

Intel Unite[®] 솔루션

엔터프라이즈 배포 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, Intel Unite, 인텔 코어 및 인텔 v 프로는 미국 및/또는 기타 국가에서 인텔사 또는 그 자회사의 상표입니다.

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

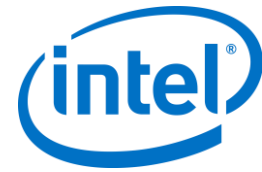
* 기타 이름 및 브랜드는 해당 소유 업체의 자산입니다.

© 2017 Intel Corporation. 모든 권한은 인텔사에 있습니다.

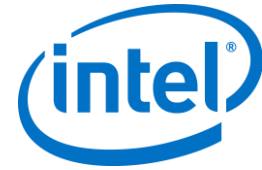


목

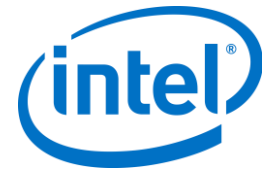
1	소개.....	7
	1.1 대상.....	7
	1.2 Intel Unite 솔루션 용어 및 정의.....	7
	1.3 Intel Unite 솔루션의 새로운 기능.....	8
2	Intel Unite 솔루션 요구 사항.....	9
	2.1 엔터프라이즈 서버 요구 사항.....	9
	2.2 허브 요구 사항.....	9
	2.3 클라이언트 요구 사항.....	9
	2.4 IT 관련 고려 사항 및 네트워크 요구 사항.....	10
	2.4.1 모바일 클라이언트 장치.....	10
3	배포 개요.....	11
	3.1 배포 리소스.....	11
4	엔터프라이즈 서버 설치.....	12
	4.1 엔터프라이즈 서버 개요.....	12
	4.2 엔터프라이즈 서버 사전 설치.....	12
	4.2.1 소프트웨어 업그레이드.....	12
	4.3 엔터프라이즈 서버 설치.....	13
	4.4 Intel Unite 응용 프로그램 제거.....	15
5	허브 설치.....	17
	5.1 허브 사전 설치.....	17
	5.1.1 공개 키.....	17
	5.2 허브 설치.....	18
	5.3 허브 구성.....	21
	5.4 허브 추천 사례.....	21
	5.5 허브 보안.....	21
	5.6 플러그인.....	21
	5.6.1 플러그인 설치 참고 사항.....	22
	5.6.2 플러그인 인증서 해시 값.....	22
	5.6.3 관리 웹 포털에서 플러그인에 인증서 해시 추가.....	23
6	클라이언트 설치.....	26
	6.1 클라이언트 사전 설치.....	26
	6.2 Windows 클라이언트 설치.....	26
	6.3 macOS 클라이언트 설치.....	30
	6.4 iOS 클라이언트 설치.....	31



6.5	Android 클라이언트 설치	32
6.6	Chrome OS 클라이언트 설치	33
6.7	클라이언트 구성	33
7	고급 설치	34
7.1	스크립트 방식의 설치 프로그램	34
7.2	레지스트리 키	35
8	관리 포털 설명서	38
8.1	관리 웹 포털 시작 페이지	38
8.1.1	계정 등록	39
8.1.2	기존 계정으로 로그인	39
8.2	관리 포털 홈 페이지	40
8.2.1	탐색 줄	40
8.2.2	아이콘/링크 명칭	41
8.3	장치 페이지	41
8.4	그룹 페이지	43
8.4.1	그룹 > 장치 그룹	43
8.4.2	그룹 > 프로필	44
8.5	관리 페이지	46
8.5.1	관리 > 서버 속성	46
8.5.2	관리 > 사용자	47
8.5.3	관리 > 역할	48
8.5.4	관리 > 중재자	48
8.5.5	관리 > 예약된 PIN	52
8.5.6	관리 > 원격 측정	54
8.6	회의 예약 페이지	55
8.7	관리 포털의 기타 구성 옵션	55
8.7.1	프로필 구성	55
8.7.2	PIN 새로 고침 간격	58
8.7.3	이메일 서버 설정	58
8.7.4	알림 및 모니터링	58
9	OS 및 PC 보안 제어	60
9.1.1	최소 보안 사항(MSS)	60
9.1.2	기기 강화	60
9.1.3	기타 보안 제어	60
10	유지 관리	61
10.1	야간 재부팅	61
10.2	패치 전략	61
10.3	보고	61
10.4	모니터링	61



10.4.1	백엔드 모니터링:.....	61
11	macOS 용 Intel Unite 솔루션.....	62
11.1	배경.....	62
11.2	일반 연결 워크플로.....	62
11.3	기본 설정 값.....	62
11.4	일반 배포 방법.....	63
12	문제 해결.....	65
12.1	Intel Unite 응용 프로그램을 서버에 설치한 뒤에 관리 포털 페이지에 접속할 수 없음.....	65
12.2	관리 포털에 액세스할 수 없음.....	65
12.3	허브 응용 프로그램 실행 시 오류.....	66
12.3.1	오류 ID 333333의 플랫폼 확인 실패.....	66
12.3.2	오류 ID 666666의 플랫폼 확인 실패.....	66
12.4	허브가 PIN 서버에서 PIN 을 가져오지 않음 - 스크롤 다시 표시됨.....	66
12.4.1	서버에서 요청을 처리할 수 없음; 사용자 "UniteServiceUser" 로그인 실패.....	66
12.4.2	서버가 없습니다. DNS 서비스 레코드: _uniteservice._tcp 다시 시도.....	67
12.4.3	'uniteserverfqdn' 권한으로 SSL/TLS 보안 채널에 신뢰 관계를 형성할 수 없음.....	68
12.5	실행/연결 시 클라이언트 응용 프로그램 충돌.....	68
12.6	주의 분야: 사용자는 평상시보다 긴 연결 시간이나 정기적으로 화면 업데이트가 느려지는 현상을 경험할 수 있습니다.....	69
12.7	주의 분야: PIN 서버 속도 저하.....	69
12.8	Mac 클라이언트 문제 해결.....	69
12.8.1	엔터프라이즈 서버 연결 오류 -1003: 지정된 호스트 이름의 서버를 찾을 수 없습니다.....	70
12.8.2	Enterprise Server 연결 오류 -1001: 요청 시간 초과.....	70
12.8.3	Enterprise Server 연결 오류 -1200: SSL 오류가 발생하여 서버에 대한 보안 연결을 구성할 수 없습니다.....	70
12.9	Mac OS Intel Unite app 앱이 클라이언트 장치에서 제거되고 다른 버전이나 최신 버전의 Intel Unite 응용 프로그램이 설치되었으나 기존 설치 속성이 그대로 남아 있습니다.....	70
12.10	오류 2147217900: SQL 문자열을 실행하지 못했습니다.....	71
12.11	오류 메시지: "데이터베이스 오류".....	71
12.12	관리자 웹 포털이 제대로 표시되지 않음(구성 요소가 누락됨).....	71
부록 A.	엔터프라이즈 서버 준비.....	73
	IIS 활성화.....	73
	Microsoft SQL Server 설치.....	78
	DNS 서비스 레코드 생성.....	82
부록 B.	ServerConfig.xml 예시.....	83
부록 C.	Intel Unite 솔루션 - 보안 개요.....	84
	Intel Unite 소프트웨어 - 보안 흐름.....	84



1 단계: PIN 할당	85
2 단계: PIN 조회	86
3 단계: 연결 초기화.....	87
4 단계: 연결 승인.....	88
부록 D. Intel Unite 솔루션 - 부하 분산기.....	89



1 소개

Intel Unite® 소프트웨어는 안전하게 연결된 회의 공간을 제공하여 협업을 간편하게 만들어줍니다. 이 소프트웨어는 회의에 참석한 모든 사람을 신속하고 간편하게 연결할 수 있도록 설계되었습니다. Intel Unite 솔루션은 간편하고 즉각적인 최신 협업 솔루션이자 향후 추가될 기능 및 혁신을 위한 기반입니다.

이 문서는 엔터프라이즈 모드로 Intel Unite 소프트웨어를 설치하는 데 사용할 수 있습니다. 기능 및 문제 해결 지원 방법에 대해 자세히 알아보십시오.

1.1 대상

이 문서는 기업에서 근무하는 IT 전문가와 엔터프라이즈 환경에 Intel Unite 솔루션을 배포하는 기타 고객을 대상으로 합니다.

1.2 Intel Unite 솔루션 용어 및 정의

엔터프라이즈 서버(서버) – 이 용어는 웹 서버 및 해당 서버에서 PIN 을 할당 및 분석하는 PIN 서비스를 나타냅니다. 또한 클라이언트 다운로드 페이지와 구성을 위한 관리 포털을 제공합니다.

클라이언트 – 이 용어는 허브에 연결하는 데 사용되는 장치(Windows*, macOS*, iOS*, Android* 또는 Chromebook*)를 나타냅니다.

허브 – 이 용어는 Intel Unite 응용 프로그램을 실행할 회의실에서 디스플레이에 연결하는 데 사용되는 인텔® v 프로™ 기술을 탑재한 미니 폼 팩터 PC 를 의미합니다.

FQDN – Fully Qualified Domain Name(전체 주소 도메인 이름)의 약어입니다.

플러그인 – 이 용어는 허브에 설치된 소프트웨어 구성 요소를 나타내며, 이는 Intel Unite 솔루션의 기능을 확장합니다.

IIS – Internet Information Services(인터넷 정보 서비스)의 약어이며 Microsoft*에서 제공하는 웹 서버입니다.



1.3 Intel Unite 솔루션의 새로운 기능

솔루션에 추가된 기능을 확인할 수 있도록 다음 표는 버전 1.0 이후에 추가된 기능을 요약하고 있습니다.

v 2.0	v 3.0	v 3.0 MR	v 3.1
확장된 디스플레이	Windows 용 HW 가속화 오디오/비디오 스트리밍 (20-30fps 에서 1080)	프레젠테이션용 iOS 지원	관리 포털의 향상된 사용자 경험, 설정 선택을 돕는 대화 상자 추가 등 달라진 모습
Windows 10 지원	보호된 게스트 액세스용 플러그인		관리 포털: 회의 예약
게스트 사용자 로그인 플러그인	회의 예약(단일 회의실)		관리 포털: 중재자 모드
비즈니스용 Skype 플러그인	회의 잠금		관리 포털: 고정 PIN
	보기용 iOS 지원		관리 포털: PIN 예약
			관리 포털: PIN 투명성
			관리 포털: 원격 보기 비활성화
			Chrome OS 지원
			Android 지원

2 Intel Unite 솔루션 요구 사항

2.1 엔터프라이즈 서버 요구 사항

- Microsoft Windows* Server 2008 이상
 - SSL 이 활성화된 Microsoft Internet Information Services
 - 내부 또는 공개 신뢰 루트를 포함하며 SHA2 기반 웹 서버 인증서가 필요합니다
 - Microsoft Internet Information Services 에서 구성된 SMTP 이메일 서버
 - Microsoft SQL Server 2008 R2 이상
 - Microsoft .NET* 4.5 이상
 - 4GB RAM
 - 32GB 의 여유 공간
- 참고: IIS 웹 서버 및 Microsoft SQL 데이터베이스 서버는 별도의 기기에 설치할 수 있습니다.

2.2 허브 요구 사항

- Microsoft Windows 7 SP1, 8.1 또는 10(32 비트 및 64 비트)
 - 권장 최신 패치 수준
- Microsoft .NET 4.5 이상
- 지원되는 SKU¹, 4 세대 이상 인텔® 코어™ v 프로™ 프로세서 기반 미니 PC
- 유선 또는 무선 네트워크 연결
- 4GB RAM
- 32GB 의 여유 공간

2.3 클라이언트 요구 사항

- Microsoft Windows 7 SP1, 8.1 또는 10(32 비트 및 64 비트)
 - 권장 최신 패치 수준
- Microsoft .NET 4.5 이상
- OS X* 10.10.5 이상
- iOS 9.3 이상
- 유선 또는 무선 네트워크 연결

¹ 지원되는 SKU 는 선호하는 OEM 또는 인텔 담당자에게 문의하십시오.

2.4 IT 관련 고려 사항 및 네트워크 요구 사항

허브 및 클라이언트 설치에 IT 담당 부서의 소프트웨어 배포 절차를 통해 관리되어야 합니다.

신뢰도를 위해 허브에는 유선 네트워크 연결을 사용하는 것이 좋습니다. 이렇게 하면 혼잡한 지역에서도 무선 대역폭 포화를 방지할 수 있습니다.

또한 Intel Unite 소프트웨어에서 들어오는 연결을 수락할 수 있도록 허용해야 합니다. 이 경우 허브에 설치된 방화벽에 예외를 추가해야 할 수 있습니다. 응용 프로그램 예외를 생성하는 방법에 대한 자세한 내용은 방화벽 공급업체에 문의하십시오.

생산 환경에서 FQDN(Fully Qualified Domain Name)을 사용하고 엔터프라이즈 서버로 안내하는 DNS 서비스 레코드를 설정해야 합니다. 이것은 허브와 클라이언트에서 엔터프라이즈 서버를 찾을 수 있는 가장 쉬운 방법입니다.

보안 업그레이드에 따라 응용 프로그램에서는 SHA-2 이상의 인증서만 허용합니다. 웹 서버에서 인증서를 업그레이드해야 할 수 있습니다. 설정할 때, IT 보안 팀의 도움을 받아 SHA-2 인증서를 획득하십시오.

2.4.1 모바일 클라이언트 장치

귀하의 조직에서 Intel Unite 클라이언트 OS 의 일부로 모바일 클라이언트 장치를 배포하려는 경우, 다음 사항에 유의하십시오.

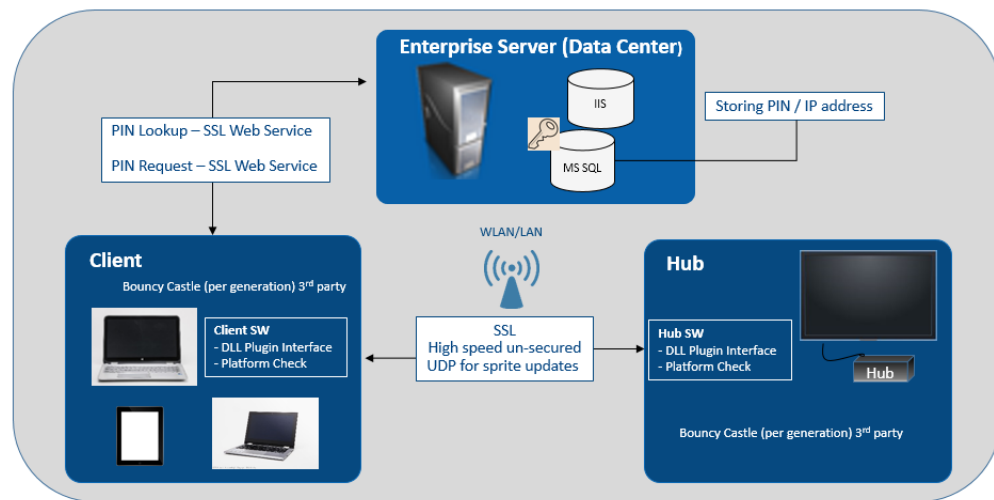
Intel Unite 솔루션에 연결하기 위해서는 iOS 및 Android 장치를 비롯한 모든 클라이언트 장치가 기업 네트워크에 연결되어 있거나 적절하게 구성된 VPN 을 사용해야 합니다. 주로 개인적인 용도로 사용되는 태블릿 및 휴대폰의 경우 기업 네트워크가 아닌 이동통신 사업자 망에 연결되어 있을 수 있습니다. 이 경우에는 기업에 연결을 허용하지 않는 방화벽으로 인해 Intel Unite 앱 세션에 연결하지 못할 수 있습니다.

IT 관리자:

- Intel Unite 앱 사용자가 개인 모바일 장치를 사용하는 경우, Intel Unite 에 연결할 수 있도록 기업 네트워크에 연결하거나 연결을 허용하는 방안을 제공하십시오.
- 이러한 개인 장치를 올바르게 관리하고 네트워크를 안전하게 보호하기 위해 필요한 도구가 있는지 확인하십시오.
- 보안 리스크를 야기할 수 있는 이러한 개인 장치를 관리할 올바른 전략을 수립하십시오.
- 개인 장치나 업무용 모바일 장치에 적용할 모바일 장치 관리 정책을 수립하십시오.
- 보호해야 할 데이터의 민감도에 따라 적정 수준의 보안이 적용되어야 합니다. 적정 보안 수준은 기업에서 어떤 데이터를 중요한 데이터로 취급하는지와 얼마나 깊이 있게 보호를 적용할 것인지에 따라 달라집니다.

3 배포 개요

Intel Unite 솔루션은 엔터프라이즈 서버, 허브 및 클라이언트의 3 가지 구성 요소로 이루어져 있습니다. 엔터프라이즈 서버는 가장 먼저 설정해야 하는 구성 요소입니다. 허브 및 클라이언트 응용 프로그램이 실행되면 엔터프라이즈 서버를 사용하여 연결 정보를 교환하고 PIN 할당을 수신합니다. 허브는 보통 회의실의 디스플레이나 프로젝터에 연결된 인텔 코어 v 프로 프로세서 기반 미니 PC입니다. 클라이언트는 허브에 표시된 지침에 따라 표시된 PIN 을 입력하여 클라이언트 소프트웨어를 다운로드하고 허브에 연결할 수 있습니다. 연결되면 클라이언트에서 콘텐츠를 프레젠테이션하고 확인하고 주석을 달 수 있으며, 동일한 허브에 연결된 다른 참가자와 파일을 공유하고 허브에 설치된 플러그인과 상호 작용할 수 있습니다. 이 다이어그램은 설치된 구성 요소의 개요를 제공합니다.



3.1 배포 리소스

설치를 완료하려면 다음이 필요합니다.

- 데이터베이스에 대한 관리 권한
- 엔터프라이즈 서버에 대한 관리 권한
- 허브에 대한 관리 권한

또한 다음이 필요할 수도 있습니다.

- SHA-2 인증서를 발급할 수 있는 IT 보안 관리자
- 방화벽 정책에 대한 IT 보안 관리자
- 허브 및 클라이언트에서 사용되는 DNS 서비스 레코드를 생성하여 엔터프라이즈 서버를 찾을 수 있는 IT 관리자(강력 권장)

4 엔터프라이즈 서버 설치

4.1 엔터프라이즈 서버 개요

엔터프라이즈 서버 설치 프로그램에는 데이터베이스, PIN 서버, 관리자 웹 포털, 클라이언트 다운로드 페이지가 포함되어 있습니다.

엔터프라이즈 서버에는 4 가지 구성 요소가 있습니다.

- 1) Microsoft SQL 데이터베이스: Intel Unite 솔루션 인프라의 모든 상태 정보를 유지 관리합니다.
- 2) 웹 서비스: 데이터베이스와 허브, 클라이언트가 통신하는 표준화된 메시지 서비스입니다.
- 3) 관리 포털 웹사이트: 허브 및 클라이언트를 관리하고, 통계를 생성하며, 모니터링 및 경고를 제공합니다.
- 4) 클라이언트 다운로드 랜딩 웹페이지: 클라이언트용 Intel Unite 소프트웨어를 포함합니다.

또한 허브 및 클라이언트는 ServerConfig.xml 파일 또는 DNS 서비스 레코드 중 하나를 사용하여 네트워크 인프라에서 엔터프라이즈 서버를 검색합니다.

이를 통해 클라이언트 및 허브에 대한 제로터치 구성이 활성화되면 DNS 서비스 레코드를 사용하는 것이 좋습니다. [DNS 서비스 레코드 생성](#) 섹션을 참조하십시오. 하지만 DNS 서비스 레코드를 획득할 수 없는 경우 엔터프라이즈 서버를 ServerConfig.xml 파일에서 구성할 수 있습니다. [ServerConfig.xml 파일의 예는 부록 B를 참조하십시오.](#)

4.2 엔터프라이즈 서버 사전 설치

- 서버가 지정된 최소 소프트웨어 및 하드웨어 요구 사항을 충족하는지 확인하십시오.
- IIS 버전 8.0 이상이 서버에 설치되어 있는지 확인하십시오. 서버 설치 프로그램에는 활성화된 IIS 가 필요하며 그렇지 않은 경우 설치 실패합니다. IIS 사용 및 설정에 관한 도움이 필요한 경우 [IIS 활성화](#) 섹션을 참조하십시오.
- IIS 관리자에서 SMTP 이메일 서버를 설정합니다.
- [이메일 서버 설정](#) 섹션을 참조하십시오.
- ASP.NET 4.5 를 설치하고 사용해야 합니다.
- IIS 에 SSL 이 활성화되어 있어야 합니다(https 사이트가 작동해야 함). **참고:** 유효한 신뢰 루트가 포함된 SHA-2 인증서를 설치하려면 IT 부서와의 협조가 필요할 수 있습니다.
- Windows 인증 또는 SQL 인증을 통해 MS SQL 에 대한 관리 액세스 권한을 보유해야 합니다. [Microsoft SQL Server 설치](#) 섹션을 참조하십시오.
- DNS 서비스 레코드를 추가하여 Enterprise Server 를 자동으로 조회할 수 있습니다. [DNS 서비스 레코드 생성](#) 섹션을 참조하십시오.

4.2.1 소프트웨어 업그레이드

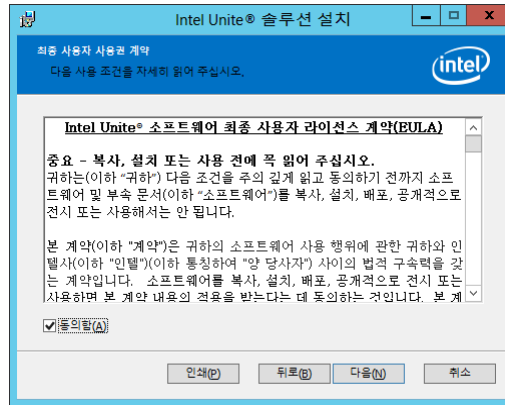
조직에서 소프트웨어 업그레이드를 수행할 경우:

- 변경 사항은 실행 취소할 수 없으므로 데이터베이스를 백업해야 합니다.
- 업그레이드 전에 데이터베이스에 대한 모든 연결을 종료해야 합니다(관리 포털에서 로그오프)
- 업그레이드 중에 로컬 및 원격 설치 모두에서 데이터베이스 옵션이 기본으로 선택됩니다(Intel Unite server.msi 가 PIN 서버에서 실행될 경우).

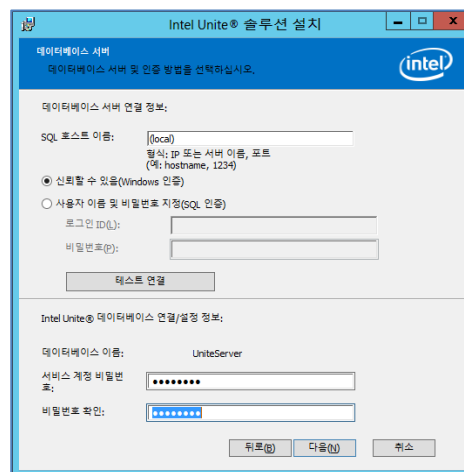
4.3 엔터프라이즈 서버 설치

이전 섹션(엔터프라이즈 서버 사전 설치)의 모든 단계를 확인하신 경우, Intel Unite 소프트웨어 설치 프로그램을 사용하여 계속합니다(이 절차는 IIS 환경을 호스트하는 서버에서 실행해야 함).

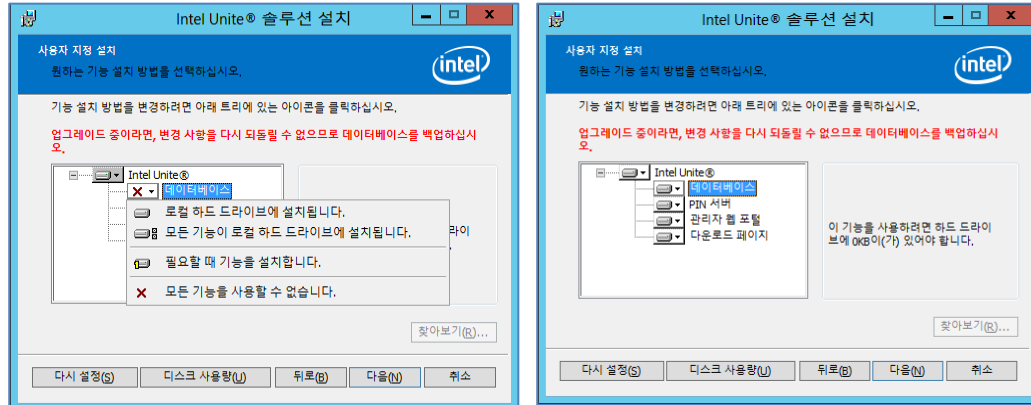
- Intel Unite Server.mui.msi 파일을 찾아 두 번 클릭하면 대상 서버에 설치할 수 있습니다.
- 설치 마법사는 데이터베이스, 웹 서비스, 클라이언트 다운로드 페이지 및 관리 포털을 설치할 수 있는 옵션을 제공합니다.
- Intel Unite Server.mui.msi 를 실행한 다음 **동의함** 확인란을 선택하여 라이선스 계약을 수락합니다.



- 다음을 클릭하여 데이터베이스 서버 창으로 이동합니다.
- 데이터베이스 서버 창에서 **데이터베이스 서버 연결 정보**를 선택합니다. 사용 가능한 옵션:
 - **SQL 호스트 이름** 확인란에서는 **(local)**이 SQL Server 에 대한 기본 값입니다. 호스트 이름을 편집하거나 기본 값으로 둡니다(SQL 이 동일한 서버에 설치되어 있는 경우, **(local)**로 둡).
 - 이미 로그인되어 있는 경우 서버에 대한 기본 값은 **신뢰할 수 있음(Windows 인증)**입니다. 데이터베이스에 액세스할 수 있는 유효한 자격 증명이 있고 SQL 인증을 선호하는 경우 **사용자 이름 및 비밀번호 지정(SQL 인증)**을 선택합니다. 후자를 선택할 경우 **테스트 연결**을 클릭하여 데이터베이스 연결을 테스트해야 합니다.
 - **데이터베이스 연결/설정 정보** 섹션에서 UniteServer 라는 새로운 데이터베이스에 액세스하는 데 사용할 **UniteServiceUser** 의 비밀번호를 생성해야 합니다. 다음 확인란에서 **비밀번호 확인**을 선택합니다.
 - 비밀번호는 8자 이상이어야 하며 하나 이상의 대문자, 하나 이상의 소문자, 하나 이상의 숫자, 하나 이상의 기호를 포함해야 합니다.



