

Dell Wyse Management Suite

버전 2.x 빠른 시작 가이드



참고, 주의 및 경고

 **노트:** 참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

 **주의:** 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

 **경고:** 경고는 재산 손실, 신체적 상해 또는 사망 위험이 있음을 알려줍니다.

© 2020 Dell Inc. 또는 자회사. 저작권 본사 소유. Dell, EMC 및 기타 상표는 Dell Inc. 또는 그 자회사의 상표입니다. 다른 상표는 해당 소유자의 상표일 수 있습니다.

1 소개	5
2 Wyse Management Suite 아키텍처	6
퍼블릭 클라우드의 Wyse Management Suite에 로그인	6
프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건	7
3 프라이빗 클라우드에 Wyse Management Suite 설치	8
Wyse Management Suite에 로그인	15
관리 콘솔의 기능 영역	15
신 클라이언트 구성 및 관리	15
정책 그룹 생성 및 구성 업데이트	16
새 신 클라이언트 등록	16
수동으로 ThinOS 장치 등록	17
DHCP 옵션 태그를 사용하여 디바이스 등록	18
DNS SRV 레코드를 사용하여 디바이스 등록	19
4 신 클라이언트에 애플리케이션 배포	21
ThinOS 펌웨어 이미지 인벤토리 업로드 및 배포	21
표준 애플리케이션 정책 생성 및 신 클라이언트에 배포	21
5 Wyse Management Suite 제거	23
6 Wyse Management Suite 문제 해결	24
7 Wyse Device Agent	26
8 추가 자료	27
부록 A: 원격 데이터베이스	28
Configure Mongo database	28
Configure Maria database	29
부록 B: 사용자 정의 설치	30
부록 C: Wyse Management Suite 아키텍처	35
부록 D: Wyse Management Suite 파일 리포지토리 액세스	37
부록 E: DHCP 옵션 태그 생성 및 구성	38
부록 F: DNS SRV 레코드 생성 및 구성	44
부록 G: 고급 애플리케이션 정책 생성 및 신 클라이언트에 배포	51

부록 H: 수동으로 Windows Embedded Standard 장치 등록.....	52
부록 I: 수동으로 ThinOS 8.x 디바이스 등록.....	53
부록 J: 수동으로 ThinOS 9.x 디바이스 등록.....	54
부록 K: 수동으로 Linux 장치 등록.....	55
부록 L: 용어 및 정의.....	56

소개

Wyse Management Suite는 Dell Wyse 씬 클라이언트를 중앙에서 구성하고 모니터링하며 관리하고 최적화할 수 있는 차세대 관리 솔루션입니다. 새로운 Suite에서는 우수한 기능, 성능, 사용 용이성으로 씬 클라이언트를 더 쉽게 배포하고 관리할 수 있습니다. 또한 클라우드 배포, 온-프레미스 배포, 모바일 애플리케이션을 사용하여 어디서든 관리, 고급 보안(예: BIOS 구성 및 포트 잠금) 등과 같은 고급 기능 옵션을 제공합니다. 그 밖의 기능에는 장치 검색 및 등록, 자산 및 인벤토리 관리, 구성 관리, 운영 체제 및 애플리케이션 배포, 실시간 명령, 모니터링, 경고 및 보고, 그리고 엔드포인트 문제 해결 등이 있습니다.

버전

Wyse Management Suite는 다음과 같은 버전으로 제공됩니다.

