService 클래스** | | | |
| **ID** | | 제품 식별자 | |
| **이름** | | 제품 이름 | |
| **설명** | | 제품 설명 | |
| **ApplicationID** | | 현재 제품의 응용 프로그램 ID | |
| **ProcessorURL** | | 프로세스 인증서에 대한 소프트웨어 라이선스 서버 URL | |
| **MachineURL** | | 바인딩 인증서에 대한 소프트웨어 라이선스 서버 URL | |
| **ProductKeyURL** | | 제품 인증서에 대한 소프트웨어 라이선스 서버 URL | |
| **UseLicenseURL** | | 사용자 라이선스에 대한 소프트웨어 라이선스 서버 URL | |
| **LicenseStatus** | | 이 제품의 응용 프로그램에 대한 라이선스 상태:  **0**=사용 허가되지 않음,  **1**=사용 허가됨, **2**=OOBGrace, **3**=OOTGrace, **4**=NonGenuineGrace, **5**=Notification, **6**=ExtendedGrace | |
| **LicenseStatusReason** | | 컴퓨터가 특정 라이선스 상태에 있는 이유를 표시하는 진단 코드. | |
| **GracePeriodRemaining** | | 상위 응용 프로그램이 알림 모드에 들어갈 때까지 남은 시간(분). 볼륨 클라이언트의 경우, 이는 정품 재인증 때까지 남은 시간입니다. | |
| **EvaluationEndDate** | | 이 제품의 응용 프로그램 만료 날짜. 이 날짜 이후에는 **LicenseStatus**가 **사용 허가되지 않음**이고 정품 인증될 수 없습니다. | |
| **OfflineInstallationId** | | 전화 또는 오프라인 정품 인증에 사용될 수 있는 이 제품의 응용 프로그램에 대한 식별자 제품 키가 설치되지 않으면 Null을 반환합니다. | |
| **PartialProductKey** | | 이 제품 키의 마지막 5문자. 제품 키가 설치되지 않으면 Null을 반환합니다. | |
| **ProductKeyID** | | 제품 키 ID. 제품 키가 설치되지 않으면 Null을 반환합니다. | |
| **LicenseFamily** | | SKU에 대한 제품군 종속성으로서 추가 기능에 대한 라이선스 관계를 결정하는 데 이용됩니다. | |
| **LicenseDependsOn** | | SKU 제품군에 대한 종속성 식별자로서 추가 기능에 대한 라이선스 관계를 결정하는 데 이용됩니다. | |
| **LicenseIsAddon** | | 제품이 추가 기능 라이선스로 확인되는 경우 **참**을 나타냅니다. | |
| **VLActivationInterval** | | 제품이 사용 허가되기 전 클라이언트가 KMS 호스트에 연결하는 분 단위 빈도 | |
| **VLRenewalInterval** | | 제품이 사용 허가된 후 클라이언트가 KMS 호스트에 연결하는 분 단위 빈도 | |
| **KeyManagementServiceProductKeyID** | | KMS 제품 키 ID. 해당하지 않는 경우 Null을 반환합니다. | |
| **KeyManagementServiceMachine** | | KMS 호스트 이름 **SetKeyManagementServiceMachine**이 호출되지 않은 경우, Null을 반환합니다. | |
| **KeyManagementServicePort** | | KMS 정품 인증 요청을 보내기 위해 클라이언트에서 사용된 TCP 포트 **SetKeyManagementServicePort**가 호출되지 않은 경우, **0**을 반환합니다. | |
| **DiscoveredKeyManagementServiceMachineName** | | DNS를 통해 마지막으로 발견된 KMS 호스트 이름. | |
| **DiscoveredKeyManagementServiceMachinePort** | | DNS를 통해 마지막으로 발견된 KMS 호스트 포트 | |
| **IsKeyManagementServiceMachine** | | 컴퓨터에서 KMS를 사용할 수 있는지 여부를 표시합니다. 참이면 **1**, 거짓이면 **0**. | |
