

Intel® Unite™ 솔루션

보호된 게스트 액세스 플러그인 설명서



법적 면책 조항 및 저작권

이 문서에 제공된 모든 정보는 예고 없이 변경될 수 있습니다. 최신 인텔 제품 사양 및 로드맵을 확인하려면 인텔 담당자에게 문의하십시오.

인텔 기술의 기능 및 이점은 시스템 구성에 따라 달라지며 지원되는 하드웨어, 소프트웨어 또는 서비스 활성화가 필요할 수 있습니다. 성능은 시스템 구성에 따라 달라집니다. 어떠한 컴퓨터 시스템도 절대적으로 안전하지는 않습니다. 시스템 제조업체 또는 소매점을 통해 확인하거나 intel.com 에서 자세한 내용을 알아보십시오.

여기에 설명된 인텔 제품에 대한 침해 또는 기타 법적 분석과 관련하여 이 문서를 사용하거나 사용을 조장해서는 안 됩니다. 귀하는 여기에 공개된 주제를 포함한 특허권 청구에 대해 비독점적이고 로열티 없이 사용할 수 있는 라이선스를 인텔에 부여하는 것에 동의합니다.

이 문서로 부여되는 지적 재산권에 대한 명시적 또는 묵시적 라이선스는 없습니다.

기술된 제품에는 정오표로 알려진 오류나 설계 결함이 있을 수 있으며, 이로 인해 게시된 사양과 다르게 작동할 수도 있습니다. 현재 정리된 정오표를 요청 시 제공하고 있습니다.

인텔은 수행 과정, 거래 과정 또는 교역 상 사용 시 발생하는 모든 보증뿐 아니라 상품성, 특정 목적에의 적합성 및 비침해성에 대한 묵시적 보증을 포함하되 이에 국한되지 않는 모든 명시적 및 묵시적 보증을 부인합니다.

인텔은 본 문서에 참조된 타사 벤치마크 데이터 또는 웹사이트를 통제 또는 감사하지 않습니다. 참조된 웹 사이트를 방문하여 참조된 데이터가 정확한지 여부를 확인해야 합니다.

인텔, 인텔 로고 및 Intel Unite 는 미국 및/또는 기타 국가에서의 인텔사 또는 자회사의 상표입니다.

이 문서의 일부 이미지는 현지화 작업으로 인해 다르게 표시될 수 있습니다.

* 기타 이름 및 브랜드는 해당 소유 업체의 자산입니다.

© 2016 인텔사. 모든 권한은 인텔사에 있습니다.



1. 소개.....	4
1.1 대상.....	4
1.2 개요.....	4
1.3 권장 보안 제어.....	5
2. 플러그인 설치 및 구성 요소.....	6
2.1 플러그인 구성 요소.....	6
2.2 플러그인 설치.....	6
2.2.1 엔터프라이즈 버전.....	7
인증서 해시 값 받기.....	7
관리자 웹 포털에서 프로파일 만들기.....	9
보호된 게스트 액세스 플러그인의 레지스트리 키.....	10
2.2.2 독립형 버전.....	10
3. Protected Guest Access 플러그인 플로우.....	12
4. 클라이언트 기기에서 게스트 액세스를 활성화하는 방법.....	13
부록 A. 방화벽 예외.....	18
부록 B. 문제 해결.....	19

1. 소개

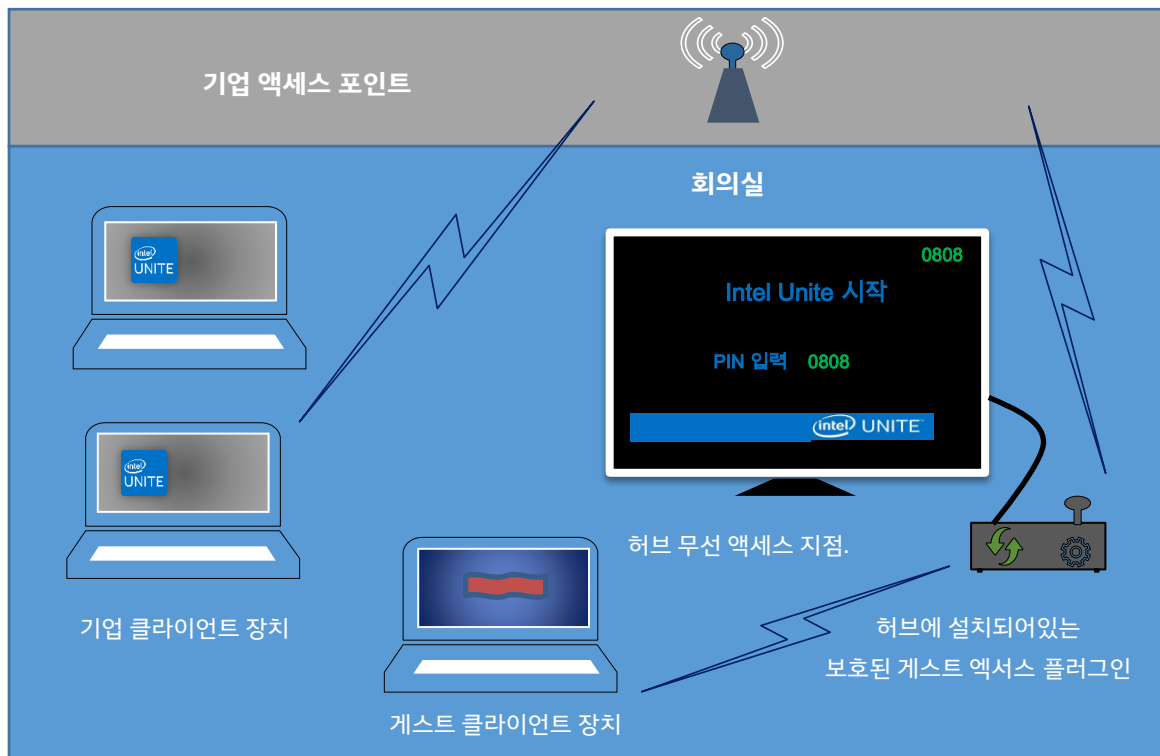
이 문서에서는 Intel Unite 솔루션에 보호된 게스트 액세스용 Intel® Unite™ 플러그인을 설치하고 사용하는 방법에 대해 설명합니다.