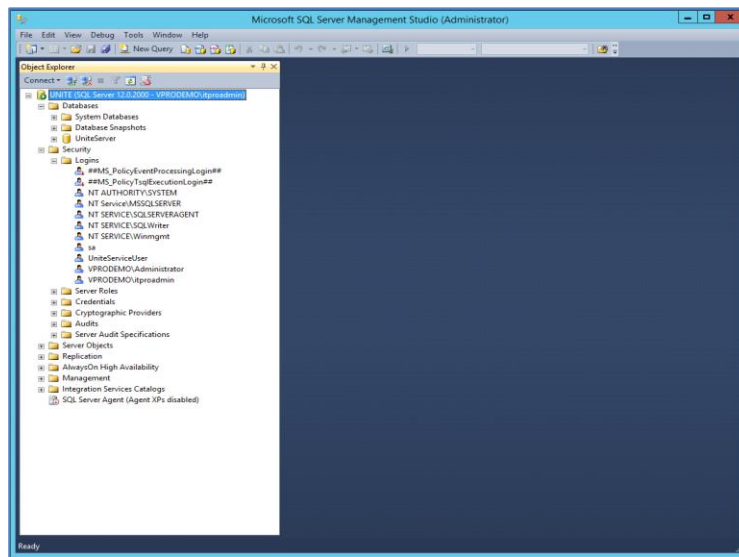
- 다음을 클릭하여 기능을 선택할 수 있는 **사용자 지정 설치** 창으로 이동합니다. 데이터베이스 기능을 확장한 다음 **로컬 하드 드라이브에 설치됩니다** 또는 **모든 기능이 로컬 하드 드라이브에 설치됩니다** 중 하나를 선택합니다. 이렇게 하면 이전 단계에서 제공된 SQL Server에 데이터베이스가 생성됩니다.



- 다음을 클릭하여 기능 선택을 확인하고 **설치**를 클릭하여 설치를 시작합니다.
- **마침**을 클릭하여 설치를 완료합니다.
- 이제 엔터프라이즈 서버가 설치되었습니다. 다음 섹션으로 이동하여 허브를 설치하십시오.

선택 사항:

- SQL Management Studio 를 사용하여 UniteServer 데이터베이스가 생성되었는지 확인하려면 서버에서 SQL Management Studio 를 연 다음 SQL Server 에 연결합니다. 왼쪽 창에서 데이터베이스를 확장하고 UniteServer 데이터베이스가 생성되었는지 확인합니다.



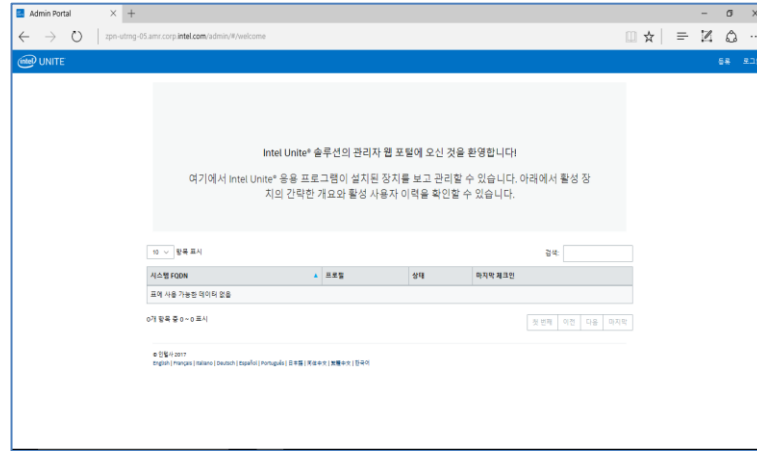
- 데이터베이스와 함께 서버 및 PIN 서버에 설치한 경우 관리 포털에 액세스하여 설치가 성공적인지 확인합니다. 링크를 따르십시오.

<https://<yourservername>/admin>

사용자 계정에 로그인하거나 기본 관리자 계정(새로운 소프트웨어 설치용)을 사용할 수 있습니다.

사용자: admin@server.com

비밀번호: Admin@1

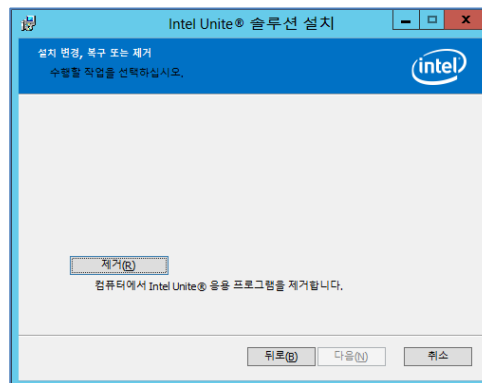


참고: 관리 포털 액세스 시 오류가 발생할 경우 문제 해결 섹션을 참조하십시오.

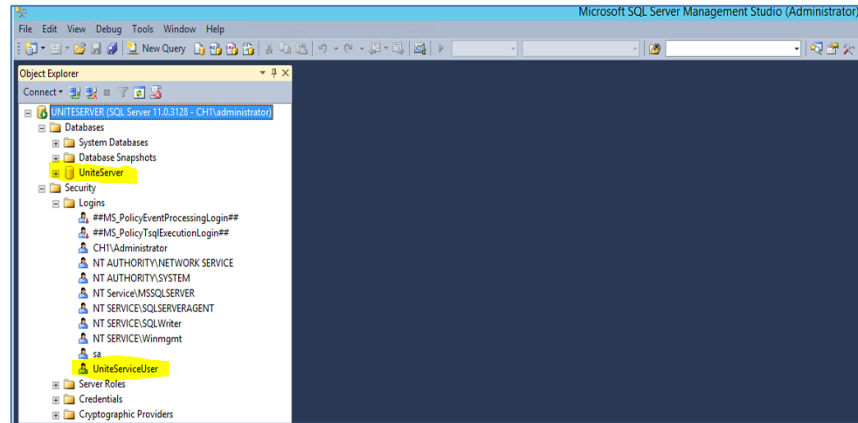
4.4 Intel Unite 응용 프로그램 제거

응용 프로그램을 제거해야 하는 경우 이전에 생성한 UniteServer 데이터베이스 및 UniteServiceUser 로그인을 삭제하여 응용 프로그램 내 충돌을 방지해야 합니다. 그 전에 **데이터베이스 백업을 생성했는지 확인합니다.**

1. 설치 프로그램 **Intel Unite Server.mui** 를 실행합니다.
2. **제거**, 다음을 차례로 클릭하여 계속 진행합니다.



3. *Microsoft SQL Server Management Studio* 로 이동한 후 **UniteServer** SQL 데이터베이스 및 **UniteServiceUser** 계정을 수동으로 삭제합니다. 아래 이미지에서 강조 표시된 영역을 확인하십시오.



5 허브 설치

5.1 허브 사전 설치

Intel Unite 응용 프로그램이 엔터프라이즈 서버에 체크인하고 통신하려면 허브 방화벽에서 제외되어야 합니다. 허브는 엔터프라이즈 서버에서 검색하고 체크인할 수 있어야 하기 때문입니다.

허브 설치 프로그램을 실행하면 DNS 서비스 레코드에서 정보를 가져오기 위해 서버 연결 정보 메시지가 표시되고 수동 조회(설치 절차에서 **서버 지정**이라고 함)을 우회하는 옵션이 제공됩니다. 허브 설치 프로그램을 실행하면 ServerConfig.xml 이 편집됩니다.

PIN 조회를 위해 선택한 방법에 따라 설치 실행 시 **자동으로 서버 찾기** 또는 **서버 지정** 선택을 사용할지 확인해야 합니다.

DNS 서비스 레코드가 존재할 경우 **자동으로 서버 찾기**를 선택하고 확실하지 않다면 **서버 지정** 옵션(수동 조회)을 사용하십시오. 이 경우 엔터프라이즈 서버의 호스트 이름을 알아야 합니다.

공개 키(다음 섹션인 [공개 키](#) 참조)로 ServerConfig.xml 을 편집한 경우 클라이언트 및 허브 설치 프로그램에 키를 다시 입력할 필요가 없습니다.

참고: 서버가 ServerConfig.xml 에서 정의된 경우 DNS 서비스 레코드에 우선합니다.

5.1.1 공개 키

공개 키는 선택 사항이며, 허브나 클라이언트에서 엔터프라이즈 서버와 통신하는 방법을 지정합니다. 비어 있거나 지정되지 않은 경우 허브와 클라이언트에서는 신뢰 루트를 검증합니다. 응용 프로그램에서 인증서를 수락하지 않으면 사용자에게 메시지가 표시됩니다.

허브 및 클라이언트에서 설치를 실행하면 공개 키가 사용됩니다. 허브 및 클라이언트용 설치 프로그램을 실행할 경우 이 키가 필요합니다. 공개 키를 확보하려면 다음 페이지로 이동하십시오.

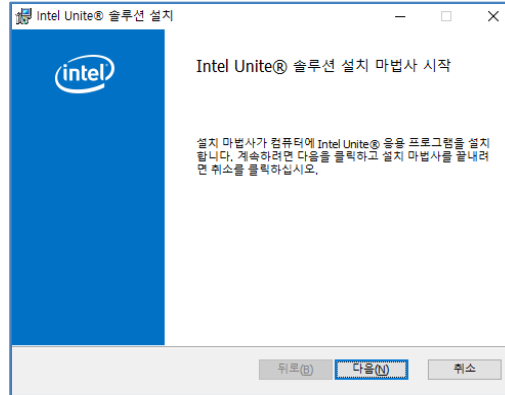
<https://yourservername/unite/ccservice.asmx>

URL 표시줄에서 잠금 표시를 클릭하여 인증서 정보를 확인합니다. 정보로 이동하여 모두 표시를 클릭한 다음 "공개 키" 필드를 아래로 스크롤하여 공개 키를 클릭하고 확인합니다. 값을 복사하여 ServerConfig.xml 파일에 붙여넣을 수도 있습니다.

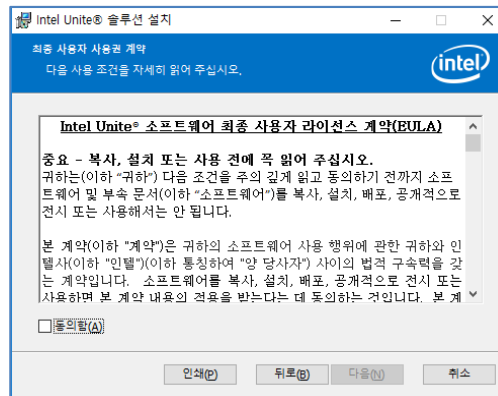
ServerConfig 파일에 붙여넣은 문자열에는 공백이 없어야 합니다. 공개 키로 ServerConfig.xml 을 편집한 경우 클라이언트 및 허브 설치 프로그램에 키를 다시 입력할 필요가 없습니다. [ServerConfig.xml 의 예](#)는 부록 B 를 참조하십시오.

5.2 허브 설치

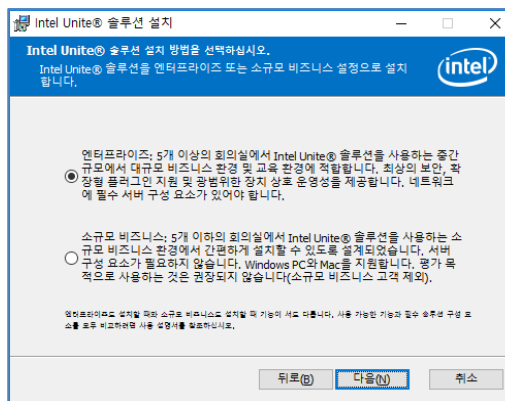
- 설치 프로그램 폴더를 찾아 허브 설치 프로그램: **Intel Unite Hub.mui.msi** 를 실행합니다.
- 다음을 클릭하여 계속합니다.



- **동의함 확인란**을 선택하고 다음을 클릭합니다.

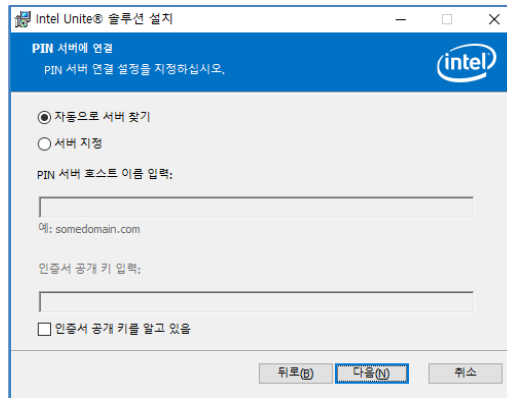


- **엔터프라이즈**를 선택하고 다음을 클릭합니다.

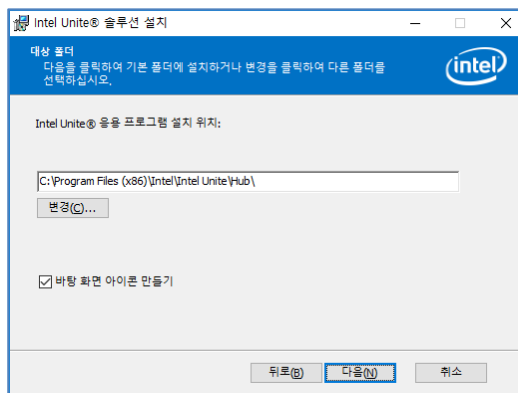


- 이 창에서 PIN 서버 연결 설정을 지정해야 합니다. 선택할 수 있는 조건은 다음과 같습니다:
 - **자동으로 서버 찾기**: 가장 권장되는 방법입니다(기본).

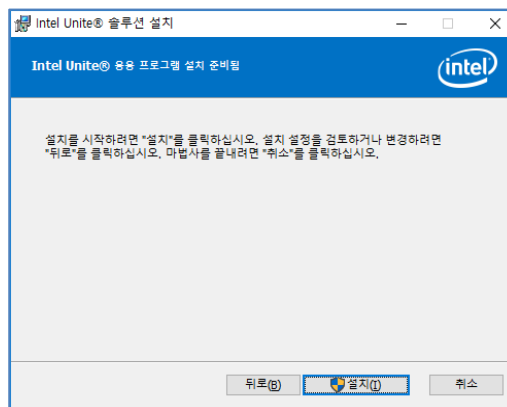
- **서버 지정:** 이 단계에서는 엔터프라이즈 서버의 호스트 이름을 알고 있어야 합니다.
 - **PIN 서버 호스트 이름을 입력합니다.**
 - **인증서 공개 키를 알고 있음** 확인란을 선택한 경우 **인증서 공개 키를** 입력합니다. 선택하고 **다음**을 클릭합니다.



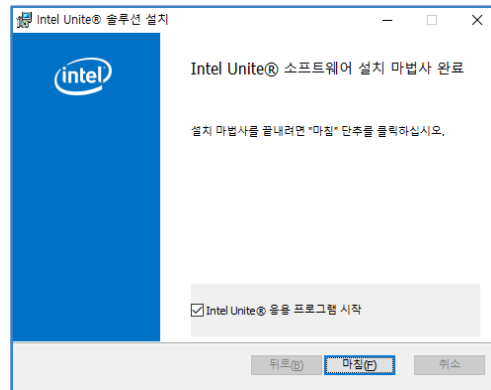
- 허브가 설치될 기본 폴더와 함께 **대상 폴더** 창이 열립니다. 원하는 경우 대상 폴더를 변경하거나 기본 위치를 유지할 수 있습니다. 이 단계에서 데스크탑 아이콘을 생성할 수도 있습니다. **다음**을 클릭하여 계속합니다.



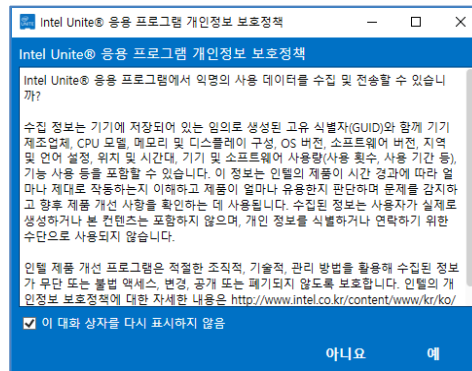
- 이 단계에서 다시 돌아가 설정을 검토하거나 **설치**를 클릭하여 계속 진행할 수 있습니다.



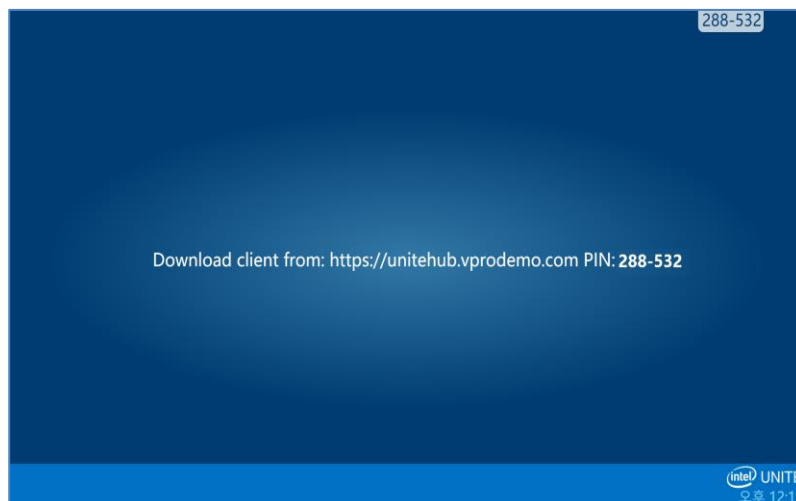
- 설치가 완료되면 **Intel Unite® 소프트웨어 설치 마법사 완료** 창이 표시됩니다. **마침**을 클릭하여 설치 절차를 완료합니다.



- 응용 프로그램을 처음 실행하면 다음과 같은 **Intel Unite® 응용 프로그램 개인정보 보호정책**이 표시됩니다.



- Intel Unite® 응용 프로그램 개인정보 보호정책은 익명의 사용 데이터를 수집하는 데 사용됩니다. 인텔은 항상 제품을 개선하기 위해 노력하고 있으며 지속적인 제품 개선을 위해 데이터를 수집합니다. **예** 또는 **아니오**를 선택한 다음 대화 상자가 다시 열리지 않도록 하려면 확인란을 선택하십시오.
- 이제 화면이나 모니터에 PIN 이 표시됩니다. 클라이언트를 허브에 연결하려면 PIN 이 필요합니다. (PIN 이 표시되지 않을 경우 [문제 해결](#) 섹션을 참조하십시오.)



5.3 허브 구성

Intel Unite 소프트웨어를 실행하는 허브의 구성 옵션은 관리 포털을 통해 수정할 수 있습니다. 관리 포털에는 기본 구성 설정과 기본 프로필이 포함되어 있으며 엔터프라이즈 서버에 체크인하는 모든 허브에 적용됩니다. 허브와 엔터프라이즈 서버의 연결이 설정되면 구성 옵션이 허브에 적용됩니다. 허브에서 체크인할 때마다 설정이 업데이트됩니다. 허브의 대부분 설정은 조직의 필요(예: 각 허브가 다른 색상, 이미지, PIN 크기를 표시할 수 있는지, 다른 플러그인이 포함되어 있는지 등)에 따라 사용자 지정할 수 있습니다.

허브 구성에 대해 자세히 알아보려면 관리 포털 설명서 섹션을 참조하십시오.

5.4 허브 추천 사례

최종 사용자에게 가능한 한 최상의 경험을 제공하기 위해 화면에 시스템 경고나 팝업이 표시되지 않고 언제든지 사용할 수 있도록 준비된 상태로 허브를 구성해야 합니다. 다음은 몇 가지 추천 사례입니다.

- Windows 가 Intel Unite 응용 프로그램이 실행되는 도메인이나 사용자로 자동으로 로그인되어야 합니다.
- 스크린 세이버가 비활성화되어야 합니다.
- 시스템이 대기 상태가 되지 않도록 설정해야 합니다.
- 시스템이 로그아웃되지 않도록 설정해야 합니다.
- 디스플레이가 꺼지지 않도록 설정해야 합니다.
- 시스템 경고가 켜지지 않도록 해야 합니다.

5.5 허브 보안

허브 관리자는 각 허브에 대해 추천 보안 사례를 따라야 합니다. 로컬 사용자가 자동으로 로그인되는 경우, 사용자는 관리자 권한으로 실행하지 않아야 합니다.

5.6 플러그인

Intel Unite 응용 프로그램에서는 플러그인 사용을 지원합니다. 플러그인은 응용 프로그램의 기능을 확장하고 사용자 경험 양식을 구현하는 소프트웨어 구성 요소입니다. 플러그인은 각 허브에 대해 고유할 수 있습니다.

다음 플러그인은 현재 Intel Unite 응용 프로그램에서 사용할 수 있습니다:

보호된 게스트 액세스용 플러그인: 이 플러그인으로 엔터프라이즈 서버 PIN 검증 없이 동일한 엔터프라이즈 네트워크에 있지 않아도 컴퓨터를 허브와 연결할 수 있습니다. 허브에서 Intel Unite 클라이언트에 연결할 수 있는 임시/호스팅된 네트워크(액세스 지점)가 생성됩니다.

Skype for Business 용 플러그인: 이 플러그인은 온라인으로 Skype 회의에 참석 중인 사람들을 Intel Unite 앱 세션에 포함시켜 주는 솔루션입니다. 플러그인은 Intel Unite 소프트웨어의 허브에서 실행되며 각 인스턴스에 해당하는 메일 계정을 관리합니다.

원격 측정 플러그인: 허브에 플러그인이 설치되어 있는 경우 엔터프라이즈 서버에서 허브 데이터를 수신하여 표시할 수 있습니다. 최소 요구 사항은 엔터프라이즈 서버 v3.0(빌드 # 3.0.38.44)입니다.

또한, 플러그인을 쓰는 데 사용하는 SDK 가 있습니다.

소프트웨어 개발 키트(SDK): 소프트웨어 개발자 또는 Intel Unite 응용 프로그램의 추가 기능을 개발하고자 하는 사람들을 지원하는 응용 프로그램 인터페이스 설명서입니다.

참고: 각 플러그인 구성 요소에 대해 자세한 내용을 확인하거나 이를 설치하고자 하는 경우 특정 플러그인 설명서를 참조하십시오.

5.6.1 플러그인 설치 참고 사항

각 플러그인은 기본적으로 설치 디렉토리 내의 디렉토리 [Program Files(x86) \Intel\Intel Unite\Hub\Plugins\PluginName (Plugin.dll)]에 설치됩니다. 플러그인은 응용 프로그램이 시작될 때 나열됩니다. 새 플러그인이 추가되면 응용 프로그램을 다시 시작해야 합니다.

플러그인을 설치하기 전에 Intel Unite 솔루션 대상 버전과의 호환성을 확인합니다[플러그인마다 요구 사항이 다르므로 특정 플러그인 설명서를 참조하십시오].

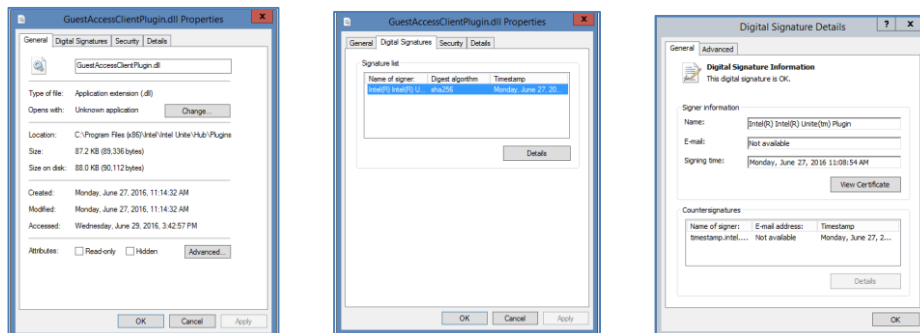
또한 사용하는 각 플러그인에 대해 관리 웹 포털에서 플러그인 인증서 해시 값을 획득하고 추가해야 합니다.

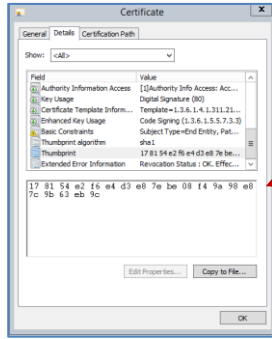
참고: 테스트 환경에서는 기본 키 값을 사용해도 되지만, 프로덕션 환경에서는 받아서 사용하는 것이 좋습니다.

5.6.2 플러그인 인증서 해시 값

플러그인의 인증서 해시 키 값을 찾으려면 다음 단계를 따릅니다.

- 플러그인 폴더에서 플러그인을 찾아 ***Plugin.dll**(예: GuestAccessClientPlugin.dll)을 마우스 오른쪽 버튼으로 클릭한 다음 **속성**을 선택합니다.
- 플러그인 **속성** 창이 열리면 **디지털 서명** 탭을 찾은 다음 클릭하여 엽니다.
- **Intel Unite 플러그인**을 선택하고 **세부 정보**를 클릭합니다.
- **디지털 서명 정보** 창에서 **인증서 보기**를 클릭합니다.
- **인증서** 창에서 **세부 정보** 탭을 선택하고 **손도장**이 보일 때까지 아래로 스크롤합니다.
- **손도장**을 선택하고 값이 표시되면 메모장이나 텍스트 파일에 복사하여 붙여 넣은 다음 공백을 제거하고 저장합니다.
- 이 키 값은 플러그인 프로필을 만들 때 사용됩니다. 프로필을 만들고 나면 키 값을 만들고 입력할 수 있습니다. 자세히 알아보려면 다음 섹션으로 계속 진행하십시오.

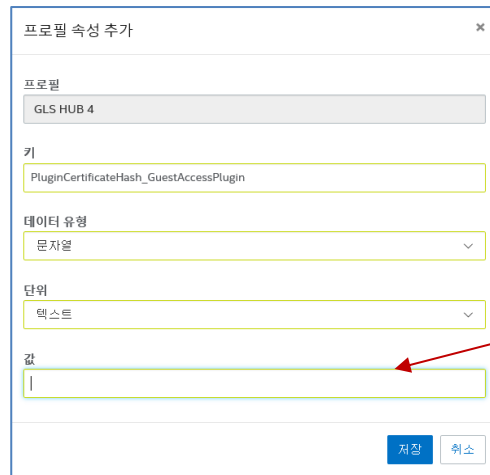




메모장이나 텍스트 파일에 값을 복사하여 붙여 넣은 다음 공백을 제거하고 저장합니다.

5.6.3 관리 웹 포털에서 플러그인에 인증서 해시 추가

관리 웹 포털로 이동하여 그룹에서 플러그인을 활성화하려는 프로필을 선택합니다. 프로필 창에서 **프로필 속성 추가**를 클릭하고 다음을 입력합니다.



이전 섹션에서 설명된 메모장 또는 텍스트 파일에 저장된 값을 사용합니다. 올바른 값(공백 없음)인지 확인합니다.

- **키:** PluginCertificateHash_XXX
 - XXX 는 해시를 추가할 플러그인의 이름입니다(예: GuestAccessPlugin). 식별을 위해 해시에 해당하는 플러그인 이름을 사용하는 것이 좋습니다.
- **데이터 유형:** 문자열
- **단위:** 텍스트
- **값:** *플러그인 인증서 해시 값* 섹션에 언급된 텍스트 파일이나 메모장에 저장한 손도장 값을 사용합니다. 키를 만들고 나면 키 값도 입력할 수 있습니다.

저장을 클릭합니다. 이 값은 **편집** 링크를 클릭하여 나중에 업데이트할 수 있습니다. 새 키가 프로필 창에 표시됩니다.