- **Standard (Free)** - Wyse Management Suite Standard Edition은 온-프레미스 배포에만 사용할 수 있습니다. Standard Edition을 사용하기 위해 라이선스 키가 필요하지 않습니다. Standard Edition은 중소기업에 적합합니다.
- **Pro (Paid)** - Wyse Management Suite Pro Edition은 프라이빗 및 퍼블릭 클라우드 배포에 모두 사용할 수 있습니다. Pro Edition은 구독 기반 라이선스를 사용하며 라이선스 키가 필요합니다. Pro 솔루션을 통해 조직은 하이브리드 모델을 채택하고 온-프레미스와 클라우드 간에 라이선스를 이동할 수 있습니다. Pro On-Premise Edition은 중소기업 및 대기업 환경에 적합합니다. 클라우드 배포의 경우 Pro Edition을 사용하여 기업 네트워크가 아닌 네트워크(홈 오피스, 타사, 파트너, 모바일 씬 클라이언트 등)에서 장치를 관리할 수 있습니다. 또한 Wyse Management Suite Pro Edition은 다음을 제공합니다.
 - 중요 경고 및 알림을 보고 명령을 실시간으로 전송할 수 있는 모바일 애플리케이션
 - 역할 기반 관리를 위한 2단계 인증 및 Active Directory 인증을 통해 보안 강화
 - 고급 앱 정책 및 보고

① 노트:

- 클라우드 서비스는 미국 및 독일에서 호스팅됩니다. 데이터 상주 제한이 있는 국가의 고객은 Wyse Management Suite Pro 클라우드 기반 서비스를 이용하지 못할 수도 있습니다.
- Wyse Management Pro Edition의 온-프레미스 버전은 데이터 상주 제한이 있는 고객에게 더 나은 솔루션입니다.

Standard 및 Pro Edition에서 지원되는 기능에 대한 자세한 내용은 [기능 매트릭스](#)를 참조하십시오.

Wyse Management Suite 아키텍처

이 섹션에서는 관리자로 시작하고 Wyse Management Suite 소프트웨어에서 싼 클라이언트를 관리하는 데 도움이 되는 일반 기능에 대한 정보를 제공합니다.

주제:

- 퍼블릭 클라우드의 Wyse Management Suite에 로그인
- 프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건

퍼블릭 클라우드의 Wyse Management Suite에 로그인

Wyse Management Suite 콘솔에 로그인하려면 지원되는 웹 브라우저를 시스템에 설치해야 합니다. Wyse Management Suite 콘솔에 로그인하려면 다음을 수행합니다.

1. 다음 링크 중 하나를 사용하여 Wyse Management Suite의 퍼블릭 클라우드(SaaS) 버전에 액세스합니다.
 - 미국 데이터 센터 - us1.wysemanagementsuite.com/ccm-web
 - EU 데이터 센터 - eu1.wysemanagementsuite.com/ccm-web
2. 사용자 이름과 암호를 입력합니다.
3. 로그인을 클릭합니다.

- ① **노트:** Wyse Management Suite 콘솔에 처음으로 로그인하거나 새 사용자를 추가하거나, 사용자 라이선스를 갱신할 때 이용 약관 페이지가 표시됩니다. 이용 약관을 읽고 해당 확인란을 선택한 다음 동의를 클릭합니다.
- ① **노트:** www.wysemanagementsuite.com에서 Wyse Management Suite 평가판에 등록하거나 구독을 구매할 때 로그인 자격 증명을 받습니다. Wyse Management Suite 구독은 Dell 영업팀 또는 현지 Dell 파트너에게 구입할 수 있습니다. 자세한 내용은 www.wysemanagementsuite.com을 참조하십시오.
- ① **노트:** 외부에서 액세스할 수 있는 리포지토리는 DMZ가 있는 서버에 설치하고, Wyse Management Suite Pro Edition은 퍼블릭 클라우드에서 사용해야 합니다. 서버의 FQDN(Fully Qualified Domain Name)은 퍼블릭 DNS에 등록해야 합니다.

암호 변경

로그인 암호를 변경하려면 관리 콘솔 오른쪽 상단에 있는 계정 링크를 클릭한 다음 **암호 변경**을 클릭합니다.

- ① **노트:** 처음으로 로그인한 후 암호를 변경하는 것이 좋습니다. 추가 관리자의 기본 사용자 이름과 암호는 Wyse Management Suite 계정 소유자가 생성합니다.