1.1 대상

이 문서는 기업에서 Intel Unite 소프트웨어의 설치와 응용 프로그램에 대한 옵션 기능 추가(예: 비즈니스에 대한 게스트 액세스 활성화)를 담당하고 있는 IT 전문가를 대상으로 작성되었습니다.

1.2 개요

보호된 게스트 액세스용 Intel Unite 플러그인을 사용하면 게스트 클라이언트 장치가 동일한 엔터프라이즈 네트워크 상에 있지 않은 경우에도 허브에 연결할 수 있습니다. 이것은 허브에서 게스트 클라이언트 기기가 해당 클라이언트 기기용 Intel Unite 응용 프로그램을 연결하고 다운로드하거나 참여할 수 있도록 임시/호스팅된 네트워크(액세스 포인트)를 생성할 수 있기에 가능합니다.



1.3 권장 보안 제어

IT 직원은 아래에 언급된 권장 보안 제어를 따르는 것이 좋습니다.

- 게스트 액세스를 실행하는 허브에서 네트워크 브리징을 끕니다.
- Active Directory 환경에서 응용 프로그램과 사용자를 제한하는 허브의 그룹 정책 개체(GPO 정책)를 설정합니다.
- 인증되지 않은 트래픽을 제한하기 위해 게스트 액세스 기기와 기업 연결 사이에 방화벽을 구축합니다.
- 사용하지 않는 포트에 방화벽이 있는지 확인합니다.
- 인증되지 않은 실행 파일이 게스트 액세스 기기에서 실행되는 것을 방지하기 위해 McAfee* Application Control 이나 Windows* AppLocker 등과 같은 소프트웨어 기반 솔루션을 구축합니다.
 - McAfee Application Control 에 대한 자세한 내용은 <http://www.mcafee.com/us/products/application-control.aspx> 를 참조하십시오.
 - Windows AppLocker 에 대한 자세한 내용은 <https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511> 을 참조하십시오.
- 인증되지 않은 실행 파일이 게스트 액세스 기기에서 실행되는 것을 방지하기 위해 Windows* 10 의 Device Guard 와 같은 하드웨어 및 소프트웨어 기반 솔루션을 구축합니다.
 - Device Guard 에 대한 자세한 내용은 <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide> 를 참조하십시오.
- 네트워크 브리징을 비활성화하는 방법에 대한 자세한 내용은
 - [https://technet.microsoft.com/en-us/library/cc732103\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732103(v=ws.10).aspx) 를 참조하십시오.

1. 플러그인 설치 및 구성 요소

1.1 플러그인 구성 요소

다음 구성 요소는 보호된 게스트 액세스 플러그인의 일부입니다.

- 게스트 액세스 클라이언트 플러그인(dll)
 - 허브에서 로드되는 플러그인입니다. 이 플러그인은 CFCPlugin.dll 에 정의된 기능을 구현합니다.
- 게스트 액세스 서비스(Windows 서비스)
 - 이것은 임시/호스팅된 네트워크(액세스 포인트)의 생성과 구성을 담당하는 Windows 서비스로, GuestAccessClientPlugin.dll 에서 보내는 명령을 수신하여 처리합니다.
- 클라이언트 다운로드 페이지
 - 임시 네트워크를 호스트하는 허브를 실행하고 이 허브에 연결하도록 구성된 클라이언트용 Intel Unite 앱 v3.0 이 필요합니다. 네트워크가 생성된 후에 다운로드할 수 있습니다.

1.2 플러그인 설치

보호된 게스트 액세스용 Intel® Unite™ 플러그인을 설치하려면 관리자 권한이 필요합니다. 설치할 Intel Unite 솔루션 버전과의 호환성도 확인해야 합니다(Intel Unite 소프트웨어 버전 1.0 및 2.0 은 최신 릴리스된 플러그인 버전과 호환되지 않습니다).

LAN 케이블 필요: 허브의 최소 요구 사항 외에도 허브가 유선 연결을 통해 기업 네트워크에 연결되어 있고 무선 네트워크 어댑터가 다른 액세스 포인트에 연결되어 있지 않은 상태로 네트워크가 구성되어 있는지 확인해야 합니다.