| **KeyManagementServiceCurrentCount** | | KMS 호스트에서 현재 정품 인증된 KMS 클라이언트 수 **-1**은 컴퓨터가 KMS로 사용되지 않았거나 어떠한 클라이언트 라이선스 요청도 받지 않았음을 나타냅니다. | |
| **RequiredClientCount** | | 볼륨 라이선스 사용을 위해 KMS 호스트에 연결하는 데 필요한 최소 클라이언트 수. | |
| **KeyManagementServiceUnlicensedRequests** | | 라이선스 상태가 0(라이선스 미취득)인 클라이언트로부터 받은 KMS 요청 수 | |
| **KeyManagementServiceLicensedRequests** | | 라이선스 상태가 1(라이선스 취득)인 클라이언트로부터 받은 KMS 요청 수 | |
| **KeyManagementServiceOOBGraceRequests** | | 라이선스 상태가 2(OOB유예)인 클라이언트로부터 받은 KMS 요청 수 | |
| **KeyManagementServiceOOTGraceRequests** | | 라이선스 상태가 3(OOT유예)인 클라이언트로부터 받은 KMS 요청 수 | |
| **KeyManagementServiceNonGenuineGraceRequests** | | 라이선스 상태가 4(비정품유예)인 클라이언트로부터 받은 KMS 요청 수 | |
| **KeyManagementServiceTotalRequests** | | 유효한 총 KMS 요청 수 | |
| **KeyManagementServiceFailedRequests** | | 실패한 KMS 요청 수 | |
| **KeyManagementServiceNotificationRequests** | | 라이선스 상태가 5(알림)인 클라이언트로부터 받은 KMS 요청 수 | |
| **GenuineStatus** | | 이 제품의 응용 프로그램에 대한 정품 상태. | |
| **ExtendedGrace** | | 상위 응용 프로그램의 라이선스가 해제될 때까지 연장된 유예 시간(분). | |
| **TrustedTime** | | 시스템에 현재 저장된 신뢰할 수 있는 시간을 표시합니다. | |
| **DisableKeyManagementServiceHostCaching** | | 볼륨 정품 인증 클라이언트 컴퓨터에서 KMS 호스트 이름 및 포트의 캐시를 사용/사용 해제합니다. 0=사용, 1=사용 해제 | |
| **//방법 SoftwareLicensingProduct 클래스** | | | |
| **UninstallProductKey** | | | 현재 제품에 대한 제품 키를 제거합니다. |
| **Activate** | | | 현재 제품을 정품 인증합니다. |
| **DepositOfflineConfirmationId** | | | 전화 또는 오프라인 정품 인증을 수행할 때 이 제품에 대한 오프라인 확인 식별자를 보관하여 이 제품을 정품 인증합니다. |
| **GetPolicyInformationDWord** | | | 유형 DWORD의 라이선스 정책 정보를 가져옵니다. |
| **GetPolicyInformationString** | | | 유형 스트링의 정책 정보를 가져옵니다. |
| **SetKeyManagementServiceMachine** | | | 볼륨 정품 인증에 사용할 KMS 호스트 이름을 지정합니다. |
| **ClearKeyManagementServiceMachine** | | | 이전에 구성된 KMS 호스트 이름을 삭제합니다. |
| **SetKeyManagementServicePort** | | | 클라이언트가 KMS 호스트 요청을 하기 위해 사용하는 TCP 포트 지정하지 않는 경우 포트 1688이 사용됩니다. |
| **ClearKeyManagementServicePort** | | | 이전에 지정된 모든 포트 번호를 삭제합니다. |

# 용어

|  |  |
| --- | --- |
| **용어** | **정의** |
| **ACID** | GUID는 소프트웨어 버전 내의 정품 인증 방법을 확인하는 데 사용됩니다. |
| **AD DS** | Active Directory 도메인 서비스 |
| **AppID** | 이름의 성처럼 SKU ID들의 집합을 묶기 위해 정의된 GUID. 모든 Windows 버전에는 동일한 AppID가 있습니다. |