프로필: Room 111 | Plugin

10 항목 표시

키	값	
PluginCertificateHash_GuestAccessPlugin		<input checked="" type="checkbox"/>
오류 이메일 주소 전송		<input checked="" type="checkbox"/>
서비스 수신 대기 포트	0	<input checked="" type="checkbox"/>
타일 압축	85	<input checked="" type="checkbox"/>
타일 크기	128	<input checked="" type="checkbox"/>
플러그인 인증서 해시 확인	거짓	<input checked="" type="checkbox"/>

또한, 플러그인 인증서 해시 확인을 참으로 설정하여 활성화해야 합니다(기본값은 거짓).

프로필: Room 111 | Plugin

10 항목 표시

키	값	
PluginCertificateHash_GuestAccessPlugin		<input checked="" type="checkbox"/>
오류 이메일 주소 전송		<input checked="" type="checkbox"/>
서비스 수신 대기 포트	0	<input checked="" type="checkbox"/>
타일 압축	85	<input checked="" type="checkbox"/>
타일 크기	128	<input checked="" type="checkbox"/>
플러그인 인증서 해시 확인	거짓	<input checked="" type="checkbox"/>

거짓에서 참으로 또는 참에서 거짓으로 전환하여 플러그인을 활성화하거나 비활성화할 수 있습니다. 키 값으로 플러그인의 유효성을 확인할 수 있다는 사실에 유의하십시오.

플러그인 인증서 해시 확인	거짓으로 설정하면 허브에서 설치된 플러그인의 코드 서명 인증서를 확인하지 않습니다. 전체 내용은 설명서를 참조하십시오.	거짓	<input checked="" type="checkbox"/>
----------------	--	----	-------------------------------------

편집 링크를 클릭하여 값을 참로 바꾸고 저장합니다.

프로필 속성 업데이트

프로필: Room 111

키: VerifyPluginCertificateHash

데이터 유형: 플러그인

단위: 참 또는 거짓

값: 거짓 참

저장 취소



이제 플러그인 설정이 활성화되었습니다.

6 클라이언트 설치

6.1 클라이언트 사전 설치

클라이언트에서는 엔터프라이즈 서버를 찾아 체크인할 수 있어야 합니다. Intel Unite 응용 프로그램은 클라이언트 방화벽에서 제외되어 엔터프라이즈 서버에 체크인하고 통신할 수 있어야 합니다.

클라이언트 설치 프로그램을 실행하면 DNS 서비스 레코드에서 정보를 가져오기 위해 서버 연결 정보 메시지가 표시되고 수동 조회(설치 절차에서 **서버 지정**이라고 함)을 우회하는 옵션이 제공됩니다. 설치 프로그램을 실행하면 ServerConfig.xml 이 편집됩니다.

PIN 조회를 위해 선택한 방법에 따라 설치 실행 시 **자동으로 서버 찾기** 또는 **서버 지정 선택**을 사용할지 확인해야 합니다.

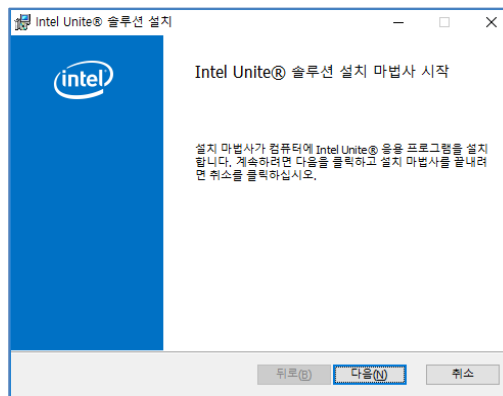
DNS 서비스 레코드가 존재할 경우 **자동으로 서버 찾기**를 선택할 수 있습니다. 잘못된 입력하는 문제를 방지하려면 자동 조회를 사용하는 것이 좋습니다. 확실하지 않다면 **서버 지정** 옵션(수동 조회)을 사용하십시오. 이 경우 엔터프라이즈 서버의 호스트 이름을 알아야 합니다.

참고: 서버가 ServerConfig.xml 에서 정의된 경우 DNS 서비스 레코드에 우선합니다.

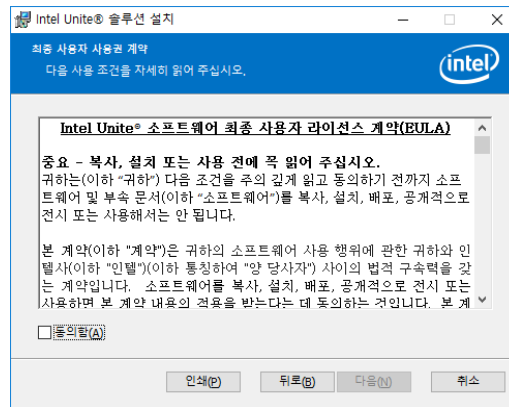
모바일 클라이언트 장치: iOS 및 Android 장치를 비롯한 모든 클라이언트 장치가 기업 네트워크에 연결되어 있거나 적절하게 구성된 VPN 을 사용해야 합니다. 주로 개인적인 용도로 사용되는 태블릿 및 휴대폰의 경우 기업 네트워크가 아닌 이동통신 사업자 망에 연결되어 있을 수 있습니다. 이 경우에는 기업에 연결을 허용하지 않는 방화벽으로 인해 Intel Unite 앱 세션에 연결하지 못할 수 있습니다. 자세한 내용은 모바일 클라이언트 장치 섹션을 참조하십시오.

6.2 Windows 클라이언트 설치

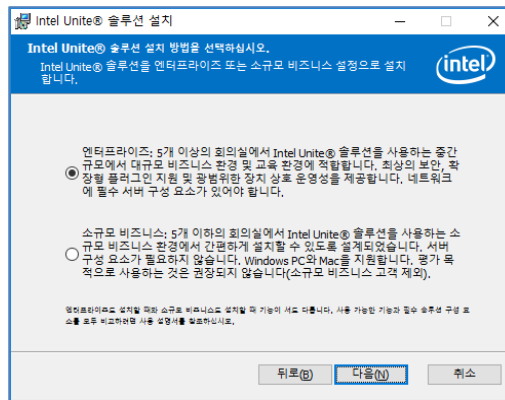
- 설치 프로그램 폴더를 찾아 클라이언트 설치 프로그램: **Intel Unite Client.mui.msi** 를 실행합니다. 다음을 클릭하여 계속합니다.



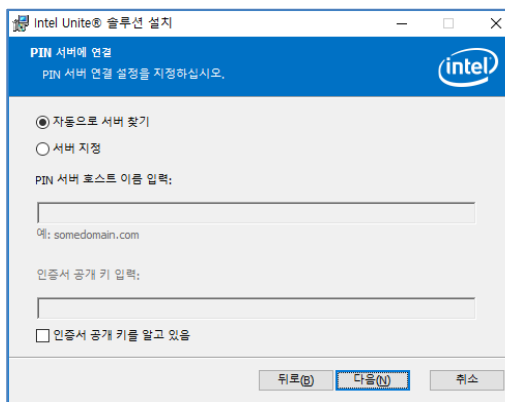
- 동의함** 확인란을 선택한 후 **다음**을 클릭합니다.



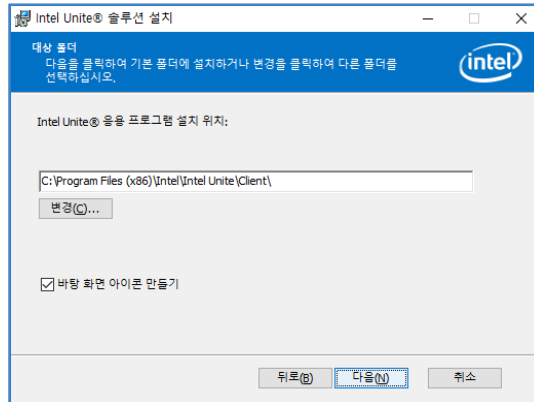
- 엔터프라이즈를 선택하고 다음을 클릭합니다.



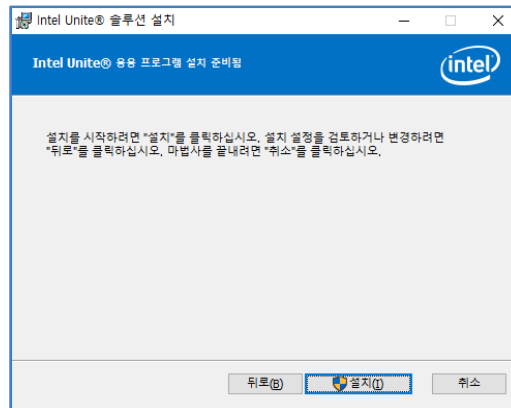
- 이 창에서 PIN 서버 연결 설정을 지정해야 합니다. 사용할 수 있는 옵션:
 - **자동으로 서버 찾기:** 가장 편리한 방법입니다(기본).
 - **서버 지정:** 이 단계에서는 엔터프라이즈 서버의 호스트 이름을 알고 있어야 합니다.
 - **인증서 공개 키 입력:** 서버 지정을 선택하면 이 옵션이 활성화됩니다.
 - **인증서 공개 키가 있어 이 방법을 선택한 경우** 이를 입력합니다.
- 선택하고 다음을 클릭하여 계속합니다.



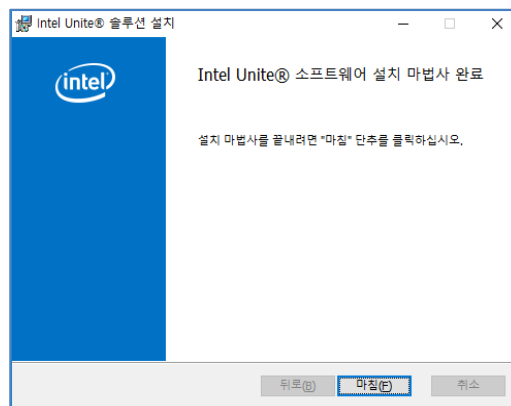
- Intel Unite 응용 프로그램이 클라이언트에 설치된 기본 폴더와 함께 **대상 폴더** 창이 열립니다. 원하는 경우 대상 폴더를 변경하거나 기본 위치를 유지할 수 있습니다.



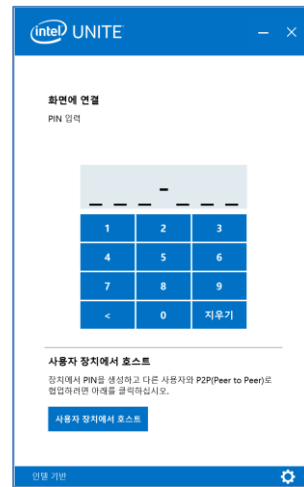
- 다시 돌아가 설정을 검토하거나 **설치**를 클릭하여 계속 진행할 수 있습니다.



- 설치가 완료되어 **Intel Unite® 소프트웨어 설치 마법사 완료** 창이 표시되면 **마침**을 클릭합니다.



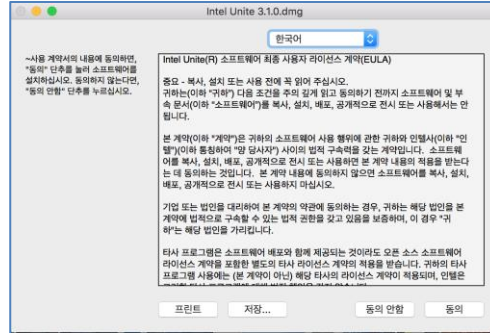
- 다음과 같은 화면에 **연결** 창이 표시됩니다.



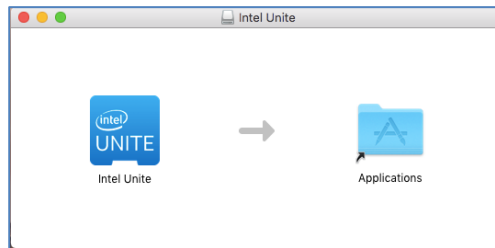
- 허브에 연결하려면 모니터 또는 화면에 표시된 PIN 번호를 입력합니다. 기본적으로 PIN 은 5 분마다 변경됩니다.
- 기능 및 사용자 정보에 대해 알아보려면 **Intel Unite® 솔루션 사용 설명서**를 참조하십시오.

6.3 macOS 클라이언트 설치

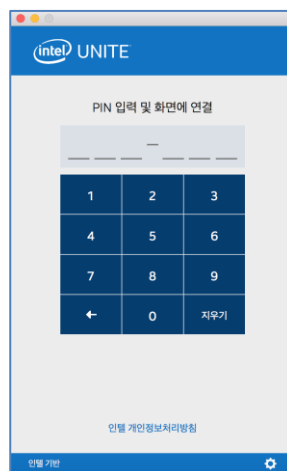
- Intel Unite macOS X,X.dmg 파일을 찾은 후 Mac 클라이언트에서 소프트웨어를 다운로드합니다. 파일을 두 번 클릭하여 응용 프로그램의 압축을 풉니다.
- 최종 사용자 라이선스 계약에 동의하는지 묻는 메시지가 표시됩니다. 계속하려면 동의를 클릭합니다.



- 압축이 풀리면 응용 프로그램 폴더에 끌어다 놓습니다.



- 응용 프로그램 폴더로 이동해서 해당 응용 프로그램을 찾은 후 클릭하여 실행합니다.
- PIN 입력 및 화면에 연결 화면이 열리면 모니터 또는 화면에 표시된 PIN 을 입력하여 허브에 연결하고 공유를 시작합니다.



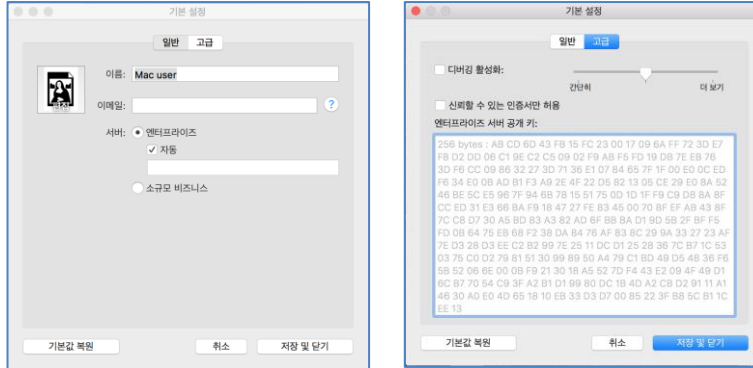
- 기능 및 사용자 정보에 대해 알아보려면 Intel Unite® 솔루션 사용 설명서를 참조하십시오.

참고: 응용 프로그램에서 DNS 자동 검색(DNS 서비스 레코드)을 사용하여 엔터프라이즈 서버를 찾습니다. 사용자의 ~/Library/Preferences 폴더에 위치한 com.intel.Intel-Unite.plist 설정을 변경하여 기본 엔터프라이즈 서버를 지정할 수 있습니다.

defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD . 자세한 내용은 이 설명서의 macOS 용 Intel Unite 솔루션 섹션을 참조하십시오.

또한, 응용 프로그램을 연결할 엔터프라이즈 서버도 변경할 수 있습니다. **연결 화면**의 오른쪽 하단에서 기어 아이콘을 클릭하여 **설정**에 액세스합니다.

2 개의 탭을 사용할 수 있습니다.



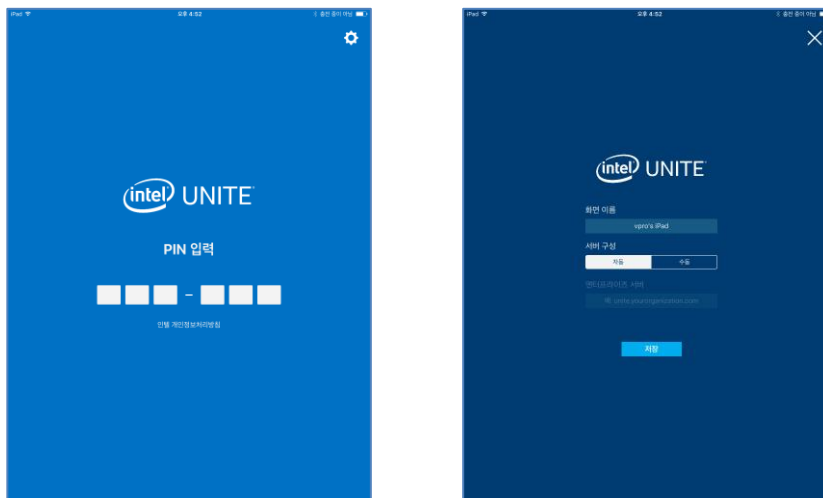
일반: 사용자의 이름, 이메일 및 아바타를 입력할 수 있습니다. 또한, 이 클라이언트 기기를 엔터프라이즈 서버에 자동으로 연결할지(기본값), 또는 정의된 서버 경로를 입력하여 연결할지 선택할 수도 있습니다.

고급: 이 탭을 통해 **디버깅을 활성화**하거나 **신뢰할 수 있는 인증서만 허용**할지 선택할 수 있습니다.

6.4 iOS 클라이언트 설치

본 앱은 2010 년형 iPad 를 제외한 모든 iPad 와 호환됩니다.

- iOS 클라이언트(예: iPad 장치)에서 Apple 앱 스토어로 이동한 뒤 클라이언트에 맞는 Intel Unite 소프트웨어를 다운로드합니다.
- 앱이 다운로드되면 이 앱을 엽니다.
- 오른쪽 상단에 있는 기어 아이콘을 클릭하여 **설정**에 액세스하고 요청된 정보를 입력합니다.



- **설정**에서 화면 이름 및 서버 정보를 입력합니다.

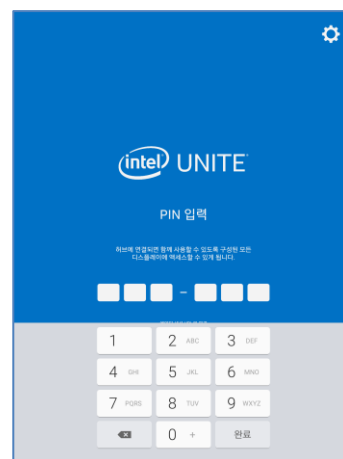
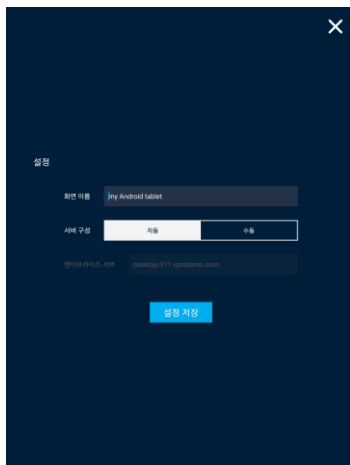
- **자동**을 선택하여 서버를 찾거나, 특정 서버에 연결하려는 경우 **수동**을 클릭하고 연결하려는 서버를 입력합니다.
- **저장**을 클릭합니다.
- 모니터 또는 화면에 표시된 PIN 을 입력하여 허브에 연결하고 공유를 시작합니다.
- 기능 및 사용자 정보에 대해 알아보려면 **Intel Unite® 솔루션 사용 설명서**를 참조하십시오.

6.5 Android 클라이언트 설치

- Android 장치에서 Google 앱 스토어로 이동한 뒤 클라이언트에 맞는 Intel Unite 소프트웨어를 다운로드합니다.
- 앱이 다운로드되면 이 앱을 엽니다.
- 오른쪽 상단에 있는 기어 아이콘을 클릭하여 **설정**에 액세스하고 요청된 정보를 입력합니다.



- **설정**에서 화면 이름 및 서버 정보를 입력합니다.
- **자동**을 선택하여 서버를 찾거나, 특정 서버에 연결하려는 경우 **수동**을 클릭하고 연결하려는 서버를 입력합니다.
- **설정 저장**을 클릭합니다.



- 모니터 또는 화면에 표시된 PIN 을 입력하여 허브에 연결하고 공유를 시작합니다.

- 기능 및 사용자 정보에 대해 알아보려면 **Intel Unite® 솔루션 사용 설명서**를 참조하십시오.

6.6 Chrome OS 클라이언트 설치

- Chromebook 장치에서 Google 앱 스토어로 이동한 뒤 클라이언트에 맞는 Intel Unite 소프트웨어를 다운로드합니다.
- 앱이 다운로드되면 이 앱을 엽니다.
- 오른쪽 상단에 있는 기어 아이콘을 클릭하여 **설정**에 액세스하고 요청된 정보를 입력합니다.



- 설정에서 화면 이름, 이메일, 서버 정보를 입력합니다. **자동**을 선택하여 서버를 찾거나, 특정 서버에 연결하려는 경우 **수동**을 클릭하고 연결하려는 서버를 입력합니다.
- **설정 저장**을 클릭합니다.

모니터 또는 화면에 표시된 PIN 을 입력하여 허브에 연결하고 공유를 시작합니다.

기능 및 사용자 정보에 대해 알아보려면 **Intel Unite® 솔루션 사용 설명서**를 참조하십시오.

6.7 클라이언트 구성

클라이언트 구성은 관리 포털을 통해 변경할 수 있습니다. 관리 포털에는 기본 구성 설정과 기본 프로필이 포함되어 있으며 서버에 체크인하는 모든 클라이언트에 적용됩니다. 클라이언트와 엔터프라이즈 서버의 연결이 설정되면 구성 옵션이 클라이언트에 적용됩니다. 클라이언트에서 체크인할 때마다 설정이 업데이트됩니다.

구성 옵션을 이해하려면 [프로필 구성](#)을 참조하십시오.

7 고급 설치

7.1 스크립트 방식의 설치 프로그램

이 섹션에서는 메뉴나 창을 표시하지 않고 자동으로 설치 프로그램을 실행하는 방법에 대한 정보를 제공합니다. 이러한 방법에서는 명령줄을 통해 자산 매개변수가 설치 프로그램으로 전달됩니다.

자동 설치 프로그램을 실행하려면 명령 프롬프트를 열고 다음 명령줄을 사용합니다.

```
msiexec /i "PATH_TO_CLIENT_MSI" PARAMETER=VALUE PARAMETER=VALUE ... /qn /!* "PATH_TO_LOG"
```

- 설치 시 지정된 MSI /i 에 플래그를 지정합니다. "PATH_TO_CLIENT_MSI"는 호출 중인 설치 프로그램의 파일 이름입니다.
- "PARAMETER=VALUE PARAMETER=VALUE ..."는 아래 표에 지정되어 있는 매개변수의 목록입니다.
- /qn 플래그가 설치 프로그램을 자동 모드로 실행합니다.
- /!* 플래그가 지정한 로그파일에 출력을 기록합니다.

참고: 명령 msiexec /?를 실행하면 **msiexec** 에 대한 모든 옵션을 볼 수 있습니다.

다음은 각 설치 프로그램에 전달할 수 있는 자산 매개 변수의 전체 목록입니다.

서버 설치 매개 변수	설명
DBHOSTNAME = "local" or "{IP}" or "{server},{port}" (로컬 기본값)	Microsoft SQL Server 의 호스트 이름입니다. 설치 프로그램이 UniteServer 데이터베이스를 생성하고 데이터베이스 서비스 계정을 추가하는 위치입니다. 데이터베이스를 현재 장치에 설치할 경우에는 이 매개 변수가 로컬 기본값이므로 포함할 필요가 없습니다.
DBLOGONTYPE = "WinAccount" or "SqlAccount" □ defaults to WinAccount	Microsoft SQL Server 에 액세스할 수 있는 로그인 유형을 지정합니다. 옵션은 Windows 인증 또는 SQL 인증입니다.
DBUSER = "{SQL username}" DBPASSWORD = "{SQL password}"	로그온 유형이 SqlAccount 이면 사용자 이름과 암호를 제공합니다. 참고: 이 계정에는 데이터베이스를 추가하고 데이터베이스 서비스 계정을 생성할 수 있는 권한이 있어야 합니다.
DBLOGONPASSWORD = "{service account password}"	UniteServer 데이터베이스에 연결할 서비스 계정에서 사용하는 비밀번호입니다.
DBLOGONPASSWORDCONF = "{service account password}"	이 변수의 값은 DBLOGONPASSWORD 에서 지정된 값과 동일해야 합니다.
서버 기능 선택 매개 변수	설명



ADDLOCAL = "ALL"	두 가지 옵션이 있습니다. ALL = 데이터베이스, PIN 서버, 관리 포털, 다운로드 페이지를 설치합니다. (이 변수를 지정하지 않음) = PIN 서버, 관리 포털, 다운로드 페이지를 설치합니다.
클라이언트 및 허브 설치 매개 변수	설명
PINSERVERLOOKUPTYPE = "Lookup" or "Manual" 조회 기본값	응용 프로그램에서 PIN 서버를 찾는 방법을 지정합니다. Manual 에는 매개 변수 PINSERVER 를 입력해야 하며 Lookup 은 DNS 서비스 레코드를 활용합니다.
PINSERVER = "{hostname}"	연결할 서버의 호스트 이름입니다.
CERTKEYCHECKED = "1" or "0" 기본값: 0	이 매개 변수는 선택 사항입니다. 0 = 인증서 키 해시를 확인하지 않음 1 = 인증서 키 해시 확인, CERTKEY 를 지정해야 함
CERTKEY = "{certificate key}"	이 매개 변수는 선택 사항입니다. PIN 서버의 인증서 공개 키를 입력합니다.
SHORTCUTS	선택 사항. "1"로 설정하면 바탕 화면 바로 가기 아이콘이 설치됩니다.
INSTALLTYPE = "Enterprise"와 "StandAlone" 값이 가능합니다.	INSTALLTYPE 이 "Enterprise"일 경우 클라이언트/허브가 엔터프라이즈로 설치됩니다. INSTALLTYPE 이 "StandAlone"일 경우 클라이언트/허브가 독립형으로 설치됩니다.
SKIP_EXTENDED_DISPLAY = "1" 또는 "0" 기본값: 0	0 = 거짓 1 = 참

7.2 레지스트리 키

설치 프로그램과 응용 프로그램을 실행할 때 레지스트리에 레지스트리 키가 작성됩니다. 원하는 결과에 따라 이러한 키의 일부 값을 조정할 수 있습니다. Intel Unite 응용 프로그램에서 작성한 키를 확인하려면 아래 목록을 참조하십시오.