보호된 게스트 액세스 플러그인을 설치하기 전에 최신 인텔 무선 드라이버가 있는지 확인합니다. 없는 경우 최신 인텔 무선 드라이버를 설치합니다.

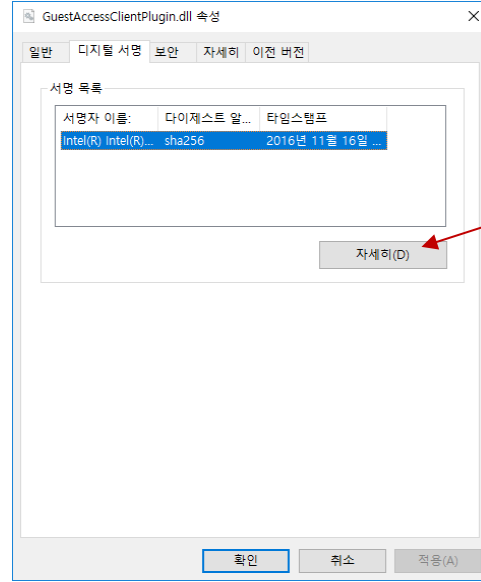
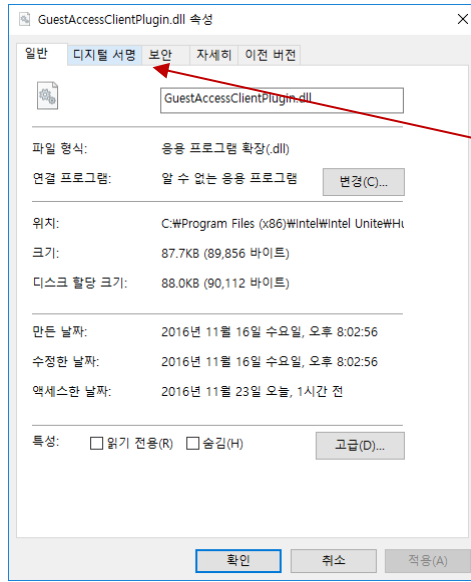
3.3.3 엔터프라이즈 버전

1. **Intel Unite 보호된 게스트 액세스 플러그인 설치 프로그램**(Windows 설치 프로그램 패키지)을 실행합니다.
2. GuestAccessClient Plugin.dll 이 설치된 Program Files(x86) \Intel\Intel Unite\Hub\Plugins 폴더로 이동합니다.
3. 다음 단계는 게스트 액세스 클라이언트 플러그인의 인증서 해시 값(키 값)을 받는 것입니다. 키 값은 보안을 강화하고 허브에 악성 플러그인이 설치되어 실행되는 것을 방지하므로 기본값을 사용하는 대신 플러그인용 키 값을 받아서 사용하는 것이 좋습니다.

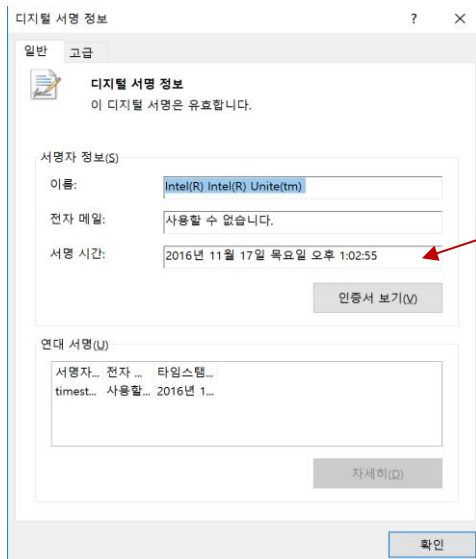
참고: 테스트 환경에서는 기본 키 값을 사용해도 되지만, 프로덕션 환경에서는 받아서 사용하는 것이 좋습니다.

인증서 해시 값 받기

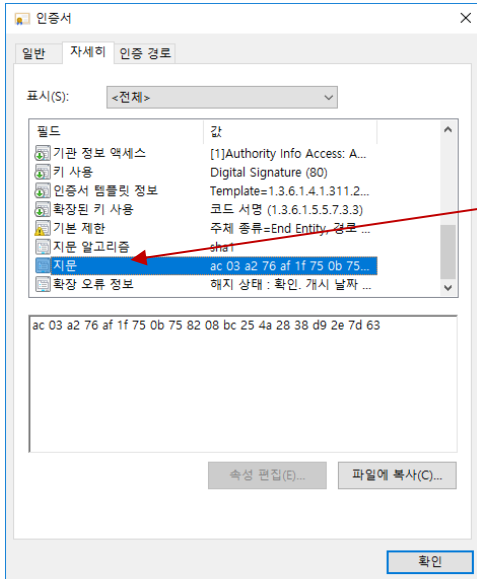
1. Intel Unite\Hub\Plugins 폴더에서 **GuestAccessClientPlugin.dll** 을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
2. 플러그인 속성 창이 열리면 **디지털 서명** 탭을 엽니다.



4. Intel Unite 플러그인을 선택하고 세부 정보를 클릭합니다.
5. 디지털 서명 정보 창에서 인증서 보기를 클릭합니다.



6. 인증서 창에서 세부 정보 탭을 선택하고 손도장이 보일 때까지 아래로 스크롤합니다.
7. 손도장을 선택합니다. 값이 표시되면 메모장이나 텍스트 파일에 복사하여 붙여 넣은 다음 공백을 제거하고 저장합니다.