Wyse Management Suite에서 로그아웃

관리 콘솔에서 로그아웃하려면 관리 콘솔 오른쪽 상단에 있는 계정 링크를 클릭한 다음 **로그아웃**을 클릭합니다.

프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건

표 1. 사전 요구 사항

설명	디바이스 10,000대 이하	디바이스 50,000대 이하	디바이스 120,000대 이하	Wyse Management Suite - 소프트웨어 리포지토리
운영 체제	Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019 지원되는 언어 팩 - 영어, 프랑스어, 이탈리아어, 독일어, 스페인어, 일본어, 중국어(미리보기 릴리스)			
최소 디스크 공간	40GB	120GB	200GB	120GB
최소 메모리(RAM)	8GB	16GB	32GB	16GB
최소 CPU 요구 사항	4	4	16	4
네트워크 통신 포트	Wyse Management Suite 설치 프로그램은 TCP(Transmission Control Protocol) 포트 443, 8080 및 1883을 방화벽 예외 목록에 추가합니다. Wyse Management Suite 콘솔에 액세스하고 씬 클라이언트에 푸시 알림을 보내기 위해 포트가 추가됩니다. • TCP 443 - HTTPS 통신 • TCP 1883 - MQTT 통신 • TCP 3306 - MariaDB(원격인 경우 선택 사항) • TCP 27017 - MongoDB(원격인 경우 선택 사항) • TCP 11211 - Memcached • TCP 5172, 49159 - EMSDK(End-User Management Software Development Kit) - 선택 사항이며 Teradici 디바이스 관리에만 필요 설치 프로그램에 사용되는 기본 포트가 설치 중에 대체 포트로 변경될 수 있습니다.			Wyse Management Suite 리포지토리 설치 프로그램은 TCP 포트 443 및 8080을 방화벽 예외 목록에 추가합니다. Wyse Management Suite에서 관리하는 운영 체제 이미지 및 애플리케이션 이미지에 액세스하기 위해 포트가 추가됩니다.
지원되는 브라우저	Internet Explorer 버전 11 Google Chrome 버전 58.0 이상 Mozilla Firefox 버전 52.0 이상 Windows의 Edge 브라우저 - 영어로만 제공			

- Overlay Optimizer 버전 1.0 및 설치 스크립트는 Wyse Management Suite 설치 프로그램과 함께 제공됩니다. 관리자는 Wyse Management Suite에서 Overlay Optimizer를 사용할 수 있도록 활성화하는 스크립트를 실행해야 합니다.
- Dell Secure Client 버전 1.0 설치 스크립트는 Wyse Management Suite 설치 프로그램과 함께 제공됩니다. 관리자는 Wyse Management Suite에서 Dell Secure Client를 사용할 수 있도록 활성화하는 스크립트를 실행해야 합니다.

이 노트: WMS.exe 및 WMS_Repo.exe를 서로 다른 두 서버에 설치해야 합니다. 퍼블릭 클라우드용 Wyse Management Suite 원격 리포지토리를 설치해야 합니다. 프라이빗 클라우드의 경우 Wyse Management Suite 원격 리포지토리와 로컬 리포지토리를 설치해야 합니다. 물리적 컴퓨터 또는 가상 컴퓨터에 소프트웨어를 설치할 수 있습니다. 또한 소프트웨어 리포지토리와 Wyse Management Suite 서버의 운영 체제가 같을 필요는 없습니다. 자세한 내용은 [파일 리포지토리 액세스](#)를 참조하십시오.

프라이빗 클라우드에 Wyse Management Suite 설치

프라이빗 클라우드에서 Wyse Management Suite를 설정하려면 다음 요구 사항을 충족해야 합니다.