레지스트리 키: (현재 사용자)	값	장치
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = 연결된 사용자 없음 1 = 연결된 사용자 있음]	허브
HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (String)	[연결 인증서의 공개 키]	모두
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (string)	[이 시스템의 현재 PIN]	허브



HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = 실행 시 개인정보 보호정책 표시 1 = 개인정보 보호정책을 표시하지 않음]	모두
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (String)	[HW 해시]	모두
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[서비스를 수신 중인 포트]	허브
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = 클라이언트 발표 중 0 = 발표 중인 클라이언트 없음]	허브
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = 응용 프로그램에 PIN 을 입력할 준비가 되었을 경우 0 = 그 외의 경우]	클라이언트
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID 참조: 게스트 액세스 플러그인 설명서	기본값으로 설정하면 게스트 액세스의 보안이 약화됩니다.	허브
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK 참조: 게스트 액세스 플러그인 설명서	기본값으로 설정하면 게스트 액세스의 보안이 약화됩니다.	허브
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download 참조: 게스트 액세스 플러그인 설명서	기본 다운로드 링크는 http://192.168.173.1/download 입니다.	허브
HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (A/V 모드 활성화/비활성화 토글)	Win7 Aero 모드. 사용자는 RTF와 WebRTC 사이를 전환할 수 있습니다.	클라이언트
레지스트리 키: (장치)	값	장치
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (String)	[허브 응용 프로그램을 종료할 수 있는 비밀번호]	허브



HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[자체 서명된 인증서에 대한 설정, 여기서 1 은 엔터프라이즈 인증서 체인을 확인하지 않음(서버 인증서)]	모두
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = 원격측정기 데이터 수집 비활성화]	모두
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (엔터프라이즈 모드가 아닌, 소규모 회사 모드에서만 작동함)	[1 = 사용자가 허브에서 창 형식의 모드를 실행하고자 하는 경우(최소화, 최대화, 종료 버튼 포함) 0 = 그 외의 경우]	허브
HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = 인증서 알고리즘 확인을 건너 뛰어야 하는 경우 0 = 엔터프라이즈 인증서가 SHA2 인증서를 사용하도록 함]	모두
HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD)	[이 키는 창 형식의 모드가 1 로 설정된 경우에만 작동합니다. 1 = 더 많은 모니터가 연결된 경우에도 1 개의 PIN 창만 표시함]	허브
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (문자열) = 심프로, 나뉘어진, 키워드, 목록	비즈니스용 Skype 플러그인에 사용되는 키	허브
HKEY_LOCAL_MACHINE\software\Intel\Unite\LogFile (String)	[런타임 디버그 메시지를 기록할 수 있는 쓰기 권한을 보유한 파일 이름 경로]	모두

8 관리 포털 설명서

관리 포털은 Intel Unite 응용 프로그램의 관리자 웹 포털로, 여기에서 Intel Unite 응용 프로그램이 설치된 장치를 확인하고 관리할 수 있습니다. 설치 시 PIN 서비스 및 웹 서버와 함께 엔터프라이즈 서버에 설치되는 구성 요소 중 하나입니다. ([엔터프라이즈 서버 설치](#) 섹션을 참조하십시오.) 관리 포털은 데이터베이스에 대한 액세스 권한을 보유하는 동안에는 데이터베이스와 동일한 서버에 있을 필요가 없습니다.

새 기능과 더불어 관리 포털이 새롭게 단장했습니다. 도움말 메뉴와 기능 정보가 추가되어 허브 및 클라이언트 장치를 원활하게 구성할 수 있습니다.

- 관리 포털에 액세스하려면 브라우저로 이동한 후 포털에 할당된 링크를 따라갑니다. 링크는 <https://<yoursevername>/admin>이며, 여기서 <yoursevername> 은 Intel Unite 서버에 할당된 이름입니다(기본 이름 = UniteServer, 예: <https://uniteserver/admin>).

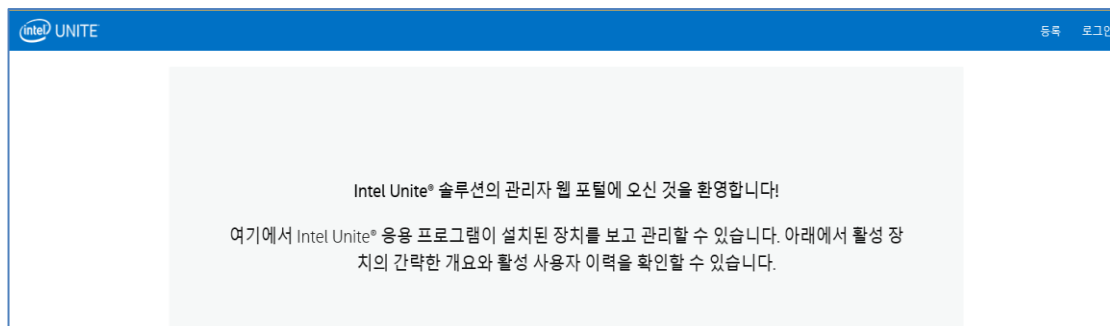
IT 관리자가 소프트웨어 설치 프로그램을 시작했을 때 다음 사용자 이름과 비밀번호로 기본 관리자 계정이 생성되었습니다:

- 사용자: admin@server.com
- 비밀번호: Admin@1

이 계정은 관리 포털에 대한 전체 액세스 권한을 보유하고 있으며 이 계정으로 로그인할 수 있지만, 시스템에서 계정을 변경하라는 메시지를 표시합니다. 이미 계정을 등록했다면 로그인 정보를 입력하여 관리 포털에 액세스하십시오.

8.1 관리 웹 포털 시작 페이지

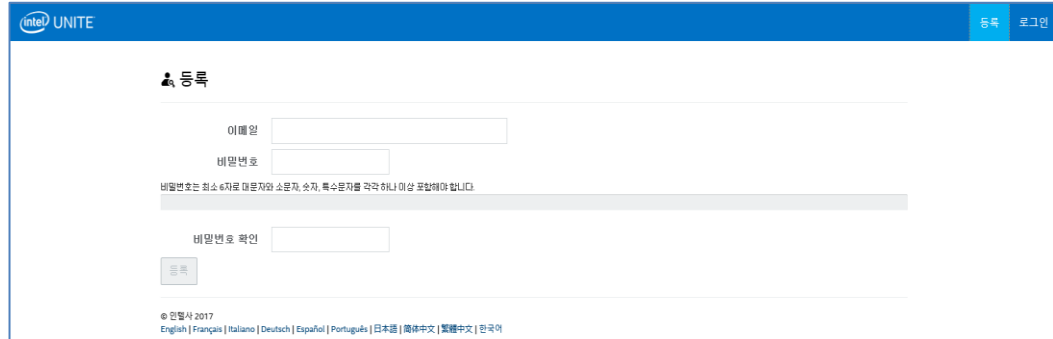
관리 포털에 연결하자마자 시작 페이지가 표시되며, 홈 페이지에 액세스하려면 설치 중 생성한 기본 계정 또는 사용자 계정 정보로 로그인해야 합니다.



8.1.1 계정 등록

계정을 등록하려면 관리 포털에서 로그아웃해야 합니다.

- 탐색 줄 오른쪽 상단에 있는 **등록** 링크를 클릭합니다.
- 원하는 이메일 주소와 비밀번호로 양식을 작성한 다음 **등록**을 클릭합니다.



- 또는 관리 포털에 로그인한 후 관리 탭을 통해 사용자를 추가/등록할 수 있습니다.

8.1.2 기존 계정으로 로그인

등록 계정으로 로그인하거나 설치 중 생성된 기본 계정을 사용할 수 있습니다. 하지만 이 계정은 관리 포털에 대한 전체 액세스 권한을 보유하고 있으므로 포털에 대한 액세스를 제한하려면 비밀번호를 변경하는 것이 좋습니다.



8.2 관리 포털 홈 페이지

홈 페이지에는 환영 메시지가 포함되어 있으며 서버에 체크인한 모든 활성 시스템(클라이언트 및 허브)에 대해 간단한 개요를 제공합니다. 이 표는 각 시스템의 이름, 각 시스템에 할당된 프로필, 켜기 또는 끄기 상태, 마지막 체크인 날짜 및 시간을 표시합니다.

Intel Unite® 솔루션의 관리자 웹 포털에 오신 것을 환영합니다!

여기에서 Intel Unite® 응용 프로그램이 설치된 장치를 보고 관리할 수 있습니다. 아래에서 활성 장치의 간략한 개요와 활성 사용자 이력을 확인할 수 있습니다.

10 항목 표시

시스템 FQDN	프로필	상태	마지막 체크인
UNITEHUB1		On	Apr 3, 2017 9:25:06 PM
UNITEHUB2		On	Apr 3, 2017 9:26:12 PM
UNITEHUB3		On	Apr 3, 2017 9:27:47 PM
UNITEHUB4		On	Apr 3, 2017 9:24:22 PM

총 4개 항목 중 1~4 표시

다양한 키워드로 검색 상자를 사용하여 표 항목을 필터링할 수 있으며 각 키워드는 모든 열을 검색합니다. <number of>개 항목 표시를 클릭하여 이 창에 표시할 항목 수를 선택할 수 있습니다. 10, 25, 50 또는 최대 100 개 항목을 볼 수 있습니다.

8.2.1 탐색 줄

탐색 줄을 통해 웹 포털의 다른 영역으로 이동할 수 있고 여기에 현재 로그인한 사용자가 표시되거나 로그인한 사용자가 없는 경우 등록이 표시됩니다.

intel UNITE 장치 그룹 관리 회의 예약 안녕하세요, admin@server.com님! 로그아웃

웹 포털 페이지 및 하위 페이지는 다음과 같습니다:

- 장치
- 그룹
 - 장치 그룹
 - 프로필
- 관리
 - 서버 속성
 - 사용자
 - 역할
 - 중재자
 - 예약된 PIN

- 원격 측정
- 회의 예약

자세히 알아보려면 관리 포털의 이 장에서 각 항목에 할당된 섹션으로 이동합니다.

8.2.2 아이콘/링크 명칭

관리 포털 전체에서 다음 아이콘 또는 링크가 일관되게 표시됩니다.

	편집
	상세 정보 보기
	장치 보기
	삭제
	특정 값에 대한 정보가 포함된 대화 상자

아이콘에 커서를 올려 놓으면 각 항목에 해당하는 정보를 볼 수 있습니다.

8.3 장치 페이지

장치 페이지에는 현재 데이터베이스에 있는 모든 장치가 포함되어 있습니다. 특정 장치를 선택하고 **보기**, **편집**, **업데이트** 또는 **제거**를 수행합니다.

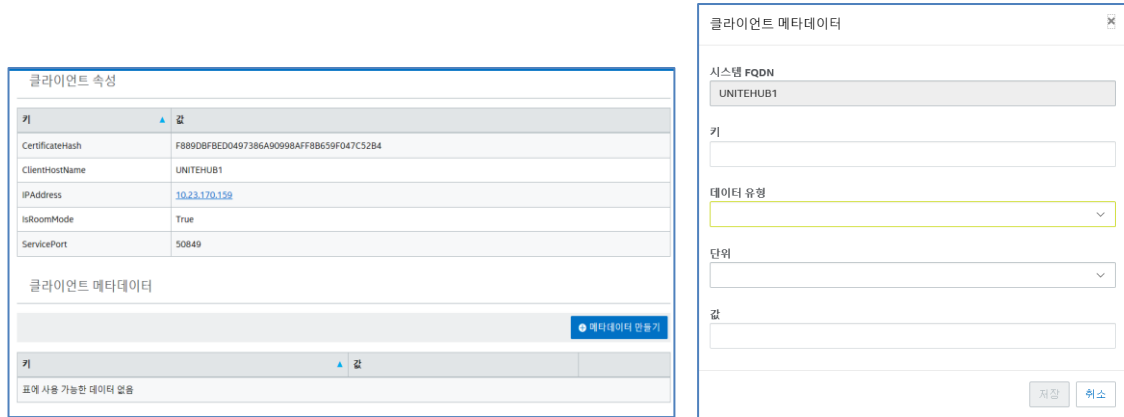
<input type="checkbox"/>	시스템 FQDN	프로필	그룹	상태	마지막 체크인	
<input checked="" type="checkbox"/>	UNITEHUB3			끄기	Apr 5, 2017 8:17:18 PM	
<input type="checkbox"/>	UNITEHUB2	TEST CLIENTS		켜기	Apr 5, 2017 8:22:47 PM	
<input type="checkbox"/>	UNITEHUB1			켜기	Apr 5, 2017 8:25:02 PM	

장치 페이지에서는 다음이 표시됩니다:

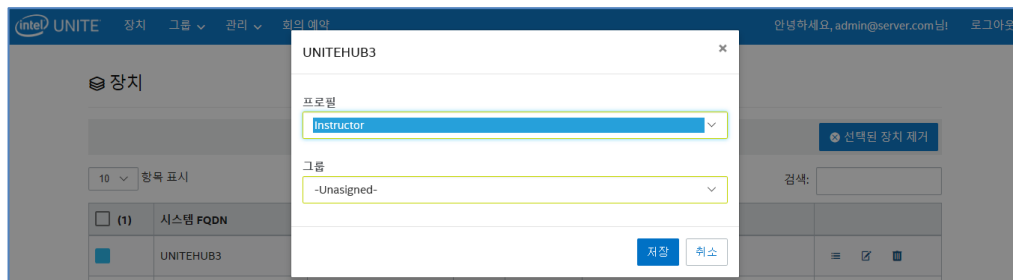
- **시스템 FQDN** 은 클라이언트/허브의 전체 주소 도메인 이름(Fully Qualified Domain Name)입니다
- **프로필**은 장치에 적용되는 구성 설정을 보유합니다
- **그룹**은 장치가 할당된 그룹의 이름입니다
- **상태**는 장치가 활성화(켜기, 녹색) 또는 비활성(끄기, 회색) 상태인지 표시합니다
- **마지막 체크인**은 장치가 서버에 마지막으로 체크인한 시간입니다
- **상세 정보:** 상세 정보 보기 링크를 클릭하면 시스템 속성 및 해당 메타데이터를 보여주는 **클라이언트 속성** 창이 표시됩니다 **클라이언트 속성**의 일부 키는 다음과 같습니다:
 - CertificateHash
 - ClientHostName

- IPAddress
- IsRoomMode
- SevicePort

각 키의 유효한 값에 대해 자세히 알아보려면 프로필 구성 섹션으로 이동하여 키와 해당 값에 대한 자세한 내용을 확인하십시오.



편집 링크 - 편집 링크를 클릭하면 장치 프로필을 편집하고 장치를 특정 그룹에 할당할 수 있습니다.



삭제 링크 - 삭제 링크를 클릭하면 관리 포털에서 장치가 제거됩니다. 장치가 제거되기 전에 확인 메시지가 표시됩니다. 또는 왼쪽 열에서 하나 또는 여러 개의 장치를 선택하고 **선택한 장치 삭제** 버튼을 클릭할 수 있습니다.

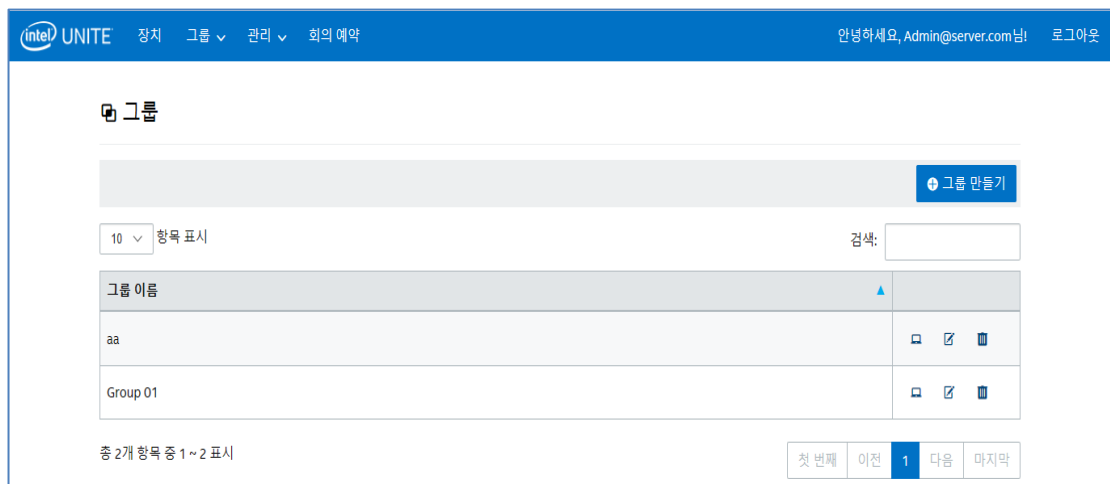
8.4 그룹 페이지

그룹 페이지는 메뉴에 **장치 그룹**과 **프로필**의 두 가지 옵션이 제공됩니다.



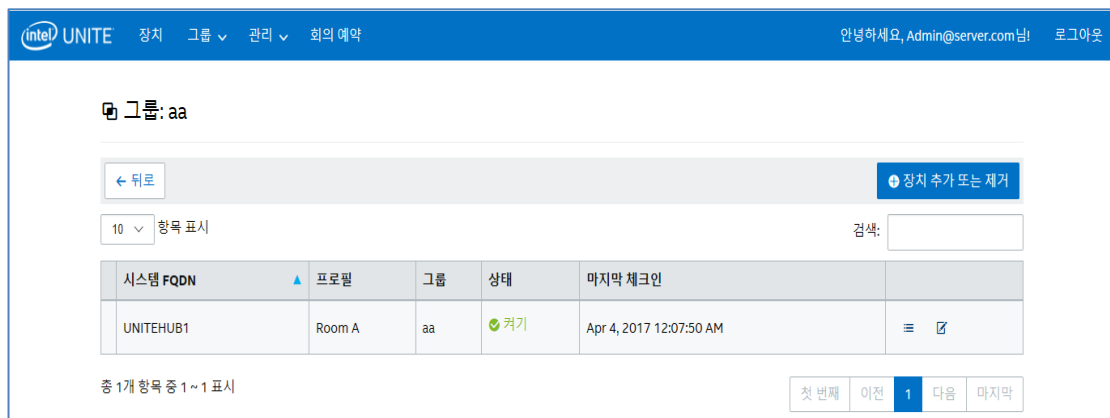
8.4.1 그룹 > 장치 그룹

장치 그룹에서는 모니터링, 기능 또는 편의성을 위해 장치를 그룹화할 수 있는 방법을 제공합니다. 그룹에 할당된 프로필이 같거나 다른 장치가 있을 수 있습니다. 이 페이지에서 그룹과 각 그룹에 대한 항목을 생성, 조회 및 삭제할 수 있습니다. **그룹 만들기**를 클릭하고 그룹 이름을 제공하면 새 그룹을 생성할 수 있습니다.



그룹이 생성되면 다음을 수행할 수 있습니다.

- **장치 보기** 링크를 클릭하여 선택한 그룹에 장치를 추가 또는 제거하거나 오른쪽 열의 **상세 정보** 링크를 클릭하여 이 그룹에 속한 각 시스템의 속성과 메타데이터를 볼 수 있습니다.



- **편집** 링크를 클릭하여 **그룹 이름**을 업데이트 또는 변경합니다.
- 변경한 후 **저장**을 클릭하여 변경 사항을 저장합니다.

8.4.2 그룹 > 프로필

이 페이지에서는 프로필을 생성, 조회 및 제거할 수 있습니다. 레이아웃과 기능은 **장치 그룹**과 유사하지만 프로필이 포함됩니다. **프로필과 그룹** 간의 차이는 프로필에는 장치 구성 옵션이 포함되어 있다는 점입니다. 장치는 여러 개의 장치 그룹에 포함될 수 있고 하나의 프로필에만 포함될 수 있습니다.

프로필 페이지에는 서버에서 사용 가능한 각 프로필의 **프로필 이름**과 **설명**이 표시됩니다. 엔터프라이즈 서버에 체크인하는 모든 장치에 프로필이 적용되며, **기본** 프로필은 관리 포털에서 삭제할 수 없습니다.

장치 보기 링크를 클릭하면 선택한 프로필에 할당된 시스템이 표시됩니다.

편집 링크를 클릭하면 프로필 이름과 해당 설명을 업데이트할 수 있습니다.

특정 프로필의 **세부 정보 보기** 링크를 클릭하면 기본 또는 새로 생성한 프로필의 키 및 값 설정에 액세스하고 편집할 수 있습니다. 각 키, 해당 값 및 **편집** 링크를 보여주는 목록이 표시되어 적절하게 업데이트 또는 사용자 지정할 수 있습니다. 키 및 해당 값에 대한 자세한 내용은 **프로필 구성** 섹션을 참조하십시오.

8.4.2.1 기본 프로필





기본 프로필은 관리 포털에서 삭제할 수 없으며, 기본 프로필을 삭제할 수 없다는 사실을 알고 다른 프로필을 생성할 수 있습니다.

시스템 FQDN	프로필	그룹	상태	마지막 체크인
UNITEHUB1	default		켜기	Apr 4, 2017 12:17:52 AM
UNITEHUB3	default		켜기	Apr 4, 2017 12:18:25 AM
UNITEHUB4	default		켜기	Apr 4, 2017 12:19:59 AM

기본 키 및 값:

키	값	
파일 전송 허용 	거짓	
오디오 비디오 스트리밍 지원 	참	
회의 중에 PIN 변경 	참	
원격 보기 비활성화 	거짓	
PIN 크기 표시 	48	
PIN 투명도 표시 	100	
차단된 파일 확장자 		
최대 파일 크기 	2147483647	
전체 화면 회의실 모드 	참	
전체 화면 회의실 모드 배경색 		
전체 화면 회의실 모드 배경 이미지 확대 	거짓	
전체 화면 회의실 모드 배경 URL 		
전체 화면 회의실 모드 지침 	{pin}	
전체 화면 회의실 모드 PIN 색상 		
전체 화면 회의실 모드 PIN 표시 	참	
전체 화면 회의실 모드 텍스트 색상 		
전체 화면 회의실 모드 텍스트 글꼴 		
허브 키보드 잠금 	거짓	
허브 시계 표시 	참	
중재자 모드 	0	
오류 이메일 주소 전송 		
서비스 수신 대기 포트 	0	
타일 압축 	85	
타일 크기 	128	
플러그인 인증서 해시 확인 	참	

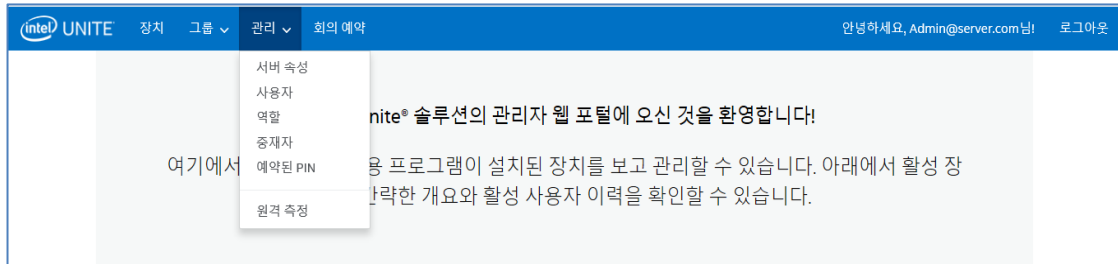
각 키 옆에는 대화 상자가 있으며 대화 상자에 커서를 올려 놓으면 키를 편집하기 전에 필요한 정보를 제공하는 각 키에 대한 값 및/또는 정보를 볼 수 있습니다. 다음 두 가지 예를 참조하십시오:

전체 화면 회의실 모드 PIN 표시 	거짓으로 설정하면 전체 화면 회의실 모드 지침에 PIN이 표시되지 않습니다.	참	
중재자 모드 	0 = 중재 없음, 1 = 자체 승격, 2 = 엄격. 전체 내용은 설명서를 참조하십시오.	0	

또한, 키와 해당 값에 대한 자세한 내용은 프로필 구성에 제공된 표를 참조할 수도 있습니다.

8.5 관리 페이지

관리 페이지는 몇 개의 하위 페이지로 구성됩니다.



- **서버 속성:** 서버 키와 값을 조회 및 수정하기 위한 인터페이스
- **사용자:** 이 페이지의 모든 계정을 추가, 제거 또는 수동으로 편집 가능
- **역할:** 새 역할을 생성하고 기존 역할을 업데이트하며 역할에 사용자를 할당하고 사용자 관리에 대한 권한을 편집할 수 있습니다.
- **중재자:** 기능을 역할로 그룹화하여 사용자가 회의를 제어할 수 있습니다. 이 섹션에서는 중재자를 쉽게 추가 또는 삭제할 수 있습니다.
- **예약된 PIN:** IT 관리자가 PIN 을 특정 회의실에 할당할 수 있습니다. PIN 을 자동 생성하거나, 열릴 세션의 요구 사항 또는 회의실 위치에 따라 IT 에서 수동으로 설정할 수 있습니다.
- **원격 측정:** 원격 측정 데이터를 보려면 Intel Unite® 솔루션용 원격 측정 플러그인을 설치해야 합니다. 원격 측정 플러그인 사용하면 IT 관리자가 Intel Unite 응용 프로그램, 그리고 각 허브에 연결된 클라이언트 장치의 사용 정보를 수집할 수 있습니다.

이 하위 페이지에 대한 상세 정보는 아래 섹션을 참조하십시오.

8.5.1 관리 > 서버 속성

이 페이지에서는 서버에 대한 키 값 쌍을 조회, 생성, 편집 및 삭제할 수 있습니다.

The screenshot shows the '서버 속성' (Server Properties) page. At the top, there is a '속성 만들기' (Create Property) button. Below it, there is a search bar with the text '10 항목 표시' (Show 10 items) and '검색:' (Search:). The main content is a table with columns '키' (Key), '값' (Value), and actions (edit and delete). The table contains the following data:

키	값	Actions
asd	sa	[Edit] [Delete]
EmailServer		[Edit]
InactiveCount	0	[Edit]
WarningThreshold	60	[Edit]

At the bottom of the table, there is a pagination control showing '총 4개 항목 중 1~4 표시' (Showing 1~4 of 4 total items) and buttons for '첫 번째' (First), '이전' (Previous), '1' (Current page), '다음' (Next), and '마지막' (Last).

관리 포털에서 사용하는 키는 다음과 같습니다:

- **EmailServer:** 서버가 알림을 전송하는 이메일입니다.
- **InactiveCount:** 첫 번째 키는 Intel Unite 응용 프로그램의 상태 모니터링 도구에서 사용되며 Notifications 역할이 할당된 사용자에게 이메일을 보냅니다.
- **WarningThreshold:** 장치가 비활성 상태인 것으로 간주되는 임계값(분 단위)을 결정하는 데 사용됩니다(기본값 60 분).

편집 링크를 클릭하여 키를 적절하게 업데이트할 수 있습니다.

8.5.2 관리 > 사용자

사용자 페이지에는 관리 포털에 등록된 모든 사용자 목록이 표시되며 해당 계정이 잠긴 경우에는 역할이 표시됩니다. 또한, 편집 링크를 클릭하여 이 정보를 업데이트할 수 있습니다.

사용자 + 사용자 만들기

10 항목 표시 검색:

이메일	사용자 계정 잠김	역할	
abc@abc.com	false	기본값	✎ 🗑
admin@server.com	false	관리자	✎ 🗑
instructor1@gmail.com	false	기본값	✎ 🗑

사용자 만들기를 클릭하고 이메일, 전화 번호 및 비밀번호를 제공하면 새 사용자를 추가할 수 있습니다. 사용자를 생성하는 중에 특정 역할을 할당하거나 기본값을 유지할 수도 있습니다. 새로운 사용자에게 액세스 권한을 할당하기 위해 역할을 정의하고 사용자를 역할에 할당할 수 있습니다.

사용자 만들기 x

이메일

전화 번호

역할

비밀번호

비밀번호는 최소 6자로 대문자와 소문자, 숫자, 특수문자를 각각 하나 이상 포함해야 합니다.

비밀번호 확인

이 페이지에서 역할(기본값 또는 관리)을 클릭하면 역할 페이지가 열립니다. 역할에 대해 자세히 알아보려면 다음 섹션으로 계속 진행하십시오.