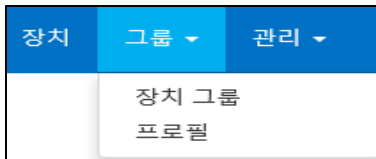


메모장이나 텍스트 파일에 값을 복사하여 붙여 넣은 다음 공백을 제거하고 저장합니다.

- 이 정보는 관리자 웹 포털에서 플러그인 프로필을 만들 때 사용됩니다. 프로필을 만든 다음에 키 값을 만들고 입력해도 됩니다.

관리자 웹 포털에서 프로필 만들기

- 관리자 웹 포털로 이동하여 그룹에서 프로필을 선택합니다.



- 만들기를 클릭하여 게스트 액세스 플러그인 인증서 해시 키를 만듭니다. 프로필 속성 창이 열리면 다음을 입력합니다.

프로필 속성 생성

키 및 값 필드는 필수이며 다른 설명이 없는 경우 텍스트여야 합니다.

키:

데이터 유형:

값:

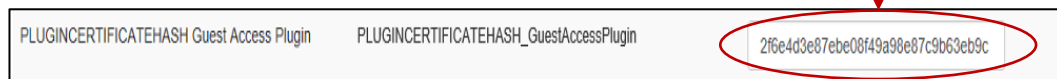
- 키: PluginCertificateHash_GuestAccessPlugin

(PluginCertificateHash_XXXX 형식으로 표시됩니다. X 는 사용자가 플러그인에 지정하는 이름입니다.)

- **데이터 유형:** 텍스트
- **값:** 섹션 - 인증서 해시 값 받기 - (손도장 값)에서 메모장이나 텍스트 파일에 저장한 값을 붙여 넣습니다. 이 데이터는 키를 만든 다음에 입력해도 됩니다.

3. **만들기**를 클릭하여 프로필을 저장합니다.

4. **프로필 정보** 창에 입력한 플러그인의 새 프로필과 입력한 키 값이 표시됩니다.



5. **프로필 정보** 창의 **플러그인 인증서 해시 확인**이 활성화되어 있는지(녹색) 확인해야 합니다. 활성화되어 있지 않으면 붉은색에서 녹색으로 변경하여 활성화합니다.



참고: 테스트 환경에서는 인증서 확인을 비활성화해도 됩니다(프로덕션 환경에서는 권장되지 않음).

보호된 게스트 액세스 플러그인의 레지스트리 키

레지스트리 키에 정의된 데이터:

- HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID
- HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK

중요: 암호를 지정할 경우 암호는 8 자 이상이어야 합니다. 암호가 8 자보다 짧은 경우 게스트 액세스가 시작되지 않을 수 있습니다.

- HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download

□.□.□ 독립형 버전

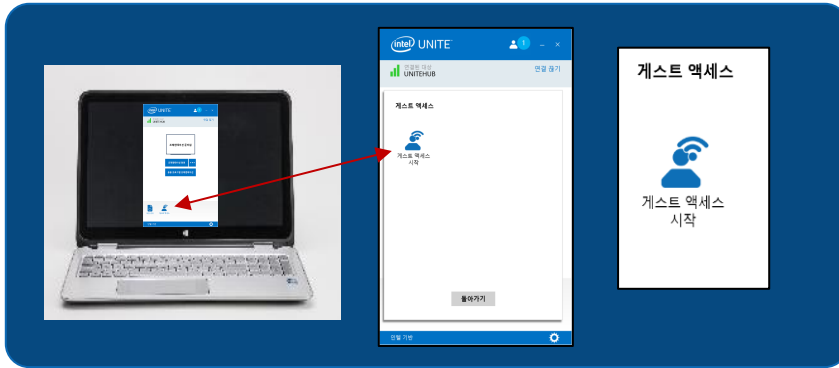
독립형 버전에서는 허브에서 실행 중인 Intel Unite 응용 프로그램을 닫은 뒤 바탕 화면 실행 프로그램을 클릭하거나 시작 메뉴에서 Intel Unite 응용 프로그램 **설정**을 엽니다.

1. 설정 창에서 **플러그인** 탭으로 이동합니다.

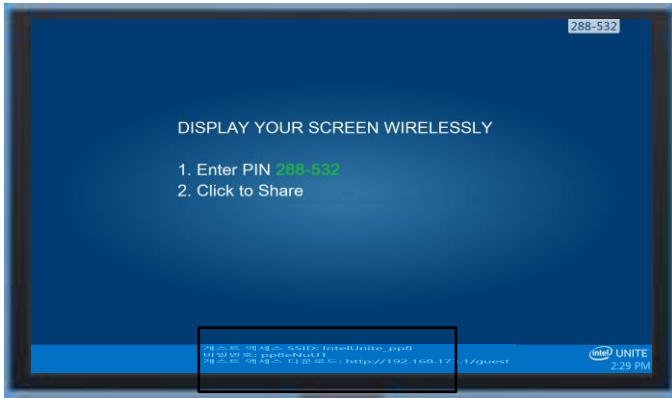


2. **플러그인에서 인증서 확인**에서 예를 선택합니다. 이 설정을 사용하면 신뢰할 수 있는 플러그인만 로드됩니다.
 - 신뢰하는 디지털 서명 플러그인만 로드하려면 **예**로 설정합니다. **아니오**로 설정하면 설치된 모든 플러그인이 로드됩니다.
3. **신뢰할 수 있는 플러그인**에서 게스트 액세스 플러그인 상자를 선택하여 활성화하고 **저장**을 클릭합니다. 이 옵션은 **플러그인에서 인증서 확인**이 **예**로 설정된 경우에만 표시됩니다. 신뢰할 수 있는 플러그인 목록이 비어 있는 경우 디지털 서명된 플러그인이 설치되어 있지 않은 것입니다.