| **DNS** | 도메인 이름 서비스 |
| **FQDN** | 정규화된 도메인 이름(예: phred.microsoft.com). |
| **GVLK** | 모든 Windows 볼륨 버전에 기본적으로 설치되는 버전 별 제품 키인 일반 볼륨 라이선스 키 기본 KMS 클라이언트 설치 키라고도 불립니다. 자세한 내용은 표 9를 참조하십시오. |
| **KMS** | 키 관리 서비스 |
| **KMSID** | KMS 클라이언트가 KMS 호스트의 정품 인증을 위해 보내는 GUID. 다수의 ACID에서 공유될 수 있습니다. |
| **컴퓨터 인증서 저장소** | 이 인증서 및 인증서의 개인 키는 토큰 기반 제품 인증을 시도하는 사용자가 액세스할 수 있어야 합니다. |
| **MAK** | 복수 정품 인증 키 |
| **N-policy** | KMS가 반환한 시스템의 최소 수를 지정하는 라이선스 정책으로서 클라이언트가 자동 정품 인증할지 여부를 결정하는 데 사용합니다. |
| **PIN** | 인증 자격 증명으로서 스마트 카드와 함께 사용되는 개인 식별 번호 |
| **SKU** | Windows 또는 기타 소프트웨어의 독특한 버전을 나타냅니다. |
| **SKUId** | 위의 ACID와 동일 |
| **SPPSVC** | 소프트웨어 보호 서비스, Windows 7 및 Windows Server 2008 R2에 내장된 서비스 플랫폼으로서 Windows 및 기타 응용 프로그램의 라이선스 활동을 관리합니다. |
| **SRV** | DNS에서 지원되는 리소스 레코드 유형(RFC(Request for Comments) 2782 참조) |
| **토큰** | 관련 개인 키를 포함하는 x509 인증서는 토큰 기반 정품 인증을 사용하도록 하는 컴퓨터에서 Windows를 정품 인증하기 위해 사용됩니다. |
| **VL** | 볼륨 라이선스 |
| **WMI** | Windows Management Instrumentation |

# 리소스 링크

* 볼륨 정품 인증
* TechNet에서 볼륨 정품 인증: <http://go.microsoft.com/fwlink/?LinkId=150083>
* Windows Server 2003 SP1 이상을 위한 키 관리 서비스 1.2: <http://go.microsoft.com/fwlink/?LinkId=155083>
* 제품 정품 인증 및 주요 정보: <http://go.microsoft.com/fwlink/?LinkId=74008>
* 볼륨 정품 인증 배포 가이드: <http://go.microsoft.com/fwlink/?LinkId=150083>
* 볼륨 정품 인증 운영 가이드: <http://go.microsoft.com/fwlink/?LinkId=150084>
* 볼륨 정품 인증 계획 가이드: <http://go.microsoft.com/fwlink/?LinkId=155926>
* 볼륨 정품 인증 기술적 참조 가이드: <http://go.microsoft.com/fwlink/?LinkId=152550>
* 배포 도구:
* Windows 7용 Windows 자동 설치 키트(AIK): <http://go.microsoft.com/fwlink/?LinkId=136976>
* 관리 도구:
* System Center 팩 카탈로그: <http://go.microsoft.com/fwlink/?LinkID=110332>
* 볼륨 라이선스:
* 정품 Microsoft 소프트웨어: <http://go.microsoft.com/fwlink/?LinkId=151993>
* 정품 Microsoft 소프트웨어 인증 페이지: <http://go.microsoft.com/fwlink/?LinkId=64187>
* Microsoft 정품 인증 센터 전세계 전화 번호: <http://go.microsoft.com/fwlink/?LinkId=107418>
* Microsoft 볼륨 라이선스: <http://go.microsoft.com/fwlink/?LinkId=73076>
* Microsoft 볼륨 라이선스 서비스 센터: <http://go.microsoft.com/fwlink/?LinkId=107544>
* Windows Vista 개인 정보 보호 표시 하이라이트: <http://go.microsoft.com/fwlink/?LinkID=52526>