- 필요한 모든 하드웨어 및 소프트웨어를 가져와서 구성합니다. downloads.dell.com/wyse/wms에서 Wyse Management Suite 소프트웨어를 다운로드할 수 있습니다.
- 하나 이상의 서버 컴퓨터에 지원되는 서버 운영 체제를 설치합니다.
- 시스템에 최신 Microsoft 서비스 팩, 패치 및 업데이트가 설치되어 있는지 확인합니다.
- 지원되는 최신 버전의 브라우저가 설치되어 있는지 확인합니다.
- 설치에 포함되는 모든 시스템에서 관리자 권한 및 자격 증명을 확보합니다.
- Pro 기능의 경우 유효한 Wyse Management Suite 라이선스를 확보합니다. Standard Edition에는 라이선스가 필요하지 않습니다.

Wyse Management Suite의 간단한 설치는 다음과 같이 구성됩니다.

- Wyse Management Suite 서버(애플리케이션 및 운영 체제 이미지용 리포지토리 포함)
- 선택 사항 - 추가 Wyse Management Suite 리포지토리 서버(추가 이미지, 애플리케이션 및 AD 인증을 위한 리포지토리)
- 선택 사항 - 인증 기관(예: www.geotrust.com/)의 HTTPS 인증서.

프라이빗 클라우드에 Wyse Management Suite를 설치하려면 다음을 수행합니다.

1. 설치 관리자 패키지를 두 번 클릭합니다.
2. 시작 화면에서 라이선스 계약을 읽고 다음을 클릭합니다.
3. 설치 유형 페이지에서 설치할 구성 요소를 선택하고 다음을 클릭합니다. 사용 가능한 옵션은 다음과 같습니다.
 - Wyse Management Suite - Wyse Management Suite 구성 요소에 사용할 수 있는 두 가지 설치 유형이 있습니다.
 - 일반 - 최소 사용자 상호 작용이 필요하며 임베디드 데이터베이스를 설치합니다.
 - 맞춤 구성 - 최대 사용자 상호 작용이 필요하며 고급 사용자에게 권장됩니다. 자세한 내용은 [사용자 정의 설치](#)를 참조하십시오.
 - Teradici EM SDK - Teradici EM SDK 구성 요소가 서비스로 설치됩니다.

이 노트: Internet Explorer 보안 강화 구성 기능이 활성화되면 알림 창이 표시됩니다. 이 기능을 비활성화하려면 설치 유형 페이지에서 IE 보안 강화 비활성화 확인란을 선택합니다.

EM SDK가 이전 설치에서 Wyse Management Suite와 함께 서버에 설치된 경우 Teradici EM SDK 구성 요소가 자동으로 업데이트됩니다.

4. 설치 유형으로 일반을 선택합니다. 임베디드 데이터베이스에 대한 새 데이터베이스 자격 증명을 입력합니다. 또한 새 관리자 자격 증명을 입력하고 다음을 클릭합니다.

이 노트: 설치 후 Wyse Management Suite 웹 콘솔에 로그인하려면 관리자 자격 증명이 필요합니다.

5. 구성 페이지에서 CIFS 사용자에게 대한 공유 폴더 및 액세스 권한을 구성합니다. 사용 가능한 옵션은 다음과 같습니다.

- 기존 사용자 사용 - 기존 사용자에게 대한 자격 증명을 확인하려면 이 옵션을 선택합니다.
- 새 사용자 생성 - 이 옵션을 선택하고 자격 증명을 입력하여 새 사용자를 생성합니다.

이 노트: 설치 유형 페이지에서 Teradici EM SDK 옵션을 활성화한 경우 구성 페이지에서 Teradici 서버에 대한 포트를 구성할 수 있습니다.

6. 소프트웨어를 설치할 경로와 로컬 테넌트 파일 리포지토리를 설치할 경로를 선택한 후 다음을 클릭합니다.

소프트웨어를 설치할 대상 폴더의 기본 경로는 C:\Program Files\Dell\WMS입니다.