3. Protected Guest Access 플러그인 플로우



모니터에 표시된 PIN 을 입력하면 클라이언트 장치에서 Intel Unite 응용 프로그램의 세션이 시작되고 게스트 액세스도 시작됩니다.

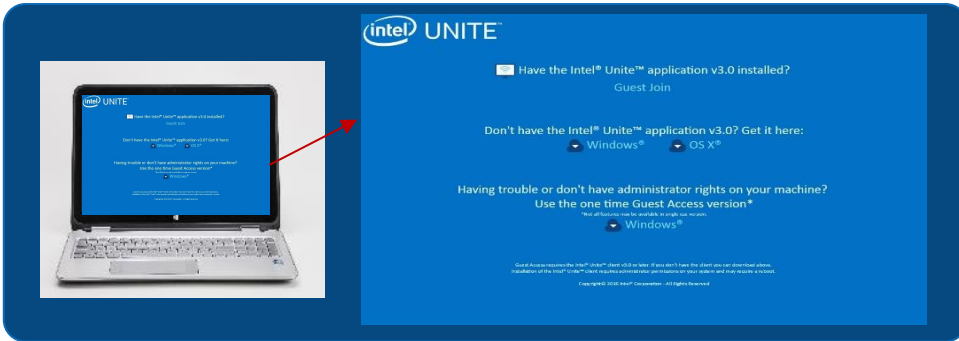


허브에서 설치된 플러그인과 서비스가 시작됩니다.

게스트 액세스 SSID: IntelUnite_pp8
비밀번호: pp8eNuU1
게스트 액세스 다운로드: <http://192.168.173.1/guest>

게스트 액세스 서비스에서 호스팅된 네트워크를 시작합니다. SSID, 암호, 다운로드 링크가 모니터에 표시됩니다.

게스트(사용자)가 관련된 암호를 사용하여 SSID 에 연결하고 응용 프로그램에 참가하거나 응용 프로그램을 다운로드합니다.

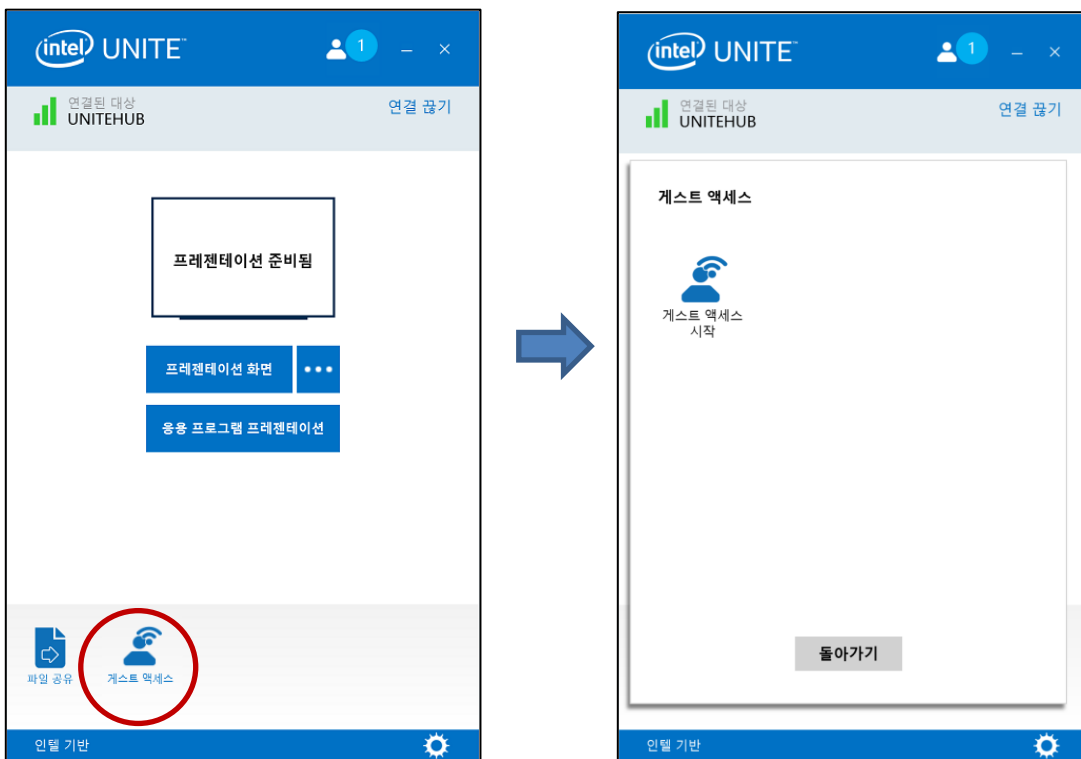


1. 클라이언트 기기에서 게스트 액세스를 활성화하는 방법

사용자는 게스트 액세스 클라이언트가 연결할 수 있는 클라이언트 기기가 필요합니다. 이 클라이언트 기기는 허브(회의실의 참석자)와 로컬로 연결되고, 모니터 또는 디스플레이에 표시된 PIN 을 사용하여 연결합니다.