기본 계정에 대한 참고: 기본 admin@server.com 계정에 로그인하여 새로운 사용자 계정을 추가하면 이메일 확인이 자동으로 발송되지 않습니다. 이메일 주소를 수동으로 확인하려면 새 계정에 로그인하여 탐색 줄 오른쪽 상단에 있는 “안녕하세요, <사용자 이름>님!”을 클릭한 다음 페이지 하단에서 “**이메일 확인 전송**” 버튼을 누릅니다. 그 전에 web.config.xml 파일에서 서버의 메일 설정을 편집해야 합니다. [이메일 서버 설정](#) 섹션을 참조하십시오.

8.5.3 관리 > 역할

이 페이지에는 현재 정의된 역할(**관리자** 및 **기본값**)이 표시됩니다. 새 역할을 추가하고 현재 역할을 편집할 수 있습니다. 역할만으로는 포털에 대한 액세스를 규제할 수 없습니다. 대신 포털에서의 작업(예: 사용자 생성)은 일련의 사용자와 연관된 역할로 제한됩니다.

각 역할에 할당된 활동 및 권한을 보려면 오른쪽 열의 기어 아이콘을 클릭합니다. 그러면 **사용 권한** 창이 표시됩니다. 할당된 작업은 일련의 역할이 작업을 수행할 수 있도록 사용자 지정할 수 있습니다.

새 역할을 추가하려면 **역할 만들기** 버튼을 클릭하고 역할을 편집한 다음, **역할** 페이지에서 기어 아이콘을 클릭한 후 이 역할을 수행하려는 활동을 선택합니다. 그러면 권한을 추가 또는 제거할 수 있습니다. 사용자를 여러 역할에 할당할 수 있다는 사실에 유의하십시오.

8.5.4 관리 > 중재자

이 페이지에는 중재자 역할이 할당된 사용자가 표시됩니다. 사용자를 중재자로 할당하려면 몇 가지 단계를 따라야 합니다.

중재자를 추가할 수 있는 두 가지 방법이 있습니다. **중재자 추가**를 클릭하고 요청된 데이터를 작성하거나 **CSV 에서 중재자 가져오기**를 클릭하여 목록에 추가하려는 이름과 해당 이메일이 포함된 CSV 파일을 가져올 수 있습니다. 중재자 이름이 포함된 CSV 파일을 가져올 경우 **이름, 이메일, 활동** 형식을 따르거나 **샘플 파일**을 클릭하여 유효한 형식을 확인합니다.

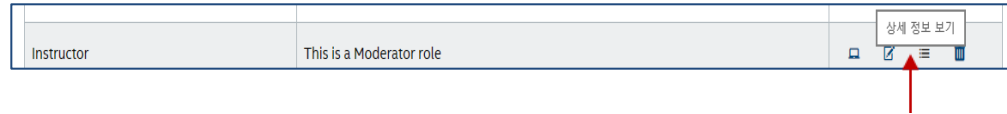
예: John Smith,jsmith@aaa.com,Add
Sandra Leon,sleon@bbb.com,Delete

중재자 추가를 클릭하여 중재자의 **이름**과 **이메일**을 직접 입력하고, 완료되면 **저장**을 클릭합니다.

중재자 기능 모드는 허브의 프로필에서 설정해야 하므로, 시스템이 혼합된 환경인 경우 다음 단계를 계속 따르십시오.

- 그룹 페이지로 이동하여 **프로필**을 선택한 후 **프로필 만들기**를 클릭하고 창이 열리면 원하는 프로필의 이름과 설명을 입력합니다.

- 프로필이 생성되면 목록에서 찾은 후 프로필 옆의 오른쪽 옆에서 상세 정보 보기를 클릭합니다.



- 키 열에서 **중재자 모드** 키를 찾은 후 이 프로필에 적용하려는 모드에 원하는 **값**을 입력합니다. 유효한 값은 아래를 참조하십시오.

프로필: Instructor | This is A Moderator Role

← 뒤로 + 프로필 속성 추가

10 항목 표시 검색:

키	값	
플러그인 인증서 해시 확인	참	
타일 크기	128	
타일 압축	85	
서비스 수신 대기 포트	0	
오류 이메일 주소 전송		
중재자 모드	0	

0 = 중재 없음, 1 = 자체 승격, 2 = 엄격. 전체 내용은 설명서를 참조하십시오.

중재자 설명 및 값:

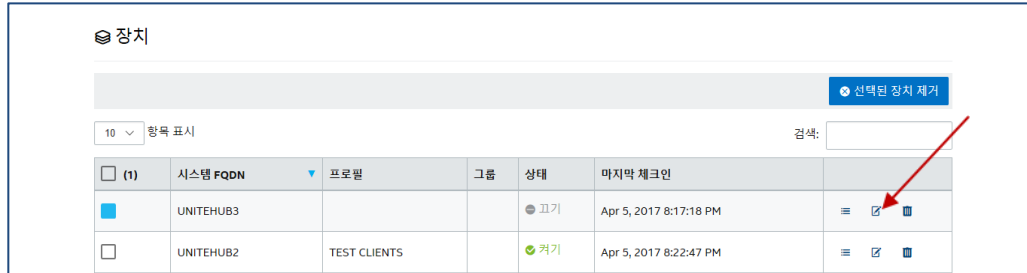
- 0- **비관리형:** 기본 모드로서, 회의/세션에 중재자가 없습니다. 모든 참가자는 보고 발표할 수 있는 동등한 권리를 가지며, 이전 Intel Unite 소프트웨어 버전(v3.1 이전)에서 이 모드를 사용했습니다.
- 1- **자체 승격:** 누군가가 중재자로 자체 승격할 때까지 회의/세션이 관리되지 않습니다. 이 경우에는 중재자만 다른 참가자를 중재자로 할당할 수 있습니다. 또한, 중재자는 세션 중 발표자를 할당할 수 있습니다.
- 2- **엄격:** 회의/세션이 지정된 중재자에 의해서만 관리됩니다. 중재자가 세션에 참가하면 이 역할로 자동 승격됩니다.

참고:

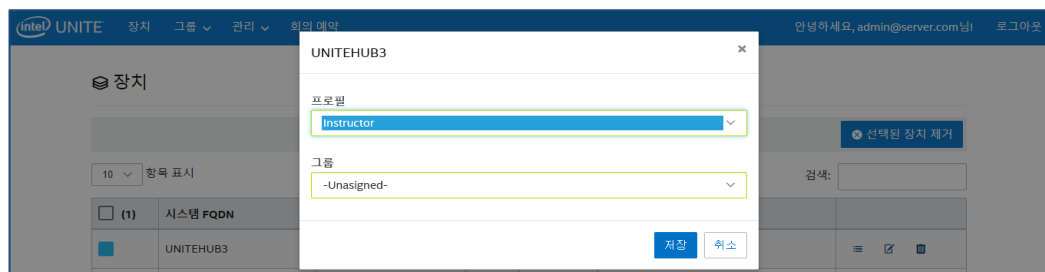
- a. 중재자 목록은 관리 포털을 통해 IT 관리자가 관리합니다. 중재자는 이메일 주소와 연결된 키를 사용하여 인증되며, 사용자가 중재자로 승격되면 관리 포털은 URI 가 포함된 이메일을 전송하고, 이 URI 를 클릭하면 클라이언트에 중재자 토큰이 설치됩니다. 사용자는 각 시스템에 대해 이 프로세스를 한 번만 진행할 수 있습니다.
- b. IT 관리자는 관리 포털에서 사용자 토큰을 제거하여 중재자 권한을 취소할 수 있습니다.
- c. 중재자에게 등록 이메일을 전송하려면 IT 담당자는 이 기능이 작동하도록 SMTP 릴레이를 구성해야 합니다.
- d. SMTP 릴레이가 없고 이메일에 전송되는 URI 를 수동으로 생성해야 할 경우 다음을 수행하십시오.
관리 탭으로 이동 후 **서버 속성**을 선택하고 **EmailServer** 옆의 **편집** 링크를 클릭한 다음 SMTP 릴레이를 입력합니다(예: smtp.example.com:22).

인증이 필요하지 않은 SMTP 릴레이만 구성할 수 있습니다. 사용자에게 대한 중재자 토큰을 가져오거나 직접 설치할 수도 있습니다. 자세한 내용은 **엄격 모드 수동 토큰 설치** 섹션을 참조하십시오.

- 선택한 허브에서 중재자 프로필을 활성화하려면 **장치** 페이지로 이동한 후 목록에서 구성하려는 허브를 선택하고 오른쪽 옆에 있는 **편집** 링크를 클릭합니다.



- 창이 열리면 **프로필** 섹션에서 중재자에 대해 생성한 프로필과 속한 그룹(있는 경우)을 선택한 후 **저장**합니다.



중재자 목록이 작성되면 선택하거나(파란색 상자) **삭제**를 클릭하여 삭제할 수 있습니다. 중재자에게 중재자로 회의/세션 참여 URL 을 전송하려면 해당 이름을 선택하고 **토큰 전송**을 클릭합니다.



8.5.4.1 엄격 모드 수동 토큰 설치

SMTP 릴레이가 없을 경우, 중재자로 추가된 사용자에게 대한 중재자 토큰을 가져와서 직접 설치할 수 있습니다. 이 작업을 수행하려면 Microsoft SQL Server Management Studio 가 설치되어 있어야 합니다.

토큰 가져오기:

- 중재자 추가
- Microsoft SQL Server Management Studio 를 열고 엔터프라이즈 서버 설치 중 사용한 관리 자격 증명을 사용하여 데이터베이스 서버에 연결합니다
- “Databases”, “UniteServer”, “Tables”를 차례로 확장합니다
- “dbo.Moderators”를 마우스 오른쪽 버튼으로 클릭하고 “Select Top 1000”을 클릭합니다
- 결과에서 이전 단계에서 추가한 것과 일치하는 “UserName”을 찾습니다
- 마우스 오른쪽 버튼으로 클릭하여 토큰을 클립보드에 복사합니다
- 메모장을 열고 URI 를 생성합니다: intelunite://localhost/SetModerationToken?Token=<전 단계의 토큰을 여기에 붙여넣으십시오>
- Intel Unite 열기
- Windows 장치: 탐색기를 열고 전체 URI 를 복사하여 붙여 넣은 후 Enter 키를 누릅니다.
- Mac 장치: Safari 를 열고 전체 URI 를 복사하여 붙여 넣은 후 Enter 키를 누릅니다.

8.5.5 관리 > 예약된 PIN

이 페이지에서는 두 가지 섹션, 즉 시스템의 **예약된** 목록과 **예약되지 않은** 목록이 표시되며, 여기에 회의/세션 중 표시된 PIN(고정 또는 변동)을 확인할 수 있습니다. IT 관리자는 선택한 회의실에 시스템을 할당할 수 있으며, 여기서 사용자는 회의 또는 세션 중 같은 PIN 을 입력하거나 순환식 PIN(기본값)을 가질 수 있습니다.

- **예약된 목록** - IT 담당자가 이미 구성한 예약 목록이며, **예약되지 않음**을 클릭하여 할당을 취소할 수 있습니다.

예약된 PIN		
예약된 목록		
10 ▾ 항목 표시	검색: <input type="text"/>	
시스템 FQDN	PIN	
Auditorium	193-345	<input type="button" value="예약되지 않음"/>
Collaboration_Room_A	999-999	<input type="button" value="예약되지 않음"/>
Hub_103	000-102	<input type="button" value="예약되지 않음"/>
Room_ABC	006-871	<input type="button" value="예약되지 않음"/>
Room_ZZZ	000-000	<input type="button" value="예약되지 않음"/>

총 5개 항목 중 1 ~ 5 표시

- **예약되지 않은 목록** - 고정 PIN 예약이 없는 시스템 목록입니다. PIN 은 직접 입력하거나, 자동 생성하거나 또는 CSV 파일에서 가져올 수 있습니다.



예약되지 않은 목록

CSV에서 PIN 가져오기 [샘플 파일](#)

10 할록 표시 검색:

시스템 FQDN	PIN
Collab_Room_B	<input type="text"/> <input type="button" value="저장"/> <input type="button" value="자동 생성"/>
Room_XYZ	<input type="text"/> <input type="button" value="저장"/> <input type="button" value="자동 생성"/>
Visitor_Centre	<input type="text"/> <input type="button" value="저장"/> <input type="button" value="자동 생성"/>

총 3개 할록 중 1 ~ 3 표시

PIN 을 할당할 경우 값을 유지하려면 **저장**을 클릭하십시오.

8.5.6 관리 > 원격 측정

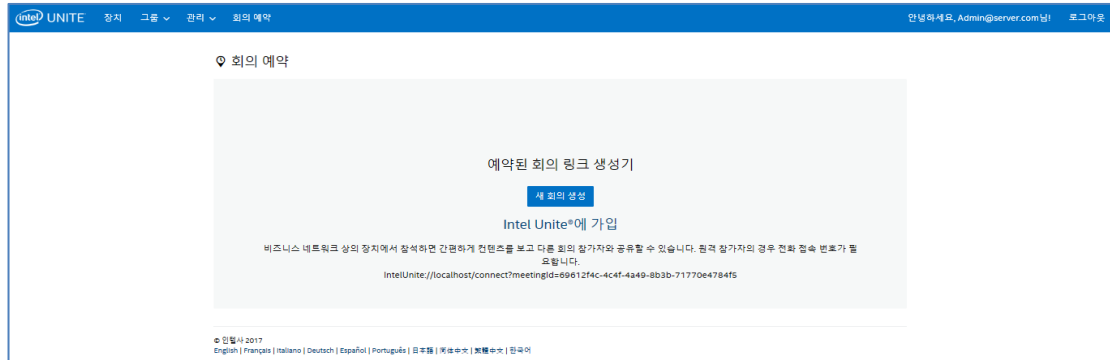
이 페이지에서는 관리 포털에서 수집한 원격 측정 데이터가 표시됩니다. 이러한 데이터를 보려면 Intel Unite® 솔루션용 원격 측정 플러그인을 설치해야 합니다. 원격 측정 플러그인 사용하면 IT 관리자가 Intel Unite 응용 프로그램, 그리고 각 허브에 연결된 클라이언트 장치의 사용 정보를 수집할 수 있습니다. IT 관리자는 각 회의실의 연결 수, 일일 연결 수, 각 연결당 소요된 시간 등의 정보를 볼 수 있습니다. 자세히 알아보고 시스템 플러그인을 배포하려면 **Intel Unite® 원격 측정 플러그인 설명서**를 참조하십시오.



8.6 회의 예약 페이지

회의 예약 페이지는 기존 Microsoft Office 용 Intel Unite 플러그인을 설치 또는 사용할 수 없는 회의/세션 참가자를 위해 회의 URL 을 생성하는 기능입니다. 모든 참가자가 이 페이지를 볼 수 있습니다.

새 회의 생성 버튼을 클릭하여 URL 을 생성한 후 회의 또는 세션에 참가하는 사용자들에게 전송하면 됩니다.



8.7 관리 포털의 기타 구성 옵션

8.7.1 프로필 구성

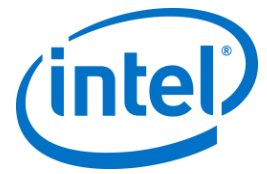
그룹 > 프로필에 액세스하고 관리 포털의 프로필에서 정보를 클릭하여 프로필을 구성할 수 있습니다. 구성 설정이 “키-값” 쌍의 형태로 표시됩니다. 값을 변경하여 응용 프로그램과 회의/세션 공간의 환경을 사용자 지정할 수 있습니다. 예를 들어 허브 디스플레이 배경 이미지, PIN 크기, 글꼴 색상, 콘텐츠와 같은 일부 설정을 사용자 지정할 수 있습니다. 프로필에서 값을 사용자 지정한 뒤 장치를 프로필에 할당하여 프로필 구성 설정을 적용합니다. 프로필을 장치에 적용하려면 장치 보기 링크와 장치 목록 업데이트를 차례대로 클릭합니다. 장치 목록이 표시되면 장치 옆의 확인란을 클릭하여 구성 설정을 적용할 수 있습니다.

표에는 사용 가능한 키, 설명, 데이터 유형 및 키에 대한 기본 값이 표시됩니다.

키	설명	데이터 유형	기본 값
파일 전송 허용	허브 또는 클라이언트의 파일 전송 기능을 활성화/비활성화하도록 플래그 지정	불리언	거짓
오디오 비디오 스트리밍 지원	Windows 사용자가 풀 A/V 환경(20-30fps 에서 1080p)에서 데스크탑을 화면에 발표할 수 있는 기능을 활성화하도록 플래그 지정	불리언	참
회의 중에 PIN 변경	회의/세션에 대한 PIN 을 잠그면 모든 사용자가 연결을 해제할 때까지 PIN 이 변경되지 않고 그대로 유지됩니다. 참 = 세션 중 PIN 을 변경할 수 있음 거짓 = 세션 중 PIN 을 잠금	불리언	참



원격 보기 비활성화	설정된 경우 특정 회의실에서 원격 보기 기능을 비활성화합니다. 사용자가 원격 보기를 사용하여 콘텐츠 보기를 시도할 경우 이 기능을 사용할 수 없다는 메시지가 나타납니다. 참 = 원격 보기 비활성화 거짓 = 원격 보기 가능	불리언	거짓
PIN 크기 표시	픽셀 단위의 크기입니다. 값은 화면 PIN 의 높이(픽셀 단위)입니다. 값이 크면 먼 거리에서도 PIN 을 읽기 쉽습니다.	정수	48
PIN 투명도 표시	모니터에 표시된 PIN 의 알파 투명도를 제어합니다. 100 = 100% 표시 1-99 = PIN 이 주변에 상자와 함께 표시되며, 불투명성은 사용한 값에 따라 변경됨 0 = PIN 이 투명함	정수	100
차단 파일 확장명이 차단된 파일 확장자로 표시됩니다	차단된 파일 확장자의 심프로 구분된 목록(예: exe, bin, msi)	문자열	비어 있음
파일 최대 크기가 최대 파일 크기로 표시됩니다.	전송할 수 있는 최대 파일 크기	정수	2147483647 바이트 (유효 범위: 0-2147483647)
전체 화면 회의실 모드	허브 전체 화면 활성화/비활성화 거짓: 오른쪽 상단에만 고정 참: 오른쪽 상단 및 전체 화면 배경에 고정	불리언	거짓
전체 화면 회의실 모드 배경색	허브에 사용되는 배경 색상입니다. HTML 색상(16 진수 색상). 올바른 값(RGB 값, 형식 #000000)의 예는 다음과 같습니다. 빨간색: #FF0000 노란색: #FFFF00 녹색: #00FF00 연파랑: #00FFFF 진파랑: #0000FF 검은색: #000000 흰색: #FFFFFF 회색: #808080	문자열	비어 있음 (검은색으로 표시)
전체 화면 회의실 모드 배경 이미지 확대	전체 화면으로 펼쳐지는 백그라운드 이미지 설정할 수 있도록 플래그 지정	불리언	거짓
전체 화면 회의실 모드 배경 URL	허브 배경을 지정된 URL 또는 이미지(jpg/png)로 설정합니다. 이 기능을 사용하려면 값을 참으로 설정	문자열	비어 있음



	예: http://myserver.com/background.jpg		
전체 화면 회의실 모드 지침	허브에 표시되는 텍스트 지침입니다. {pin} 및 {host}를 대체로 사용할 수 있음 클라이언트의 다운로드용 URL 입니다. 이 항목은 전체 화면 회의실 모드 화면에 표시됩니다.	문자열	{pin}
전체 화면 회의실 모드 PIN 색상	표시되는 PIN 색상	문자열	비어 있음 (흰색으로 표시)
전체 화면 회의실 모드 PIN 표시	지침을 표시합니다. 이 기능을 사용하려면 값을 참으로 설정	불리언	거짓
전체 화면 회의실 모드 텍스트 색상	허브에 표시되는 텍스트 색상	문자열	비어 있음 (흰색으로 표시)
전체 화면 회의실 모드 텍스트 글꼴	지침의 글꼴 이름	문자열	비어 있음
허브 키보드 잠금	다음 값 차단: 허브의 Ctrl-Esc, Alt-Tab, 참 표시줄, Windows 키, Alt-F4 참으로 설정하면 허브 잠금이 설정됩니다. 등록 키 기기에서 설정된 비밀번호 덮어쓰기 가능(REG 키 값)	불리언	거짓
허브 시계 표시	오른쪽 하단 구석에 시계 표시	불리언	참
중재자 모드	회의/세션에서 중재자 모드를 할당하며 다음 값을 사용합니다. 0 = 중재 없음 1 = 자체 승격 2 = 엄격	정수	0
오류 이메일 주소 전송	허브에서 오류 메시지를 전송할 이메일 주소 할당	문자열	비어 있음 (흰색으로 표시)
서비스 수신 대기 포트	허브에서 들어오는 연결이 통과할 포트	정수	0 (0 = 자동 할당된 포트)
타일 압축	비 AV 콘텐츠 공유 시 압축률을 조정할 수 있습니다. 압축 %가 네트워크에서 전송된 디스플레이(타일)의 변경된 부분에 적용됩니다. (높은 값일수록 대역폭을 더 많이 사용함)	정수	85 (유효 범위: 5-100)
타일 크기	비 AV 콘텐츠 공유 시 타일 크기를 조정할 수 있습니다. 화면이 덩어리로 나누어지는 타일 크기입니다. 각 타일의 크기(픽셀 단위)입니다.	정수	128 (유효 범위: 32-512)
플러그인 인증서 해시 확인	플러그인에 확인이 필요합니다. 참 = 인증서 해시 확인 거짓 = 인증서 해시 확인 안 함	불리언	참

8.7.2 PIN 새로 고침 간격

PIN의 기본 새로 고침 간격은 5분입니다. 즉, 허브에 표시되는 PIN은 5분마다 변경됩니다. 웹 서비스 사이트 가상 디렉토리 루트에서 **web.config** 파일을 수정하여 2~60분 사이에서 1분 간격으로 변경할 수 있습니다. IIS 관리자를 통해 이 기능에 액세스할 수 있습니다. 또한 Intel Unite\PinServer 디렉토리로 이동하여 파일에 액세스할 수도 있습니다. 기본적으로 C:\Program Files (x86)\Intel\Intel Unite\PinServer에 설치됩니다.

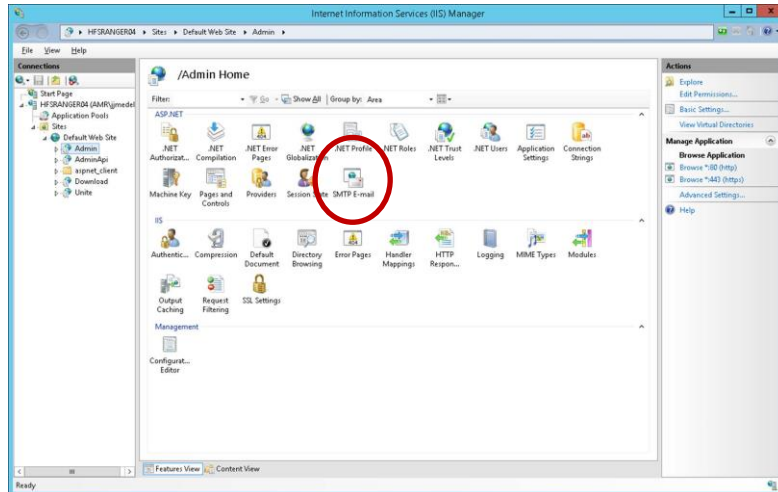
`<add key="PinExpireTimeInMinutes" value="5"></add>` 태그의 값을 원하는 새로 고침 간격으로 수정합니다.

8.7.3 이메일 서버 설정

관리 포털은 서버에 Intel Unite 응용 프로그램 설치 시 생성된 web.config.xml 파일에서 SMTP 서버를 정의합니다. SMTP 서버가 구성된 위치에 따라 web.config.xml 파일에서 **mailSettings**를 수정하면 "host"가 SMTP 서버를 가리킵니다. (Web.config.xml 파일의 기본 위치는 C:\Program Files (x86)\Intel\Intel Unite\PinServer입니다.) SMTP 이메일 서버가 IIS에서 구성되어 있고 이 설정이 엔터프라이즈 서버 사전 설치 중 응용 프로그램에 작동하기에 올바른지 확인합니다.

파일 설정은 다음과 같습니다.

```
<mailSettings>
  <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
    <network enableSsl="false" host="smtp.myco.com" port="25"
      userName="noreply@uniteserver.com" password="pass" />
  </smtp>
</mailSettings>
```



8.7.4 알림 및 모니터링

엔터프라이즈 서버에서는 알림과 모니터링이 제공됩니다. 이것은 선택 서비스이며 관리 포털에서 구성됩니다.

알림이 구성된 모든 장치가 모니터링되며 경고 임계값 내에서 체크인하지 않은 경우 지정된 사용자에게 이메일이 발송됩니다.

비활성 장치에 대한 이메일을 수신하려면 관리 포털에서 **Notifications** 역할을 사용자에게 할당해야 합니다. 장치가 모니터링되도록 선택하려면 **EnableReporting** 키를 해당 메타데이터에 추가하고 값을 **참**으로 설정합니다.

경고 임계값은 **관리 > 서버 속성**에서 구성되며 기본값은 60분입니다.

InactiveCount: 사용자가 다음 체크인 시 즉시 이메일을 받으려면 값을 낮은 숫자로 설정해야 합니다.



이메일 주소(smtp from) 및 이메일 서버(host)는 **clocktower.exe.config** 파일에서 지정해야 하며 해당 파일의 위치는 /productfiles/release/clocktower.exe.config 입니다. (clocktower.exe xml config 파일의 기본 위치는 C:\Program Files (x86)\Intel\Intel Unite\ClockTower 입니다.)

파일 설정은 다음과 같습니다.

```
<mailSettings>
  <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
    <network enableSsl="false" host="smtp.myco.com" port="25"
      userName="noreply@uniteserver.com" password="pass" />
  </smtp>
</mailSettings>
```

9 OS 및 PC 보안 제어

9.1.1 최소 보안 사항(MSS)

Intel Unite 응용 프로그램을 실행하는 모든 장치는 기본 조직 MSS 표준을 충족하고 MSS 사양에 따라 패치, 안티바이러스/IPS/IDS 및 기타 필수 제어(악성 소프트웨어, IPS, IDS 용 McAfee 호환성 테스트) 적용을 위해 에이전트를 설치해야 합니다.

9.1.2 기기 강화

Windows 부트 로더만 부팅하도록 기기 통합 확장 가능 펌웨어 인터페이스(UEFI, Unified Extensible Firmware Interface)를 잠그고(따라서 USB 디스크/DVD 부팅이 작동하지 않음), 실행 불능 비트를 활성화하며 [인텔® 신뢰 실행 기술](#)을 활성화하고 설정을 비밀번호로 잠글 수 있습니다.

Windows OS 강화: 기본적으로 시스템은 비평가 사용자 권한으로 실행됩니다. 또한 불필요한 사전 설치 소프트웨어 및 Windows 구성 요소(PowerShell, Print 및 Document 서비스, Windows 위치 제공자, XPS 서비스) 등 OS 에서 사용하지 않은 소프트웨어는 제거하는 것이 좋습니다.

GUI 하위 시스템 잠금: 시스템에서 키보드나 마우스 없이 비터치 화면만 사용하므로 GUI 하위 시스템을 분리하는 것이 어려워집니다. 침입자가 HID 장치(USB 키보드/마우스)를 부착하지 못하도록 하려면 **Alt+Tab**, **Ctrl+Shift+Esc** 및 **참표시줄**을 프로그래밍 방식으로 잠그는 것이 좋습니다.