게스트 액세스를 허용하는 클라이언트 기기의 경우:

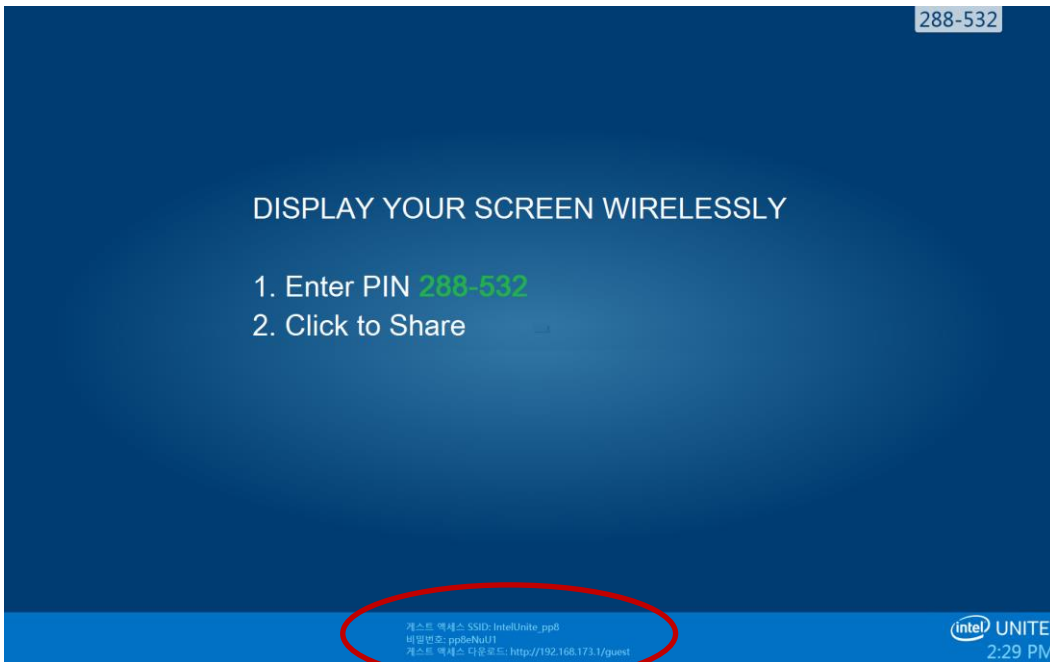
1. 허브에 표시된 PIN 을 사용하여 Intel Unite 응용 프로그램에 연결합니다.
2. 연결되면 창에 표시된 **게스트 액세스** 아이콘을 클릭합니다.



3. **게스트 액세스** 창이 표시됩니다. 이제 **게스트 액세스 시작**을 클릭하여 게스트가 참여할 수 있도록 로컬 Wi-Fi 액세스를 활성화할 수 있습니다.

4. 허브(회의실의 모니터 또는 디스플레이)에 다음 사항이 표시됩니다.

- **게스트 액세스 SSID** “고유 네트워크 이름”
- 사용할 **암호**
- **게스트 액세스 다운로드 링크**

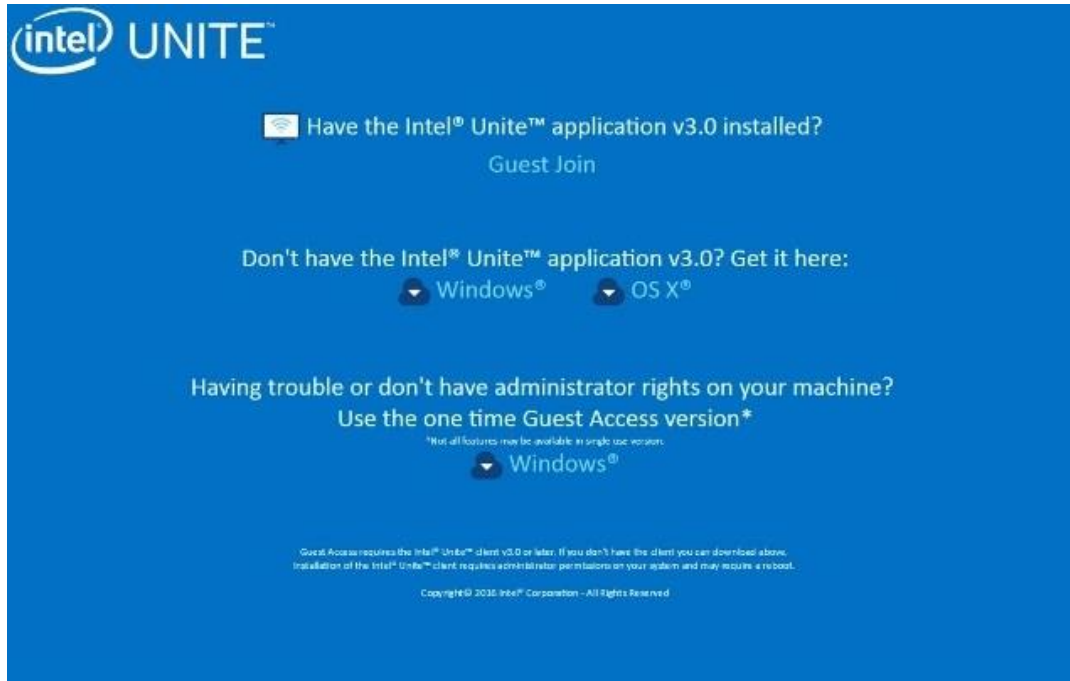


게스트 액세스 SSID: IntelUnite_pp8
비밀번호: pp8eNuU1
게스트 액세스 다운로드: <http://192.168.173.1/guest>

게스트 액세스를 통해 연결하는 클라이언트 기기의 경우(세션 게스트):

1. **게스트 액세스 SSID** 에 연결하고 허브에 표시된 **암호** 를 입력합니다.
2. 브라우저에서 모니터에 표시된 **게스트 액세스 다운로드** 링크로 이동합니다. 표시된 형식 <http://<hostIP>/guest> 를 사용하십시오.

3. 다음 웹 페이지가 표시됩니다.



4. 다음 3 가지 옵션에 따라 선택합니다.

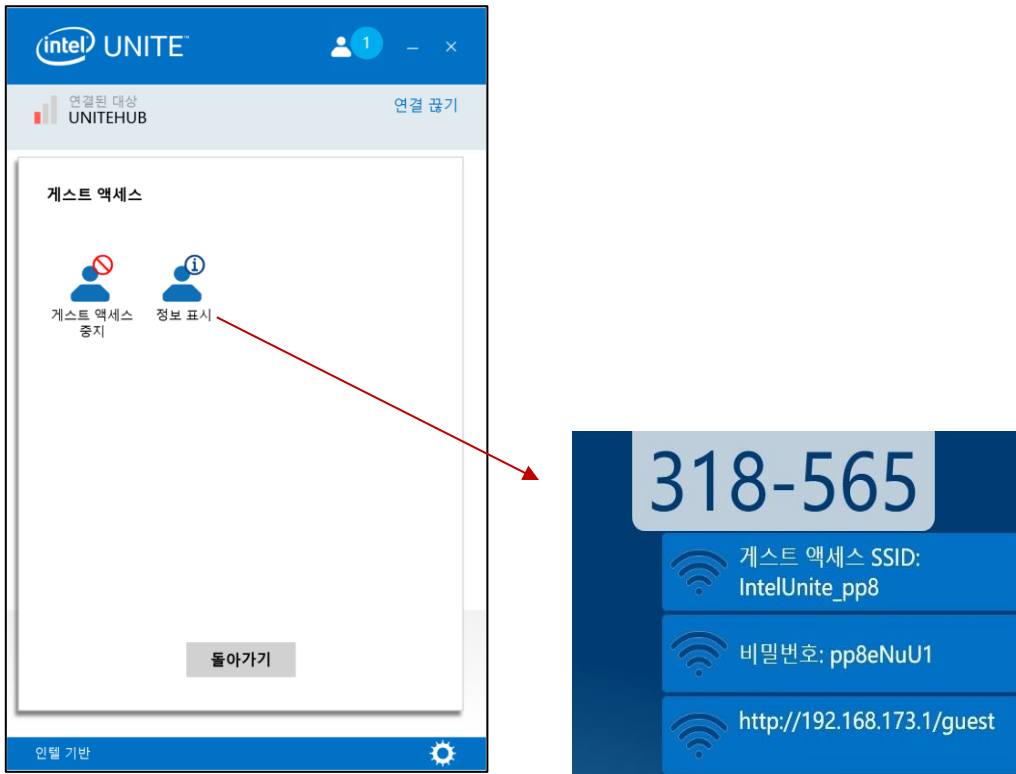
- **Intel Unite 응용 프로그램 v3.0 이 설치되어 있습니까?**
 - 클라이언트 기기에 Intel Unite 응용 프로그램이 이미 설치되어 있는 경우 이 옵션을 사용하십시오. **게스트 참여**만 클릭하면 간단히 연결할 수 있습니다(v3.0 필요).
- **Intel Unite 응용 프로그램 v3.0 이 설치되어 있지 않습니까? 여기에서 받기:**
 - 클라이언트 기기에 Intel Unite 앱이 설치되어 있지 않은 경우 이 옵션을 사용하십시오. OS 에 따라 **Windows*** 또는 **OS X***을 클릭하고 연결할 앱을 다운로드합니다.
- **문제가 발생했거나 기기에 대한 관리자 권한이 없습니까?**

일회용 게스트 액세스 버전 사용

- 기기에 Intel Unite 응용 프로그램이 없는 경우 및/또는 응용 프로그램을 다운로드하는 데 문제가 있는 경우(앞의 2 개 옵션) 또는 앱 다운로드 및 설치를 위한 관리자 권한이 없는 경우, 이 옵션을 사용하십시오. **일회용 게스트 액세스**

버전을 사용할 수 있습니다. 이 옵션을 사용하면 Intel Unite 앱이 일회 사용할 수 있도록 열리며 클라이언트 기기에 계속 남아 있지 않습니다. 이 옵션은 **Windows* OS**에서만 사용할 수 있습니다.