9.1.3 기타 보안 제어

Active Directory 에서 특정 기기 계정에 따라 기기 사용자 계정을 잠그는 것이 좋습니다. 배포에 많은 유닛이 포함된 경우 특정 빌딩의 지정된 위치에 따라 사용자 계정을 잠글 수 있습니다.

기기 소유권: 각 기기에는 식별된 소유자가 있어야 합니다. 기기가 장시간 동안 오프라인 상태이면 식별된 소유자에게 이를 알립니다.

인텔 v 프로 플랫폼과 Intel Unite 소프트웨어 자체에서 제공되는 보안 메커니즘뿐 아니라, Microsoft 의 기기 강화용 가이드라인에 따라 Microsoft* Windows* OS 를 강화하시기 바랍니다. 자세한 내용은

<https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx> 링크를 통해 Microsoft

SCM(Security Compliance Manager*)에 문의하십시오.

참고: 링크 정보에는 마법사 기반 강화 도구가 포함되어 있으며, 이 도구에는 강화에 대해 잘 알려진 방법과 관련 설명서가 제공됩니다.

10 유지 관리

조직 및 IT 관리자가 정기적인 유지 관리 프로그램을 결정합니다. 다음과 같은 유지 관리 작업을 수행하는 것이 좋습니다.

10.1 야간 재부팅

매일(심야 시간대 선호) 허브를 재부팅하고, 재부팅 전에 캐시된 임시 파일 삭제, 표준 패치 적용 실행과 같은 유지 관리 작업을 실행해야 합니다.

10.2 패치 전략

가능하다면 위에서 설명한 야간 재부팅 전에 표준 패치 메커니즘을 무인 모드(GUI 프롬프트 없음)로 실행합니다.

10.3 보고

조직의 요구에 맞게 기기 가동 시간 표시기를 수집하고 맞춤 구성된 보고서를 생성합니다.

10.4 모니터링

기기 심박수를 기준으로 하는 상태 추적 시스템을 사용하며 필요에 따라 백엔드 가동시간을 분석합니다.

10.4.1 백엔드 모니터링:

표준 가상 서버 모니터링 도구를 사용하여 두 번째 수준 지원으로 알림을 전송합니다.

11 macOS 용 Intel Unite 솔루션

11.1 배경

macOS 용 Intel Unite 소프트웨어는 기본 앱 패키지로 구성되어 있으며 IT 별 기본 설정 값을 활용할 수 있습니다. 이런 방식으로 앱에서는 일반적인 Mac 관리 소프트웨어 및 기술의 각종 일반 배포에서부터 수동 설치와 기본 설정까지를 지원합니다.

11.2 일반 연결 워크플로

기본적으로 앱에서는 DNS 자동 검색(예: DNS SRV 레코드)을 사용하여 연결할 수 있는 적절한 엔터프라이즈 서버를 판단합니다. 전체적인 워크플로는 다음과 같습니다.

- (선택 사항) 기본 설정에서 정의된 엔터프라이즈 서버
- 다음 도메인에 대한 자동 검색:
 - `_uniteservice._tcp`
 - `_uniteservice._tcp.yourSubDomain.yourDomain.yourTLD`
 - i. 예: `_uniteservice._tcp.corp.acme.com`
 - `_uniteservice._tcp.yourDomain.yourTLD`
 - i. 예: `_uniteservice._tcp.acme.com`
 - 실패할 경우 HTTP 에 이어 HTTPS 에 대한 연결 시도
- `uniteservice.yourDomain.yourTLD`

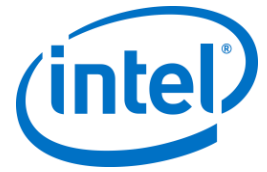
11.3 기본 설정 값

IT에서는 다음 설정을 각 사용자의 `~/Library/Preferences` 폴더에 있는 `com.intel.Intel-Unite.plist` 로 설정하여 자체 인프라나 보안 요구 사항을 충족시킬 수 있도록 Intel Unite 앱을 수정 및 사용자 지정할 수 있습니다.

- **기본 엔터프라이즈 서버 정의**
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD
- **인증서 피닝을 위한 엔터프라이즈 서버 공개 키 정의**
defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "Public Key String"
- **클라이언트에서 신뢰할 수 있는 서버 인증서만 허용**
defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true
- **클라이언트를 독립 실행형 모드로 연결**
defaults write com.intel.Intel-Unite Standalone -bool true

이러한 설정은 macOS 터미널(/Applications/Utilities)을 열고 반환 값에 이어 명령어를 입력하면 수동으로 설정하거나 수정할 수 있습니다. 각 명령에 대한 논의 및 세부 정보는 다음과 같습니다.

- **기본 엔터프라이즈 서버 정의**



기본 엔터프라이즈 서버 설정으로 자동 검색 프로세스가 중단됩니다. Mac 클라이언트가 네트워크에 단독으로 존재할 경우 이는 보안상의 이유 또는 문제 해결을 위해 Intel Unite 앱을 특정 엔터프라이즈 서버에 고정할 수 있는 유용한 설정일 수 있습니다.

- **인증서 피닝을 위한 엔터프라이즈 서버 공개 키 정의**

자동 검색의 사용 여부와 관계 없이 클라이언트 응용 프로그램을 엔터프라이즈 서버에 고정하려면 각 클라이언트에 '공개 키 문자열(Public Key String)'을 설정해야 합니다. 이 값을 얻으려면

- 기업 네트워크에 있는 Mac 에서 Safari 를 엽니다.
- 엔터프라이즈 서버의 HTTPS 주소로 이동합니다.
- 주소 표시줄의 잠금 아이콘을 클릭합니다.
- 인증서 시트에서 **인증서 표시** 버튼을 클릭합니다.
- **세부 정보** 펼침 삼각형을 클릭하여 확장합니다.
- **공개 키 정보 > 공개 키** 필드가 표시될 때까지 인증서 데이터를 아래로 스크롤합니다.
- "256 bytes:"로 시작하는 데이터 필드를 클릭합니다.
- 데이터 필드가 펼쳐집니다.
- 마우스 선택 또는 CMD+A 로 이 필드의 모든 데이터를 선택합니다.
- 컨텍스트 메뉴에서 **복사**를 선택하거나 **CMD+C** 를 이용하여 데이터를 클립보드에 복사합니다.
- 기본 명령에서 **공개 키 문자열(Public Key String)**을 클립보드의 데이터로 교체합니다. 참고: 큰 따옴표(")로 데이터를 묶어야 합니다.

기본 엔터프라이즈 서버를 정의하는 것처럼, 이 옵션을 설정하면 사용자 기반을 다른 파트너/위치에 있는 Intel Unite 솔루션 설치에 연결하는 것이 어려워집니다.

- **클라이언트에서 신뢰할 수 있는 서버 인증서만 허용**

특정 엔터프라이즈 서버를 정의하거나 인증서 공개 키를 고정하는 것뿐 아니라 Intel Unite 앱이 인증서 신뢰 체인에서 완전히 허용한 서버/인증서에 대한 연결만 허용하도록 설정할 수 있습니다. 이와 관련하여 Apple 에서 키체인에 정의한 대로 엔터프라이즈 서버 인증서가 공개 루트 서버를 다시 팔로우하도록 하거나 각 클라이언트에 필요한 자체 루트 서버 인증서와 매개 인증서를 설치해야 합니다

- **클라이언트를 독립형 모드로 연결**

이 모드를 설정하면 연결 워크플로를 변경하여 엔터프라이즈 서버가 없는 환경에서 PIN 을 생성한 허브의 UDP 자동 검색을 수행할 수 있습니다. 이 시나리오에서는 인텔 코어 v 프로 프로세서 기반 시스템이 기본 호스트의 역할을 수행하며 이는 엔터프라이즈 서버 인프라를 설치할 IT 부서가 없는 중소기업용 기업 환경에서 유용합니다. 이 모드는 UDP 패킷이 차단되지 않은 동일한 서브넷의 시스템에서만 작동합니다.

11.4 일반 배포 방법

자동 검색을 사용하면 배포가 Intel Unite 응용 프로그램을 응용 프로그램 폴더로 드래그하는 것만큼 간단해질 수 있습니다. 좀 더 복잡하거나 추가적인 보안 설정이 필요한 환경에서는 앱 패키지 배포와 관련하여 특정 기본 사항을 설정하고자 할 수 있습니다. 다양한 방법이 있으며 그 중 다음과 같이 일반적인 방법이 있습니다.

- Bash 스크립트
 - 앱 패키지와 관련하여 사용자에게 배포될 수 있는 Bash 스크립트에서 기본 설정을 정의할 수 있습니다.
- PackageMaker 를 통한 사용자 지정 설치 패키지
 - pre 또는 postflight 스크립트를 통해 기본 설정을 정의할 수 있습니다.



- Apple 원격 데스크탑을 통한 사용자 지정 설치
 - Apple 원격 데스크탑을 사용하여 Intel Unite 앱 패키지를 설치하고 **UNIX 명령 보내기...** 메뉴를 통해 모든 기본 설정을 정의할 수 있습니다.
- 엔터프라이즈 Mac 관리 소프트웨어를 통한 사용자 지정 설치
 - 다음과 같은 일반적인 엔터프라이즈 Mac 관리 솔루션을 통해 설치 및 제거가 가능합니다.
 - Casper / Bushel
 - Puppet
 - Munki
 - Chef
 - 등

12 문제 해결

12.1 Intel Unite 응용 프로그램을 서버에 설치한 뒤에 관리 포털 페이지에 접속할 수 없음

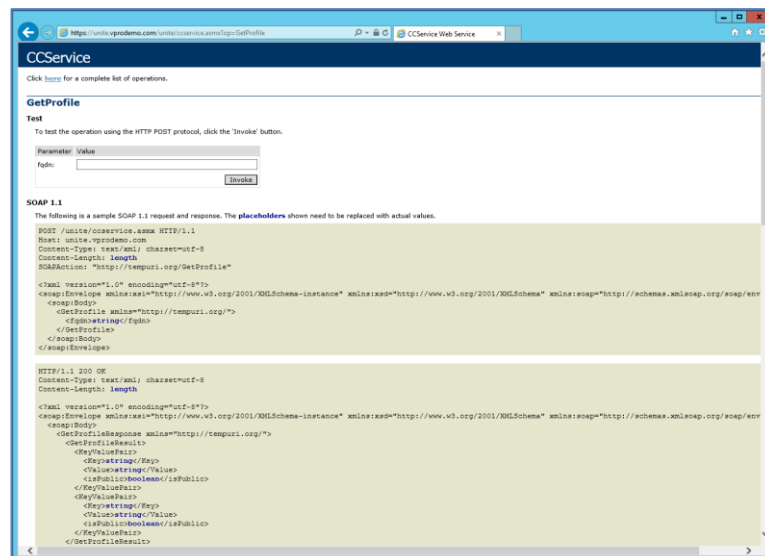
해결 방법/솔루션: 웹 서버에 필요한 역할과 기능을 서버에 추가해야 합니다.

- 서버 관리자를 사용하여 서버에 역할 및 기능 추가
 - 서버 역할: 웹 서버
 - 관리 도구 포함
 - .NET Framework 3.5 기능 추가
 - .NET Framework 4 기능 추가
 - ASP.NET
 - WCF 서비스
 - HTTP 활성화
 - 웹 서버 역할:
 - 웹 서버, 일반적인 HTTP 기능 및 기본 문서

12.2 관리 포털에 액세스할 수 없음

Web.config 의 특정 xml 태그에 대해 관리 포털에 액세스할 때 오류 페이지가 표시되는 경우, 포털 가상 디렉토리의 최상위 수준에 있는 Web.config 에서 태그를 제거하십시오(IIS 관리 콘솔에서 액세스 가능).

- 다음 링크에 따라 웹 서비스 설치에 성공했는지 확인하십시오:
<https://<yourservename>/unite/ccservice.asmx>
 - **GetProfile** 을 선택합니다.
 - **값** 필드에 **test** 를 입력하고 호출을 누릅니다.



- xml 파일에서 아래와 같이 기본 프로필을 볼 수 있어야 합니다. 이는 PIN 서비스에서 데이터베이스에 액세스하여 데이터를 성공적으로 가져올 수 있음을 의미합니다.

```

<?xml version="1.0" encoding="UTF-8"?>
- <ArrayOfKeyValuePairs xmlns="http://tempuri.org/" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:inst="http://www.w3.org/2001/XMLSchema-instance">
  <KeyValuePairs>
    <Key>AllowTransfer</Key>
    <Value>false</Value>
    <Public/>
  </KeyValuePairs>
  <Key>AudioVideoStreamingSupport</Key>
  <Value>true</Value>
  <Public/>
  <Key>ChangePinDuringTesting</Key>
  <Value>true</Value>
  <Public/>
  <Key>DisableRemoteView</Key>
  <Value>false</Value>
  <Public/>
  <Key>DisplayPinSize</Key>
  <Value>48</Value>
  <Public/>
  <Key>DisplayPinTransparency</Key>
  <Value>100</Value>
  <Public/>
  <Key>FileBlockedExtensions</Key>
  <Value></Value>
  <Public/>
  <Key>FileMaxSize</Key>
  <Value>2147483647</Value>
  <Public/>
  <Key>FullScreenRoomMode</Key>
  <Value>true</Value>
  <Public/>
  <Key>FullScreenRoomModeBackgroundColor</Key>
  <Value></Value>
  <Public/>
  <Key>FullScreenRoomModeBackgroundImageStretch</Key>
  <Value>false</Value>
  <Public/>
  </ArrayOfKeyValuePairs>
  </xml>

```

12.3 허브 응용 프로그램 실행 시 오류

오류 ID 를 나타내는 팝업 창이 나타납니다. ID 를 기준으로 오류 속성을 확인할 수 있습니다.

12.3.1 오류 ID 333333 의 플랫폼 확인 실패

이 오류는 허브가 플랫폼 확인을 통과했지만 코드 서명된 인증서를 확인할 수 없다는 것을 나타냅니다. 대체로 업데이트된 루트 인증서가 없는 OS 로 인해 발생하므로 공개 Intel Unite 코드 서명 인증서는 검증할 수 없습니다. 시스템을 인터넷에 연결하고 브라우저를 연 뒤 <https://www.microsoft.com> 으로 이동하십시오(웹사이트 연결이 시스템에서 루트 인증서를 업데이트함).

12.3.2 오류 ID 666666 의 플랫폼 확인 실패

이 오류는 플랫폼과 Intel Unite 응용 프로그램이 호환되지 않음을 나타냅니다. OEM 공급업체에 문의하여 응용 프로그램 실행이 지원되는 플랫폼인지 확인해야 합니다.

12.4 허브가 PIN 서버에서 PIN 을 가져오지 않음 - 스크롤 대시 표시됨

디버그 스위치가 있는 허브에서 Intel Unite 응용 프로그램을 실행합니다. 즉, 명령 프롬프트에서 응용 프로그램이 저장되어 있는 폴더로 이동한 다음 **IntelUnite.exe /debug** 를 실행합니다.

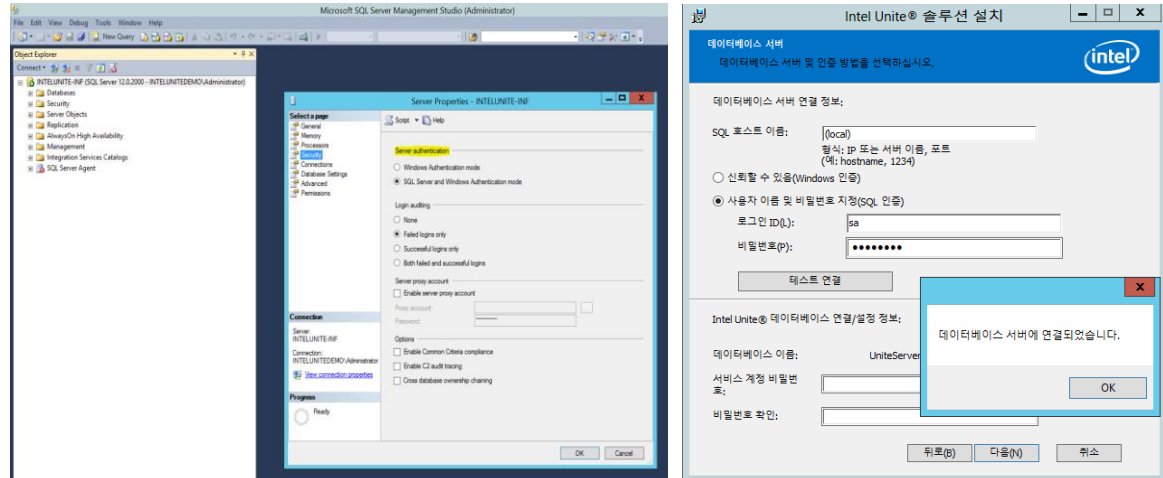
이렇게 하면 디버그 창이 열리고 연결 정보가 표시됩니다. 일반적인 오류와 해결 방법은 아래에서 설명합니다. 디버그 정보에 이러한 오류가 표시되면 솔루션/해결 방법에 따라 문제를 해결하고 허브에 PIN 을 가져올 수 있습니다.

12.4.1 서버에서 요청을 처리할 수 없음; 사용자 "UniteServiceUser" 로그인 실패

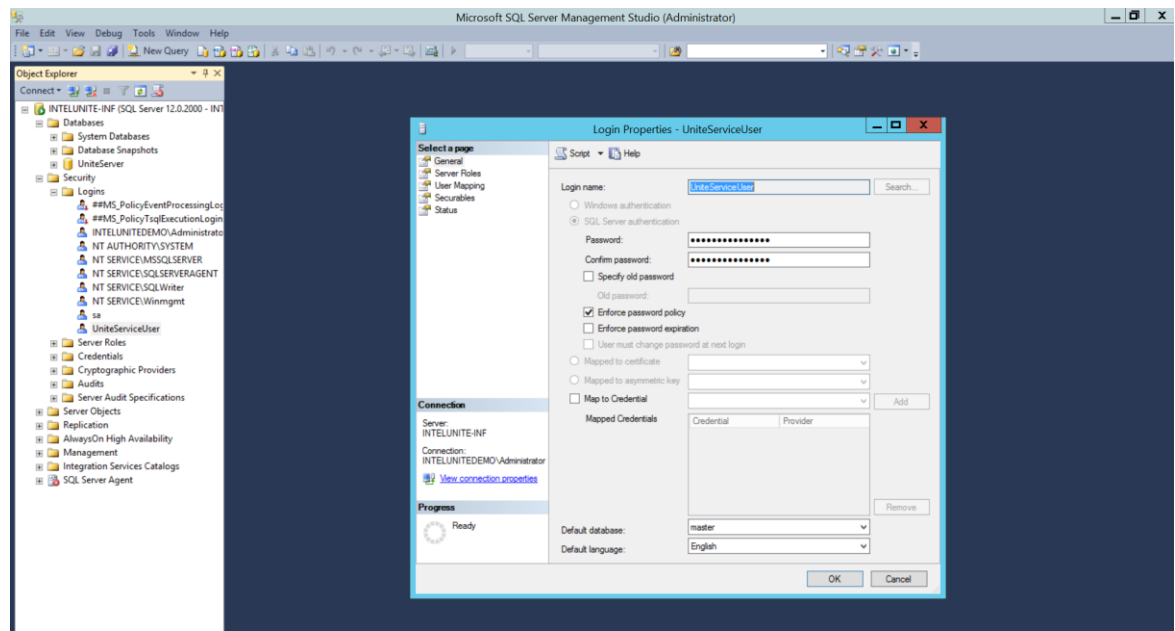
SQL 로그인 불일치가 발생했거나 사용자가 엔터프라이즈 서버를 여러 번 설치하려고 했기 때문에 데이터베이스 비밀번호가 손상된 경우 이러한 문제가 발생할 수 있습니다.

해결 방법/솔루션:

MS SQL 설치 시 사용된 인증 모드를 확인하십시오. 로그인/인증 유형을 변경하려면 Microsoft SQL Management Studio 로 이동하여 SQL Server 에 연결한 뒤 SQL Server 를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다. Intel Unite 응용 프로그램을 서버에 설치할 때 SQL 인증을 선택한 경우 보안 페이지를 선택하고 **SQL Server 및 Windows 인증** 모드가 선택되었는지 확인합니다.



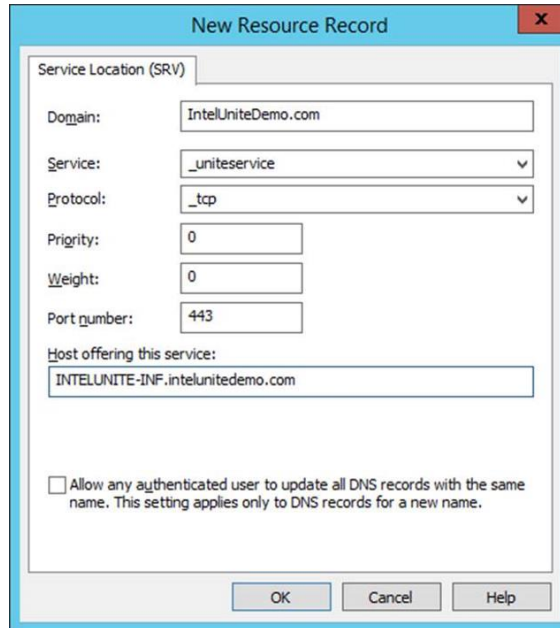
오류가 계속 표시되면 **UniteServiceUser** 비밀번호를 재설정하십시오. Microsoft SQL Management Studio 를 사용하여 SQL Server 에 연결한 후 **보안 > 로그인**으로 이동하여 **UniteServiceUser** 를 마우스 오른쪽 버튼으로 클릭하고 **로그인 속성 창** 을 엽니다. 새 비밀번호를 입력하고 **확인** 을 클릭하여 변경 사항을 저장합니다.



12.4.2 서버가 없습니다. DNS 서비스 레코드: _uniteservice._tcp 다시 시도

해결 방법/솔루션:

허브에서 DNS 레코드를 찾을 수 없을 경우 이러한 문제가 발생할 수 있습니다. 디버그 설정으로서, 명령줄 창을 열고 nslookup 명령을 실행합니다. 허브에서 DNS 서비스를 실행 중인 서버를 ping할 수 있으며 DNS 서비스 레코드를 Intel Unite 솔루션에 대해 생성해야 합니다. 서비스 레코드는 엔터프라이즈 서버에 대해 다음 값을 가져야 합니다: **서비스: _uniteservice,프로토콜: _tcp,포트 번호: 443 및 이 서비스를 제공하는 호스트: FQDN**



12.4.3 'uniteserverfqdn' 권한으로 SSL/TLS 보안 채널에 신뢰 관계를 형성할 수 없음

최신 버전의 Intel Unite 솔루션에는 SHA-2 인증서 이상만 허용됩니다. IT 부서와 논의하여 발행된 신뢰할 수 있는 웹 서버 인증서가 SHA-2 인증서이고 인증서 경로가 유효한지 확인해야 합니다.

테스트 환경에서 SHA-2 인증서를 확보하거나 사용자 환경에서 암호화를 비활성화하십시오.

- 암호화 없이 Unite 를 사용하려면 보안 포트 443 용 사이트 바인딩에 대한 세부 정보를 제공하는 다음 단계를 건너 뛰어서 MS SQL 서버를 설치와 DNS 서비스 레코드를 준비로 이동하십시오. 또한 DNS 서비스 레코드가 생성되면 서비스를 포트 80 에서 찾을 수 있는지 확인해야 합니다.
- 인증서 확인을 건너뛸 수 있는 다른 방법은 허브 및 클라이언트의 기기 계정에 레지스트리를 추가하는 것입니다. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)
 [인증서 알고리즘 확인을 건너 뛰어야 하는 경우 1, 그 외의 경우 0. (값이 0 인 경우 엔터프라이즈 인증서가 SHA2 인증서를 사용하도록 함)]

12.5 실행/연결 시 클라이언트 응용 프로그램 충돌

디버그 스위치로 응용 프로그램을 실행하고 정보를 로그 파일에 저장합니다.

(Intel Unite.exe /debug >logfile.txt 실행)

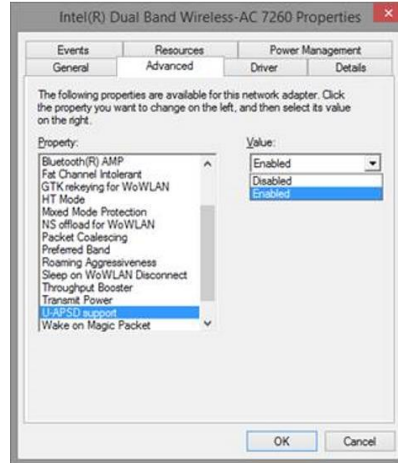
로그 파일에 “예외: - 키를 지정된 상태에서 사용하기에 부적합합니다.” 메시지가 표시되면 응용 프로그램을 닫고 C:\Users\%aviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df 파일을 삭제합니다.

12.6 주의 분야: 사용자는 평상시보다 긴 연결 시간이나 정기적으로 화면 업데이트가 느려지는 현상을 경험할 수 있습니다.

근본 원인:

이것은 U-APSD (Unscheduled Automatic Power Save Delivery)가 활성화되어 있을 때 일부 무선 액세스 지점에서 발생하는 버그입니다. <http://www.intel.com/support/wireless/wlan/sb/CS-034875.htm> 을 참조하십시오.

해결 방법: 무선 액세스 지점의 펌웨어 업데이트로 문제를 해결할 수 있습니다. 이는 대부분 기업에 쉽지 않은 일입니다. 마지막 방법으로 무선 드라이버의 고급 속성에서 클라이언트의 U-APSD 를 비활성화할 수 있습니다.



12.7 주의 분야: PIN 서버 속도 저하

해결 방법/솔루션: 엔터프라이즈 서버는 PIN 할당을 관리하고 PIN 을 찾아 회의실에 연결할 수 있습니다. 보안을 위해 사용자가 PIN 을 요청하고 데이터베이스에서 쿼리할 수 있는 속도는 지수 백오프 알고리즘으로 제한됩니다. 이 백오프 메커니즘은 사용자의 IP 주소와 시도 횟수를 기반으로 시도를 추적합니다.

생산 서버는 부하 분산기를 활용하여 환경에서 로드와 중복을 관리합니다. 부하 분산기는 트래픽을 적절한 웹 서버로 리디렉션합니다. 따라서 웹 서버에서 동일한 IP 주소의 모든 요청을 수신하여 백오프 알고리즘을 트리거하는 것처럼 보일 수 있습니다.

데이터베이스에는 계산된 지연을 몇 초 내에 웹 서버로 다시 반환하는 저장 프로시저(*spGetPinBackoffTime*)가 포함되어 있습니다. 이 기능은 비활성화할 수 있으므로 저장 프로시저에서는 항상 0 을 반환합니다. 이렇게 하면 보안 백오프 알고리즘이 비활성화됩니다.

12.8 Mac 클라이언트 문제 해결

터미널에서 Intel Unite 응용 프로그램(/Applications/Utilities)을 실행하여 디버그 메시지를 볼 수 있습니다.
`/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite`
 응용 프로그램이 시작되고 터미널에 모든 디버그 정보가 표시됩니다.