5. 선택에 따라 설치 프로그램을 다운로드하여 설치하십시오.
6. 설치를 완료한 후에 클라이언트 기기에 **연결 대상** 창이 표시되며, 게스트는 PIN 을 입력하여 세션에 연결할 수 있습니다.
7. 게스트 액세스 창에서 **정보 표시** 아이콘이 표시되면 세션에 연결된 게스트를 볼 수 있습니다. **정보 표시** 아이콘을 클릭하면 모니터(허브)에 게스트가 사용하는 게스트 액세스 정보가 포함된 메시지가 몇 초 동안 표시됩니다.



8. 세션에서 모든 사용자의 연결이 해제되면 게스트 액세스를 사용하는 클라이언트 기기의 연결도 해제됩니다. 허브(모니터 또는 디스플레이)에는 게스트 액세스를 통해 연결된 사용자가 없음을 알리는 메시지가 몇 초 동안 표시됩니다.



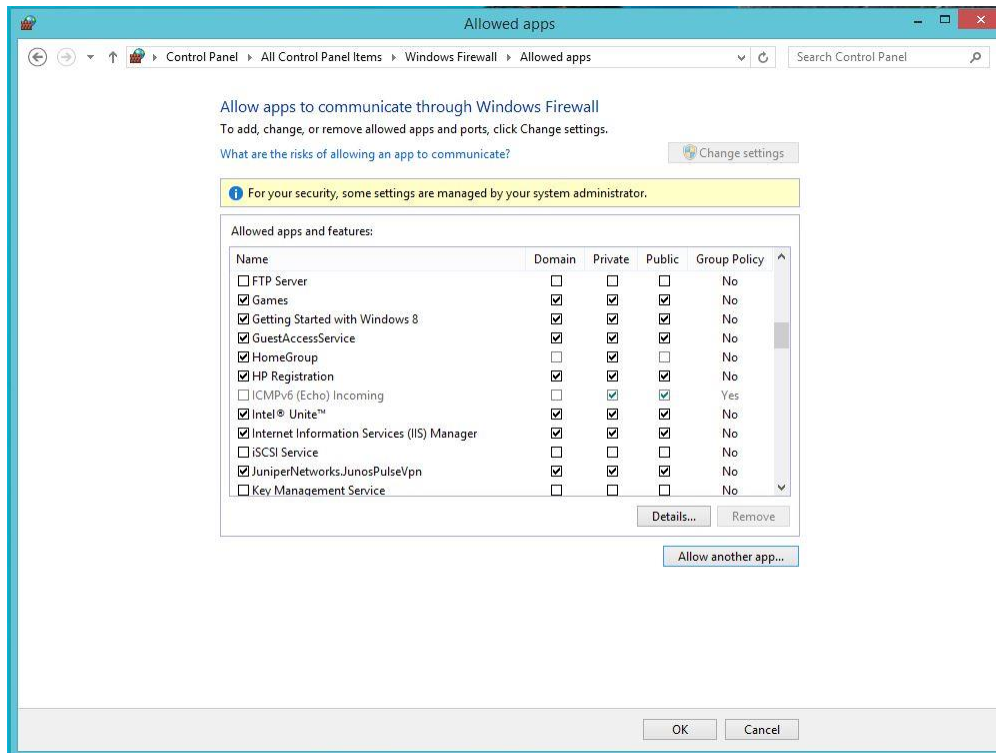
게스트 액세스가 중지되었습니다. 연결된 사용자가 없습니다.

부록 A. 방화벽 예외

Intel Unite 응용 프로그램 및 GuestAccessService 가 방화벽 설정의 허용되는 앱 목록에 추가되었는지 확인하십시오.

아래 예제에 표시된 바와 같이 다음 상자는 선택되어야 합니다.

1. Internet Information Service(IIS)
2. 관리자 및 World Wide Web(HTTP)
3. GuestAccessService



부록 B. 문제 해결

추가적인 정보는 Windows* 이벤트 로그를 참조할 수도 있습니다.

게스트 액세스가 시작되지 않음(또는 표시되지 않음)

- 플러그인의 동작을 방해하는 인증서 해시가 관리 포털에 입력되지 않았음을 확인하십시오.
- 조직 GPO 정책(그룹 정책 개체)에서 가상 호스팅 네트워크를 허용하지 않을 수 있습니다. 시스템 관리자에게 문의하십시오.
- 보호된 게스트 액세스의 플러그인 인증서 해시 키 값이 관리자 웹 포털에 입력되었는지 확인하십시오(엔터프라이즈 버전).
- 플러그인 인증서 해시가 관리자 웹 포털에서 활성화되어 있는지 확인하십시오.
- 허브가 유선 연결을 통해 기업 네트워크에 연결되어 있는지 확인하십시오.
- 독립형 버전의 경우, 설정의 플러그인 탭 섹션에서 “신뢰할 수 있는 플러그인” 상자를 클릭하여 플러그인을 활성화했는지 확인하십시오.
- 레지스트리 키 HKCU/software/intel/unite/guestaccess/PSK 에서 암호 값이 변경된 경우(기본값을 사용하지 않고 있는 경우) 암호가 최소 8 자로 이루어져 있는지 확인하십시오.
- 최신 인텔 무선 드라이버가 적용되어 있는지 확인하십시오.