12.8.1 엔터프라이즈 서버 연결 오류 -1003: 지정된 호스트 이름의 서버를 찾을 수 없습니다.

해결 방법/솔루션: DNS 검색 도메인을 제대로 정의해야 합니다.

사용자가 DNS 서버를 정의했지만 검색 도메인을 지정하지 않은 경우, MAC 에서 자동 검색을 수행하려고 할 때 검색할 DNS 도메인 접미어가 없습니다. 정의된 DNS 검색 도메인이 없는 경우 Intel Unite 응용 프로그램에서 자동 검색 또는 *uniteservice* 의 "정적" 항목에 추가할 수 없습니다. 자동 검색이 *_uniteservice._tcp* 에서 작동하지 않으면 클라이언트에서 엔터프라이즈 서버를 찾을 수 없습니다.

가장 쉬운 해결책은 DNS 검색 도메인(DNS SRV 레코드와 일치해야 함)을 추가하는 것이지만 *plist* 설정에서 엔터프라이즈 서버를 정의할 수도 있습니다.

다음 터미널 명령을 사용하십시오.

```
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD
```

12.8.2 Enterprise Server 연결 오류 -1001: 요청 시간 초과

해결 방법/솔루션: 다음과 같은 두 가지 이유 때문에 이 오류가 발생할 수 있습니다.

1. 엔터프라이즈 서버의 웹 서비스에 잠재적인 문제가 있습니다.
2. Mac 에 네트워크-서버 간 연결 문제가 있습니다.

이 문제를 해결하는 첫 번째 단계는 디버그 로그에서 웹 서비스를 찾는 것입니다.

<https://yourserver/Unite/CCService.asmx> 를 살펴보십시오.

이 URL 을 복사하여 Safari 에 붙여넣고 Mac 에서 웹 서비스에 연결할 수 있는지 확인합니다. 이렇게 하면 네트워크와 서버 간 연결 문제가 있는지, 엔터프라이즈 서버의 웹 서비스가 실행 중인지 확인할 수 있습니다.

12.8.3 Enterprise Server 연결 오류 -1200: SSL 오류가 발생하여 서버에 대한 보안 연결을 구성할 수 없습니다.

IT 부서와 논의하여 Intel Unite 솔루션에 필요한 유효 SHA-2 인증서를 확보해야 합니다.

12.9 Mac OS Intel Unite app 앱이 클라이언트 장치에서 제거되고 다른 버전이나 최신 버전의 Intel Unite 응용 프로그램이 설치되었으나 기존 설치 속성이 그대로 남아 있습니다.

Mac 클라이언트용 Intel Unite 응용 프로그램은 일반적인 OS X 규칙을 따르기 때문에 앱은 삭제되어도 사용자 설정은 제거되지 않습니다.

해결 방법/솔루션:

클라이언트 장치에서 Intel Unite 응용 프로그램을 제거합니다. 설정을 제거하고 클린 상태로 돌아가는 방법에는 두 가지 있습니다.

1. 터미널(/응용 프로그램/유틸리티)에 다음 명령을 입력합니다.

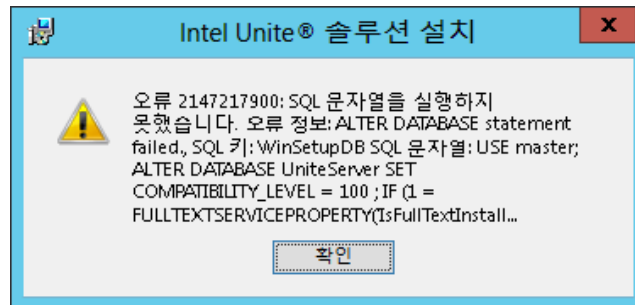
```
defaults delete com.intel.Intel-Unite
```

2. Finder 에서 ~/Library/Preferences/com.intel.Intel-Unite.plist 파일을 삭제한 다음...

시스템을 재부팅합니다. plist 파일은 Mac OS 에 의해 과도하게 캐시되기 때문에 일반적으로 plist 파일을 삭제하고 OS 에서 변경 내용을 따라가도록 할 수 없습니다.

12.10 오류 2147217900: SQL 문자열을 실행하지 못했습니다.

이 오류는 Intel Unite 서버 설치 프로그램이 실행되고 Unite 데이터베이스가 이미 있지만 서버 이름이 비어 있는 경우에 발생합니다.



해결 방법/솔루션:

데이터베이스가 이미 클러스터에 있는 경우 설치 프로그램에서 오류가 발생합니다. 이 오류를 해결하려면 데이터베이스를 삭제하고 DBAdmin 권한이 있는지 확인한 후 설치 프로그램을 다시 실행합니다.

12.11 오류 메시지: “데이터베이스 오류”

IT 관리자가 관리 콘솔에서 “토큰 전송” 옵션을 선택하고 “데이터베이스 오류” 오류 메시지가 표시되면 SMTP 서버 설정이 잘못되었을 가능성이 높습니다. SMTP 이메일 서버 설정을 확인해야 합니다.

12.12 관리자 웹 포털이 제대로 표시되지 않음(구성 요소가 누락됨)

Intel Unite 소프트웨어를 업그레이드한 뒤 관리자 웹 포털의 텍스트 상자, 옵션 또는 아이콘과 같은 구성 요소가 누락되어 제대로 표시되지 않습니다. 이 문제는 IIS 의 요청 필터링 옵션에 의해 MIME 형식이 차단되어 발생합니다.

해결 방법/솔루션:

1. IIS 관리자를 엽니다.
2. IIS 서버의 속성을 표시합니다.
3. **MIME 형식**을 클릭하고 다음과 같은 JSON 확장자를 추가합니다.
 - 파일 이름 확장자: .json
 - MIME 형식: application/json
4. IIS 서버 속성으로 돌아갑니다.
5. **핸들러 매핑**을 클릭합니다.
 - 스크립트 맵 추가
 - 요청 경로: *.json



- 실행 파일: C:\WINDOWS\system32\inetrv\asp.dll
 - 이름: JSON
6. **연결** 창에서 요청 필터링 설정을 수정하려는 연결, 사이트, 응용 프로그램 또는 디렉토리로 이동합니다.
 7. **홈** 창에서 **요청 필터링**을 두 번 클릭합니다.
 8. 파일 이름 확장자 허용을 찾습니다.
 9. 다음과 같은 4 개의 확장자를 추가합니다.
 - .json
 - .less
 - .woff
 - .woff2

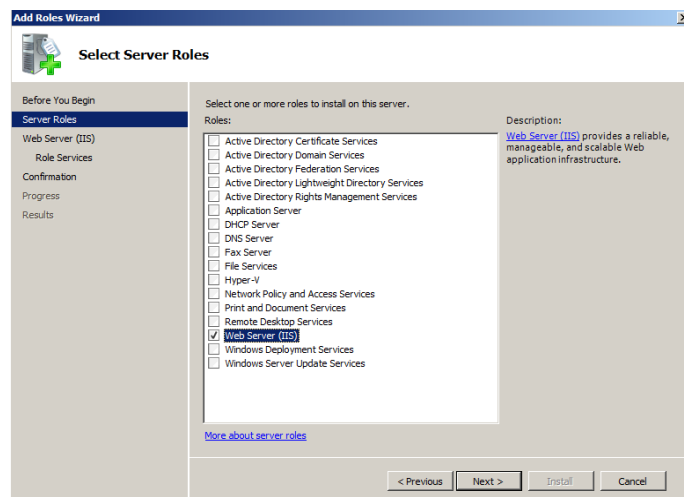
부록 A. 엔터프라이즈 서버 준비

IIS 활성화

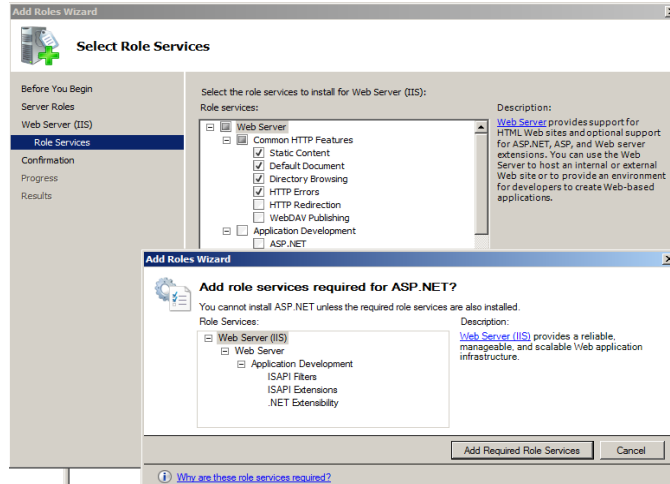
Windows 2008 의 경우:

Windows Server 2008 의 경우 .NET Framework 4.5(<https://www.microsoft.com/en-us/download/details.aspx?id=40779>) 업데이트를 다운로드해야 합니다.

- 시작을 클릭한 뒤 **관리 도구**에서 **서버 관리자**를 클릭합니다.
- **역할 요약**에서 **역할 추가**를 클릭합니다.
- **역할 추가 마법사**를 사용하여 **웹 서버(IIS)** 역할(이 상자를 선택)을 추가합니다.



- **역할 서비스 선택** 창이 표시되면 다음을 클릭합니다.
- **응용 프로그램 개발** 섹션에서 ASP.NET 이 선택되었는지 확인합니다. 선택되지 않은 경우, 선택하십시오. ASP.NET 은 기본적으로 선택 해제되어 있습니다. ASP.NET 에 **필요한 역할 서비스**를 추가합니다. ASP.NET 4.5 도 필요합니다.



- 역할이 생성되면 **역할** 메뉴에서 패널 오른쪽에 있는 **웹 서버(IIS)**로 이동한 다음 **IIS(인터넷 정보 서비스) 관리자**의 왼쪽 **연결** 창에서 서버를 선택합니다.

참조: Windows Server 라이브러리 링크 [Windows Server 2008 에 IIS 설치](#)

다음 단계를 통해 자체 서명된 인증서를 설치하고 솔루션을 테스트할 수 있습니다. 이 방법은 권장되지 않습니다. 신뢰할 수 있는 웹 서버 인증서를 요청하려면 IT 부서에 문의하십시오.

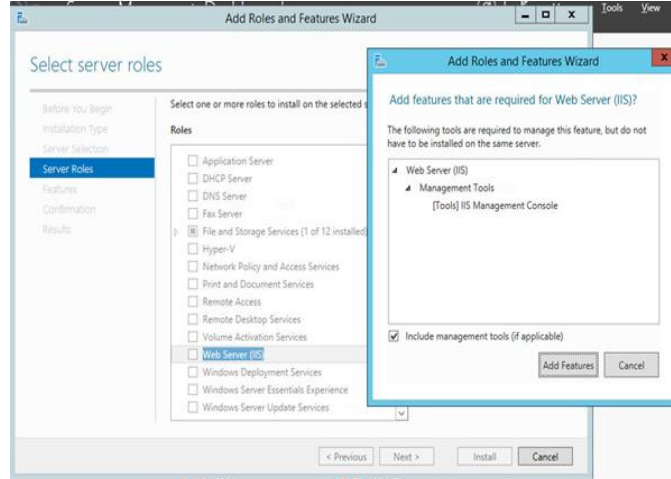
- 가운데 창에 있는 서버에서 **서버 인증서**를 클릭합니다.
- **작업**(오른쪽 창)에서 **자체 서명된 인증서 만들기를** 클릭합니다.
- 인증서에 원하는 이름을 지정한 다음 **확인**을 클릭합니다.
- 왼쪽 **연결** 창에서 사이트를 확장하고 **기본 웹 사이트**를 클릭합니다.
- 오른쪽 **작업** 창에서 **바인딩**(사이트 편집에 있음)을 선택합니다.
- **사이트 바인딩** 창에서 **추가**를 클릭합니다.
- 다음 정보를 사용하십시오.
 - 유형: https (참고: http 아님)
 - IP 주소: 모두 할당되지 않음
 - 포트: 443
 - 호스트 이름: (비워 둠)
 - SSL 인증서: (위 단계에서 생성한 인증서 선택)

확인을 클릭합니다.

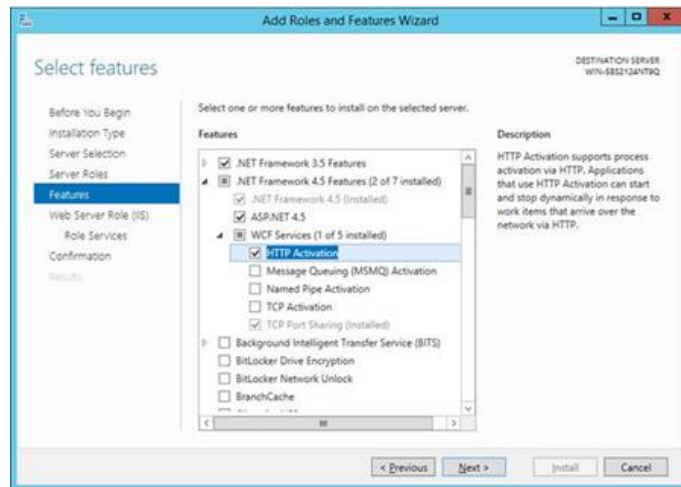
Windows 2012:

- **서버 관리자**를 엽니다.
- **관리** 메뉴에서 **역할 및 기능 추가**를 선택합니다.
- **역할 기반 또는 기능 기반 설치**를 선택합니다.
- 적절한 서버를 선택합니다(기본적으로 로컬이 선택되어 있음).
- **웹 서버(IIS)**와 웹 서버(IIS)에 필요한 **기능 추가**를 선택하고 **다음**을 클릭합니다.

참고: Unite 서버에서 인터넷 서버 인증서를 요청하기 위해 추가적인 세부 정보가 필요한 경우, Microsoft 웹 링크(<https://technet.microsoft.com/en-us/library/cc732906.aspx>)로 이동하여 SSL 인증서 공급업체 단계에 따라 서명된 인증서를 받습니다.



- 기능에서 IIS 에 다음 기능을 추가합니다(기본 옵션이 아님).
 - .NET Framework 3.5 기능
 - ASP.NET 4.5
 - WCF 서비스
 - HTTP 활성화(메시지가 표시되면 HTTP 활성화에 필요한 기능 추가), 그리고 다음을 를 클릭합니다.

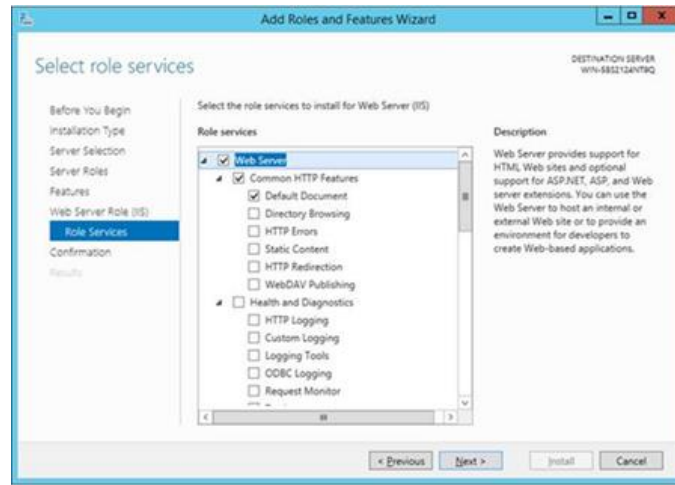


참고: 설치 중 .NET 3.5 에 오류가 발생할 수 있습니다. 대상 컴퓨터에 Windows Update 에 대한 액세스 권한이 없는 경우 대체 원본 경로를 제공합니다. **대체 원본 경로 지정** 링크를 클릭하여 설치 미디어에 있는 `\sources\sxs` 폴더에 대한 경로를 지정할 수 있습니다.

참조: <https://technet.microsoft.com/en-us/library/dn482071.aspx>

- 역할 서비스 페이지에서 **웹 서버 역할(IIS)**을 역할로 추가하거나 기본 값을 수락합니다.
- 다음 중 웹 서버에 설치할 역할 서비스를 선택합니다.

- 일반적인 HTTP 기능
- 기본 문서



- 다음을 클릭하여 계속하거나 다음 창에서 **설치**를 클릭하여 선택한 역할 및 기능을 설치할 수 있습니다.
- 역할이 생성되면 **역할** 메뉴에서 패널 오른쪽에 있는 **웹 서버 역할(IIS)**로 이동한 다음 **IIS(인터넷 정보 서비스) 관리자**의 왼쪽 **연결** 창에서 서버를 선택합니다.

참고: 최신 버전의 Intel Unite 솔루션에는 SHA-2 인증서 이상만 허용됩니다. IT 부서와 논의하여 발행된 신뢰할 수 있는 웹 서버 인증서가 SHA-2 인증서이고 인증서 경로가 유효한지 확인해야 합니다.

테스트 환경의 경우 암호화를 비활성화하거나 자체 서명된 SHA 2 인증서를 생성하십시오.

- 암호화 없이 Unite 를 사용하려면 보안 포트 443 용 사이트 바인딩에 대한 세부 정보를 제공하는 다음 단계를 건너 뛰어서 MS SQL 서버를 설치와 DNS 서비스 레코드를 준비로 이동하십시오. 또한 DNS 서비스 레코드가 생성되면 서비스를 포트 80 에서 찾을 수 있는지 확인해야 합니다.
- 관리자로서 다음과 같은 PowerShell 명령을 실행하십시오.
 - `New-SelfSignedCertificate -dnsname "yourservername" -CertStoreLocation cert:\LocalMachine\My ;` 여기서 "yourservername"은 엔터프라이즈 서버의 FQDN 입니다.
 - 허브 및 클라이언트의 기기 계정에 레지스트리를 추가하여 인증서 확인을 건너뛸 수도 있습니다. `HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)`
[인증서 알고리즘 확인을 건너 뛰어야 하는 경우 1, 그 외의 경우 0. (값이 0 인 경우 엔터프라이즈 인증서가 SHA2 인증서를 사용하도록 함)]
- 인증서를 할당하려면 왼쪽 **연결** 창에서 사이트를 확장하고 **기본 웹 사이트**를 클릭합니다.
- 오른쪽 **작업** 창에서 **바인딩**(사이트 편집에 있음)을 선택합니다.
- **사이트 바인딩** 창에서 **추가**를 클릭합니다.
- 다음 정보를 사용하십시오:
 - 유형: https (참고: http 아님)
 - IP 주소: 모두 할당되지 않음
 - 포트: 443
 - 호스트 이름: (비워 둠)



- SSL 인증서: (이전 단계에서 설치한 인증서 선택)
- **확인**을 클릭합니다.
- **닫기**를 선택합니다.

참조: Windows Server 라이브러리 링크 [Windows Server 2012 에 IIS 설치](#)

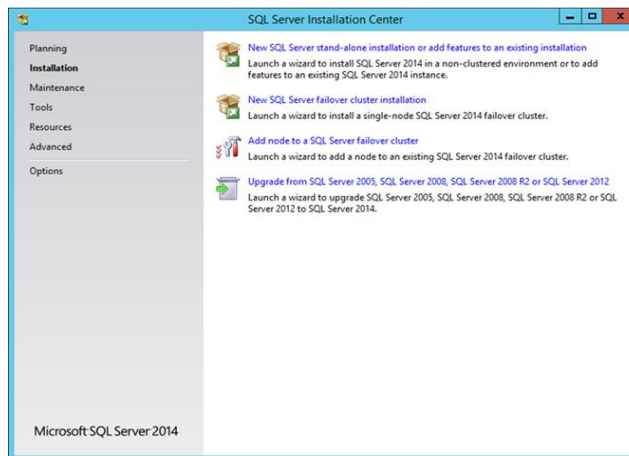
포트 443 에 대한 참고 사항: Intel Unite 응용 프로그램의 웹 서비스는 포트 443 을 사용하는 클라이언트 및 허브와 통신하므로 이 포트는 위에서 설명된 바와 같이 설정되어야 합니다.

Microsoft SQL Server 설치

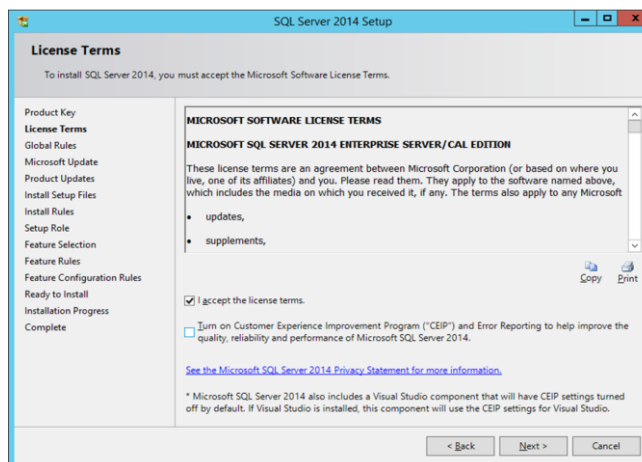
엔터프라이즈 서버는 MS SQL 을 실행해야 하며 최소 요구 사항은 버전 2008 R2 이상입니다. “테스트 환경”을 실행하여 응용 프로그램에 익숙해지려면 새로운 전용 SQL Server 를 설치할 수 있습니다(필수 사항 아님). Intel Unite 응용 프로그램은 다른 테이블이나 기존 데이터에 영향을 주지 않고 기존 데이터베이스에 자체 데이터베이스, 데이터 테이블 및 인덱스를 생성합니다.

MS SQL 2014 설치하는 다음을 참조하십시오.

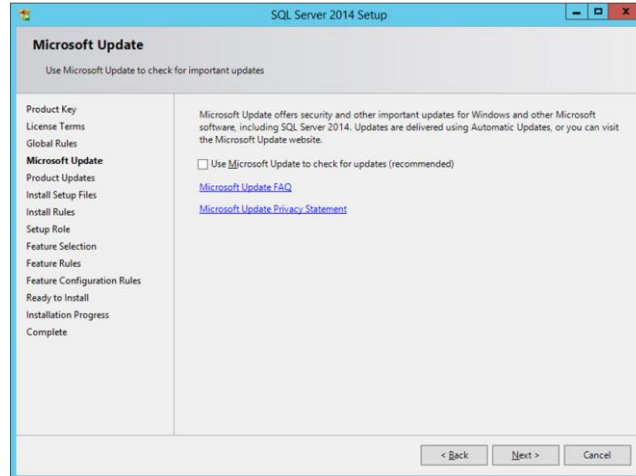
- SQL Server 설치를 실행하고 SQL Server 설치 센터를 엽니다. 왼쪽 창에서 **설치**를 클릭하고 **새 SQL Server 독립 실행형 설치 또는 기존 설치에 기능 추가**를 선택합니다.



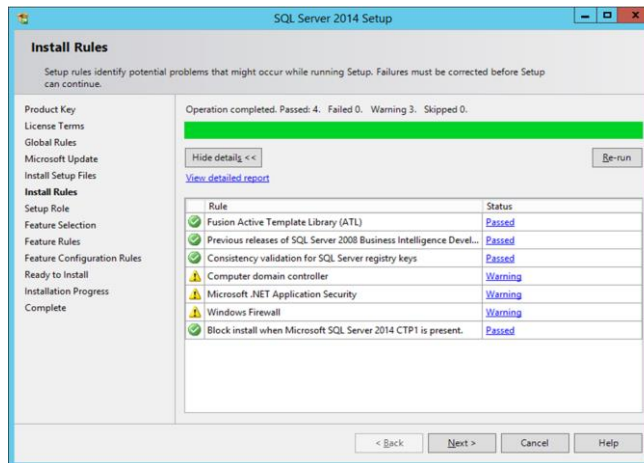
- 제품 키를 입력하고 라이선스 계약을 수락한 뒤 다음을 클릭합니다.



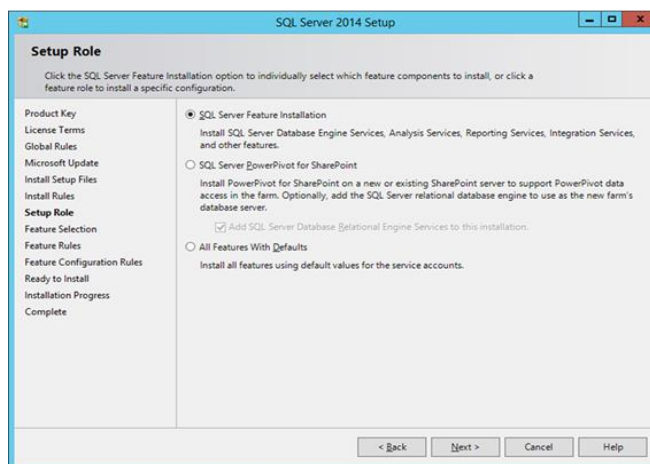
- **Microsoft Update** 를 통해 **업데이트 확인(권장)** 을 선택하여 업데이트를 선택하고 다음을 클릭합니다. 다음 창에서 제품 업데이트를 찾아 필요한 업데이트를 설치합니다. 계속하려면 다음을 클릭하십시오.



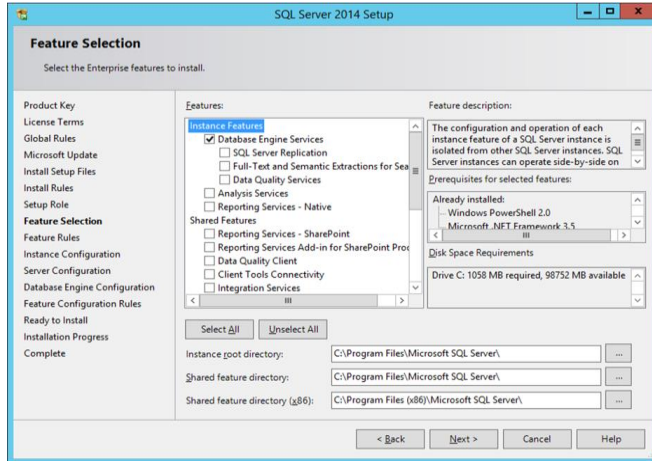
- SQL 설치 시, 설치 전에 잠재적인 오류 및 요구 사항 충족 여부를 확인합니다. 다음을 클릭하여 계속합니다.



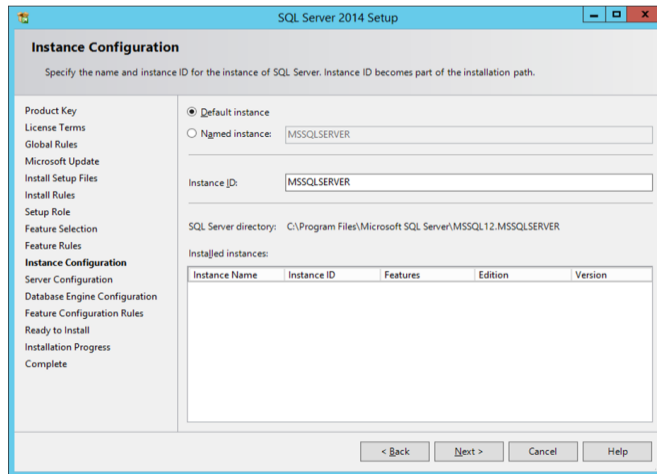
- SQL Server 기능 설치를 선택하고 다음을 클릭합니다.



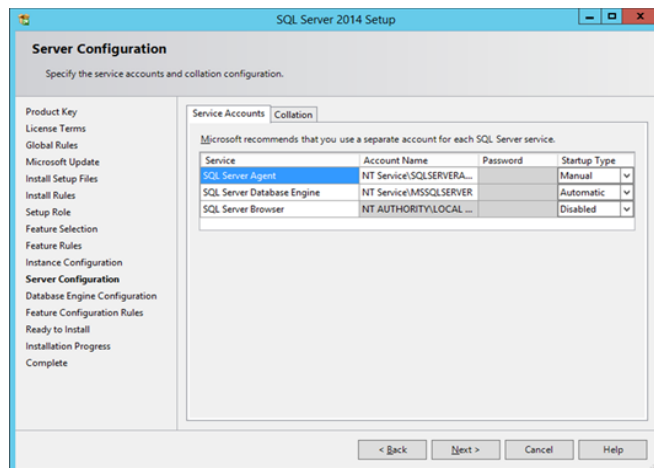
- 기능 선택에서 데이터베이스 엔진 서비스, 관리 도구- 완료를 선택하고 다음을 클릭합니다.



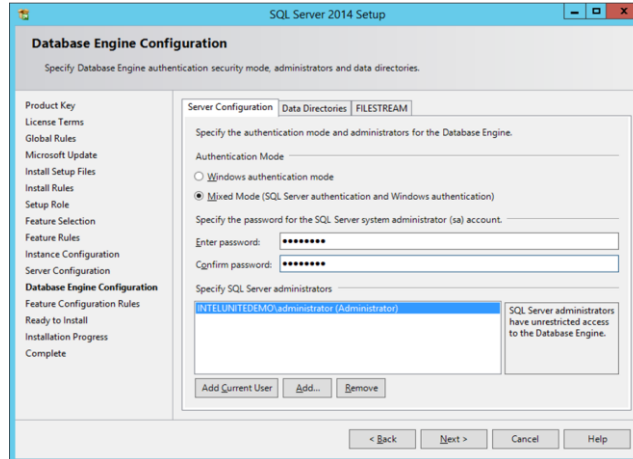
- SQL Server 이름과 인스턴스 ID 를 지정하고 다음을 클릭합니다.



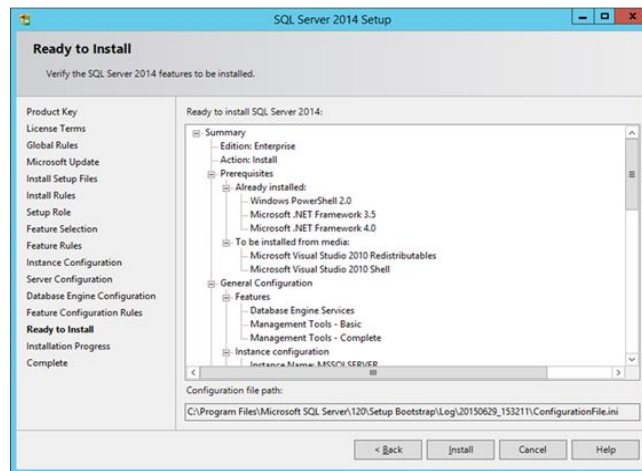
- 각 서비스에 서비스 계정을 지정하고 다음을 클릭하여 계속합니다.



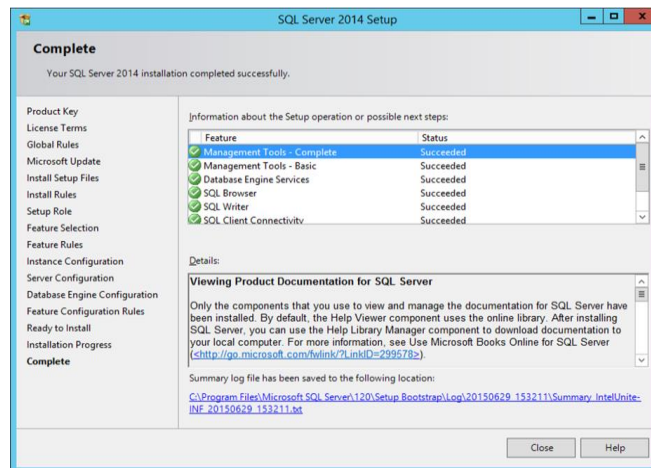
- 혼합 모드 인증(SQL Server 및 Windows 인증 포함)을 선택한 다음 SQL Server 관리자를 지정하고 다음을 클릭합니다.



- 기능이 설치되었는지 확인한 다음 **설치**를 클릭합니다.



- 설치가 완료되면 **닫기**를 클릭해서 대화 상자를 닫습니다.



DNS 서비스 레코드 생성

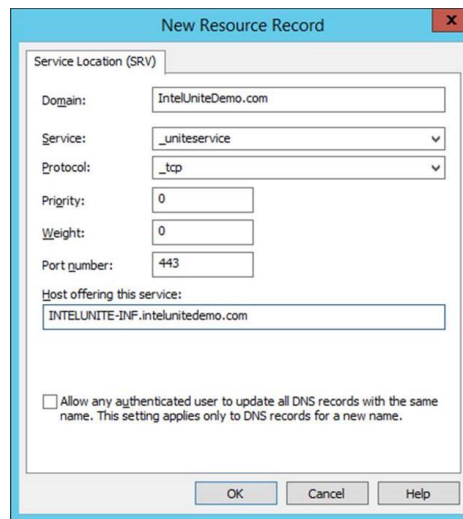
허브나 클라이언트에서는 엔터프라이즈 서버 자동 검색 중에 DNS 서비스를 사용하여 엔터프라이즈 서버를 찾습니다. 수동 조회를 사용할 수도 있지만 DNS 를 사용할 것을 권장합니다. 허브 및 클라이언트 설치 중에 엔터프라이즈 서버 호스트 이름을 수동으로 제공하고자 하는 경우 이 섹션을 건너뛸 수 있습니다.

DNS 서비스 레코드가 사용되는 경우, 허브 또는 클라이언트에서 DNS 서비스 레코드

_uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com 내에서 _uniteservice._tcp 라는 서비스를 찾습니다.

Microsoft Windows 에서 DNS 서비스 레코드를 추가하는 방법:

- DNS 서버에서 DNS 관리자를 엽니다.
- 왼쪽 창에서 정방향 조회 영역을 확장합니다.
- 영역을 마우스 오른쪽 버튼으로 클릭한 뒤 "다른 새 레코드..."를 선택합니다.
 - 리소스 레코드 종류 선택: 서비스 위치(SRV)를 선택한 다음 레코드 만들기를 선택합니다.
 - 서비스의 경우 _uniteservice 를 입력합니다.
 - 프로토콜의 경우 _tcp 를 입력합니다.
 - 포트 번호의 경우 443 을 입력합니다.
 - 이 서비스를 제공하는 호스트의 경우 엔터프라이즈 서버의 호스트 이름/IP를 입력합니다.



참고: 전달자를 사용하도록 DNS 서버를 구성하는 방법은 Microsoft

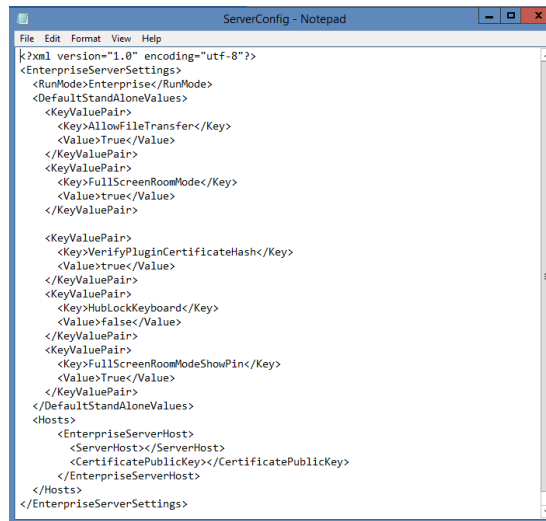
링크(<https://technet.microsoft.com/en-us/library/cc754941.aspx>)를 참조하십시오.

부록 B. ServerConfig.xml 예시

ServerConfig.xml 파일은 Intel Unite 소프트웨어의 허브 및 클라이언트 구성 요소 설치 중에 생성됩니다. xml 파일의 기본 위치는 허브와 클라이언트의 경우 각각 C:\Program Files (x86)\Intel\Intel Unite\Hub 와 C:\Program Files (x86)\Intel\Intel Unite\Client 입니다.

허브나 클라이언트에서 Intel Unite 소프트웨어를 설치하는 동안 **서버 지정**을 선택하고 서버 호스트 이름을 입력하거나 **공개 키**를 수동으로 입력하면 이 파일이 편집됩니다.

설치 후에 serverconfig.xml 파일을 편집하려면 파일이 존재하는 폴더로 이동하여 필요한 항목을 변경합니다.



```
<?xml version="1.0" encoding="utf-8"?>
<EnterpriseServerSettings>
  <RunMode>Enterprise</RunMode>
  <DefaultStandAloneValues>
    <KeyValuePair>
      <Key>AllowFileTransfer</Key>
      <Value>true</Value>
    </KeyValuePair>
    <KeyValuePair>
      <Key>FullScreenRoomMode</Key>
      <Value>true</Value>
    </KeyValuePair>
    <KeyValuePair>
      <Key>VerifyPluginCertificateHash</Key>
      <Value>true</Value>
    </KeyValuePair>
    <KeyValuePair>
      <Key>HubLockKeyboard</Key>
      <Value>false</Value>
    </KeyValuePair>
    <KeyValuePair>
      <Key>FullScreenRoomModeShowPin</Key>
      <Value>true</Value>
    </KeyValuePair>
  </DefaultStandAloneValues>
  <Hosts>
    <EnterpriseServerHost>
      <ServerHost></ServerHost>
      <CertificatePublicKey></CertificatePublicKey>
    </EnterpriseServerHost>
  </Hosts>
</EnterpriseServerSettings>
```

서버가 ServerConfig.xml 에서 정의된 경우 DNS 서비스 레코드보다 우선합니다.

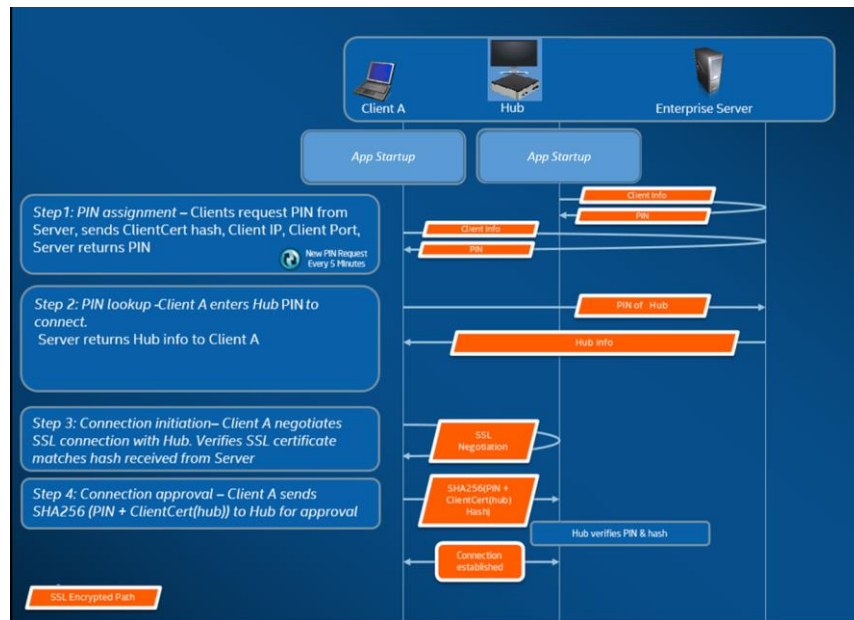
부록 C. Intel Unite 솔루션 - 보안 개요

Intel Unite 소프트웨어 - 보안 흐름

이 섹션에서는 Intel Unite 응용 프로그램의 보안 측면에 대해 간단하게 설명합니다. 연결 보안 측면은 다음 4 단계로 설명합니다.

1. PIN 할당
2. PIN 조회
3. 연결 초기화
4. 연결 승인

다음 이미지에는 클라이언트(인텔 v 프로 기술 제공)와 허브 응용 프로그램에서 엔터프라이즈 서버로부터 PIN 을 안전하게 수신하고 PIN 을 해결하며 연결을 설정하는 방법에 대한 개요가 포함되어 있습니다.



1 단계: PIN 할당

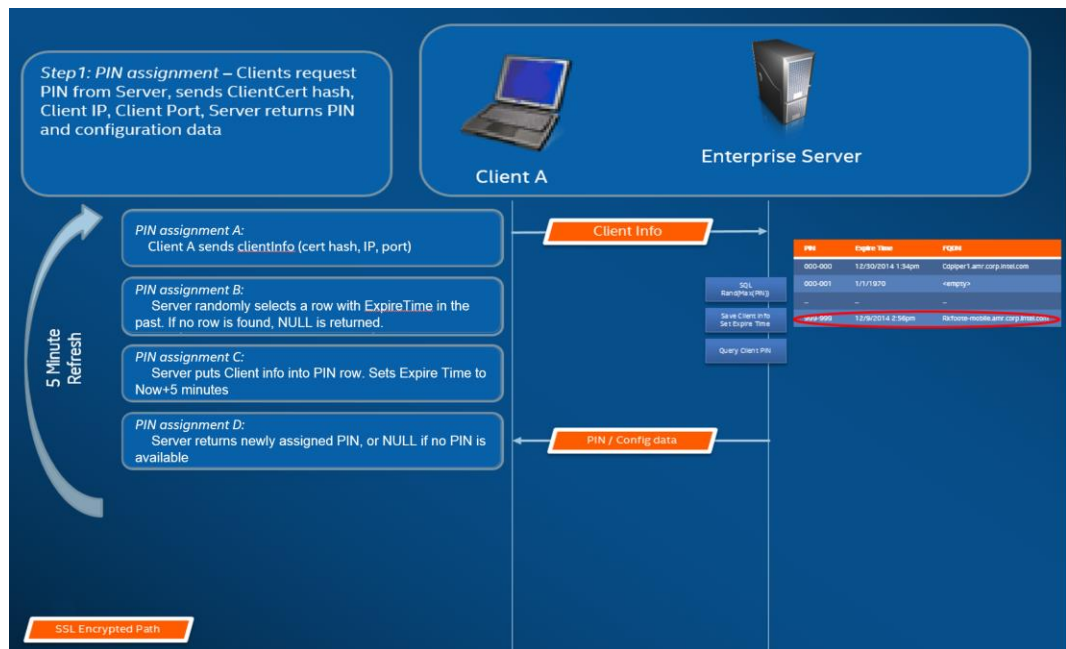
아래 이미지는 PIN 이 할당되는 방법을 보여 줍니다. 이 절차 중의 모든 네트워크 통신은 웹 서비스에서 SSL 암호화됩니다(TCP 443).

PIN 을 수신하는 것 외에도 허브와 클라이언트는 서버에 대한 연결 정보와 공개 키를 등록합니다. 연결 중에 사용되는 공개 키로 각 구성 요소가 원하는 대상과 통신 중인지 확인할 수 있습니다.

참고: 클라이언트(인텔 v 프로 기술 적용) 및 허브에 대한 PIN 할당은 동일한 흐름을 따릅니다.

또한 다음을 참고하십시오.

- PIN 새로 고침 간격은 구성 가능합니다.
- 허브나 클라이언트에서 연결 정보를 전송하면 로컬 호스트(127.0.0.0/8) 및 169.254.0.0/16 범위의 IP 주소가 무시됩니다.
- 클라이언트나 허브에 따라 TCP 포트를 구성하거나 관리 포털에서 프로필을 통해 푸시할 수 있습니다. 기본 동작은 운영 체제에서 포트를 할당하는 것입니다.
- 만료된 PIN 은 최대 15 초 동안 액세스가 허용됩니다.
- 만료된 PIN 은 사용자가 잘못된 디스플레이에 실수로 연결되지 않도록 만료 이후 최대 5 분 간 재할당되지 않습니다.



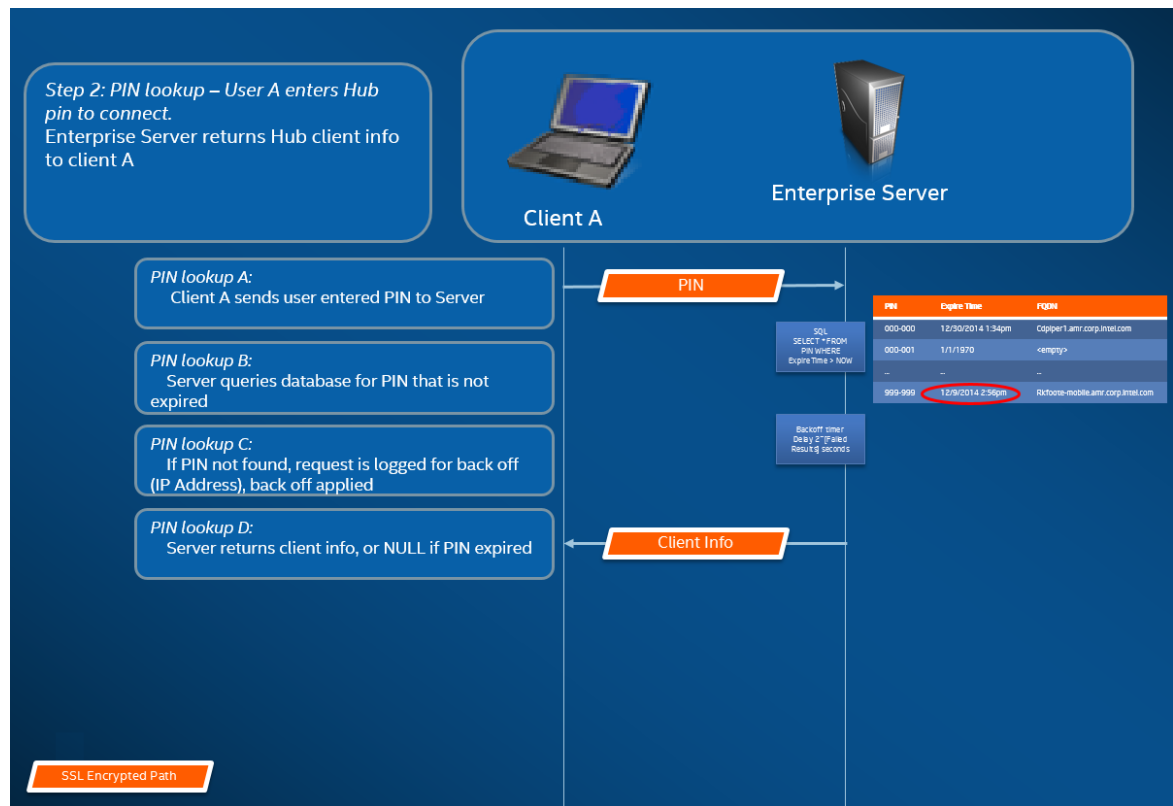
2 단계: PIN 조회

아래 이미지는 엔터프라이즈 서버에서 PIN 을 어떻게 해결하는지 보여 줍니다. PIN 조회 절차 중의 모든 네트워크 통신은 웹 서비스에서 SSL 암호화됩니다(TCP 443).

사용자가 클라이언트에 대상의 PIN 을 입력하면 클라이언트에서 엔터프라이즈 서버에 PIN 을 전송하여 연결 정보를 확보합니다. 조회에 성공하면 엔터프라이즈 서버에서 대상에 대한 유효한 연결 정보를 반환합니다. 대상은 Intel Unite 소프트웨어를 실행하는 허브 또는 클라이언트(인텔 v 프로 기술 적용)일 수 있습니다.

연결 정보 수신 외에도 대상의 공개 키가 제공되므로 클라이언트 응용 프로그램이 올바른 대상과 통신 중인지 확인할 수 있습니다.

참고: 허브 및 클라이언트의 PIN 조회는 동일한 흐름을 따릅니다.

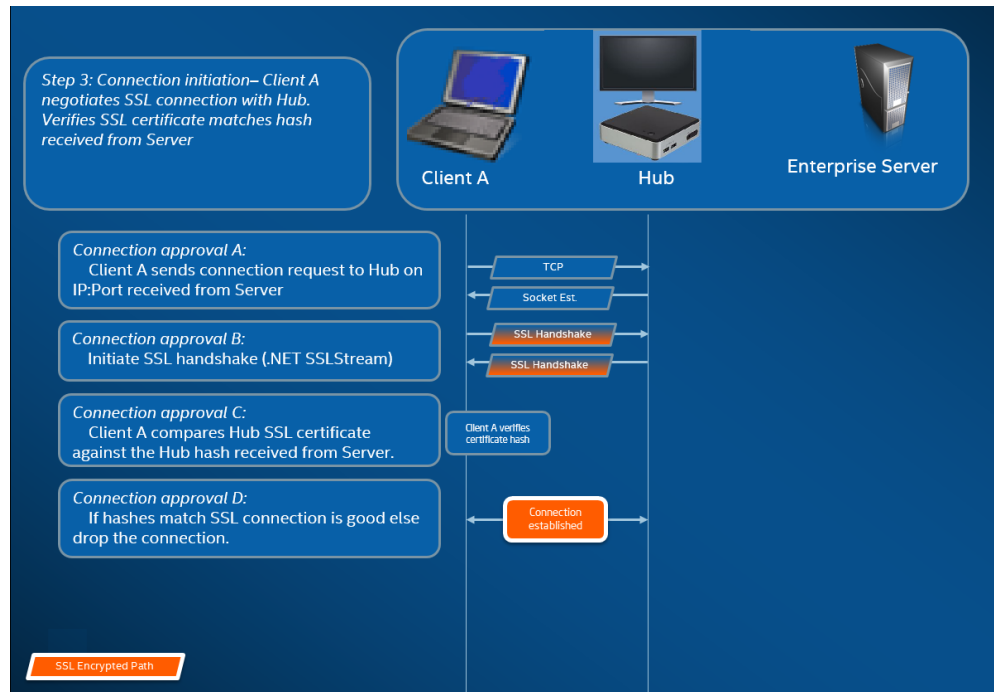


PIN 조회 백오프

침입자가 엔터프라이즈 서버의 PIN 을 수집하지 못하도록 하기 위해, 실패한 시도를 기록합니다. 사용자는 백오프 매커니즘으로 응답이 지연되기 전에 10 초 간격으로 최대 3 번까지 시도할 수 있습니다(2^x 초, x=5 분 동안 실패한 시도 횟수).

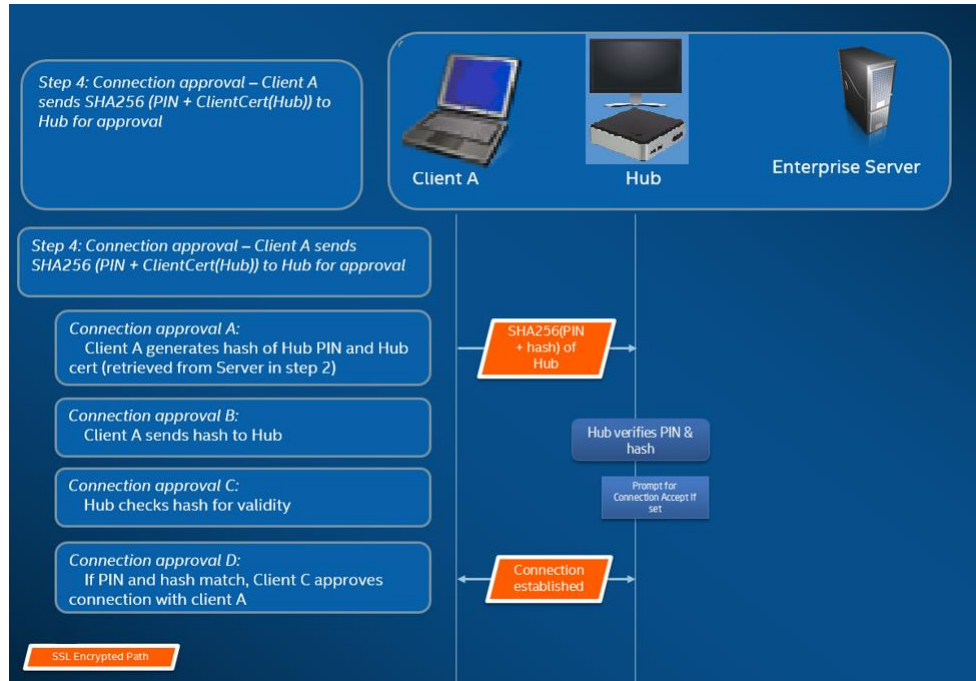
3 단계: 연결 초기화

아래 이미지에서는 연결이 초기화되는 방법을 보여 줍니다. 클라이언트는 대상(인텔 v 프로 기술이 적용된 허브나 클라이언트)에서 TCP P2P 연결을 초기화하고 SSL 핸드셰이크를 시작합니다. 대상에서 제공하는 인증서는 해시되고 클라이언트가 2 단계에서 수신한 해시와 비교됩니다. 이러한 유형의 확인은 공격을 예방하고 DHCP 클라이언트의 IP 주소가 변경되는 상황을 방지합니다.



4 단계: 연결 승인

아래 이미지에서는 클라이언트와 대상 간의 연결이 설정되는 방법을 보여 줍니다. 여기에서 대상은 Intel Unite 소프트웨어를 실행하는 허브 또는 클라이언트(인텔 v 프로 기술 적용)일 수 있습니다. 대상에서 PIN 과 클라이언트 인증서를 확인하면 연결을 허용되고 클라이언트와 대상 간의 연결이 설정됩니다.



부록 D. Intel Unite 솔루션 – 부하 분산기

이 섹션에서는 부하 분산기/프록시 뒤에서 PIN 백오프를 우회하는 방법에 대해 간략하게 설명합니다.

부하 분산기 뒤에 있는 경우 SQL 저장 프로시저 dbo.spGetPinBackoffTime 에서 **항상 0** 을 반환하도록 해야 합니다.

단계:

- 저장 프로시저 dbo.spGetPinBackoffTime 을 변경합니다. 모두 주석으로 처리하고 마지막에 있는 “Select 0”만 사용하면 됩니다.
- 스크립트를 실행합니다.

부하 분산기 뒤에 있지 않은 경우 저장 프로시저를 기본값으로 두어야 합니다.

```
USE [UniteServer]
GO
/***** Object: StoredProcedure [dbo].[spGetPinBackoffTime]    Script Date: 9/29/2016 3:27:54 PM *****/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
ALTER PROCEDURE [dbo].[spGetPinBackoffTime]
-- Add the parameters for the stored procedure here
@source nvarchar(255)
AS
BEGIN
---- SET NOCOUNT ON added to prevent extra result sets from
---- interfering with SELECT statements.
--SET NOCOUNT ON;
--declare @failCount int

---- Insert statements for procedure here
--SELECT @failCount = count(*) from tblPinRequestLog where SourceId = @source and [Timestamp] > DATEA
--SET @failCount = @failCount - 5 --Free failures allowed

--if (@failCount > 0)
-- begin
-- select POWER(2, @failCount)
-- end
--else
-- begin
-- select 0
-- end
select 0
END
```