7. 다음을 클릭합니다.
사전 설치 요약 페이지가 표시됩니다.

8. 다음을 클릭하여 소프트웨어를 설치합니다.

설치 프로그램이 설치를 완료하는 데 약 4~5분이 소요됩니다. VC-runtime과 같은 종속 구성 요소가 시스템에 설치되어 있지 않은 경우 더 오래 걸릴 수 있습니다.

9. 실행을 클릭하여 Wyse Management Suite 웹 콘솔을 엽니다.

10. 웹 콘솔에서 시작하기를 클릭합니다.

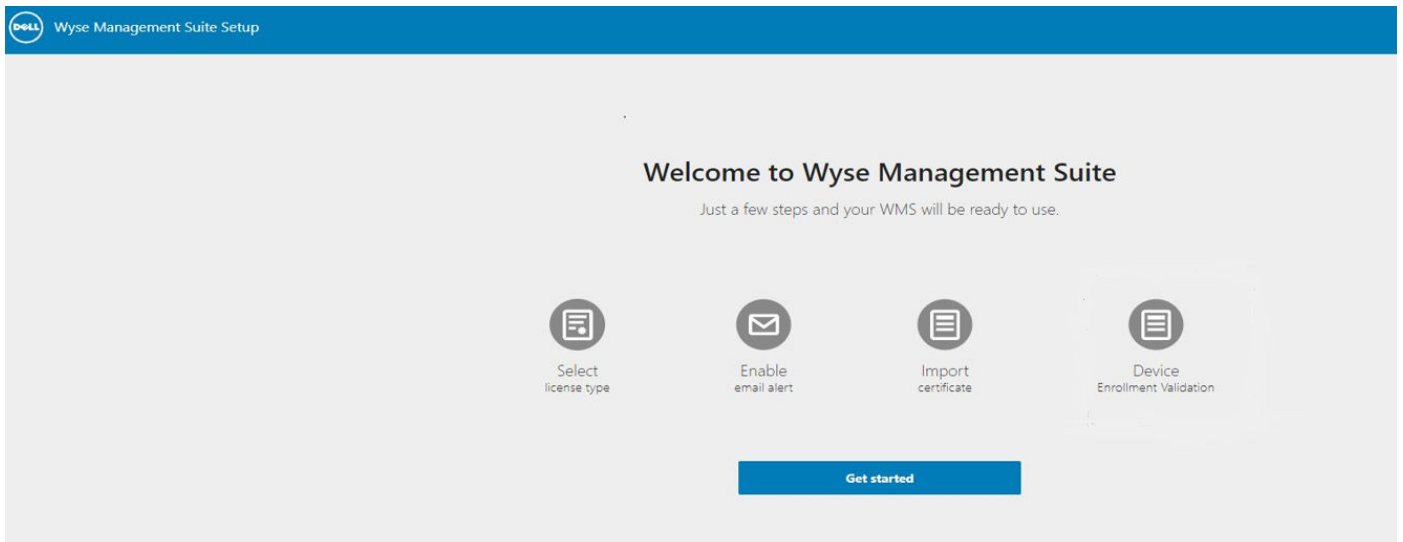


그림 1. 시작 페이지

11. 원하는 라이선스를 선택합니다.

- 라이선스 유형을 **Standard**로 선택한 경우 다음을 클릭하여 표준 Wyse Management Suite 설치를 계속합니다.
- 라이선스 유형을 **Pro**로 선택한 경우 유효한 Wyse Management Suite 라이선스를 가져와야 합니다. 서버가 인터넷에 연결되어 있는 경우 Wyse Management Suite 라이선스를 가져오려면 라이선스를 가져오기 위해 요청된 정보를 입력합니다. 또한 Wyse Management Suite 퍼블릭 클라우드 포털에 로그인하여 라이선스 키 필드에 키를 입력하여 라이선스 키를 생성할 수 있습니다.

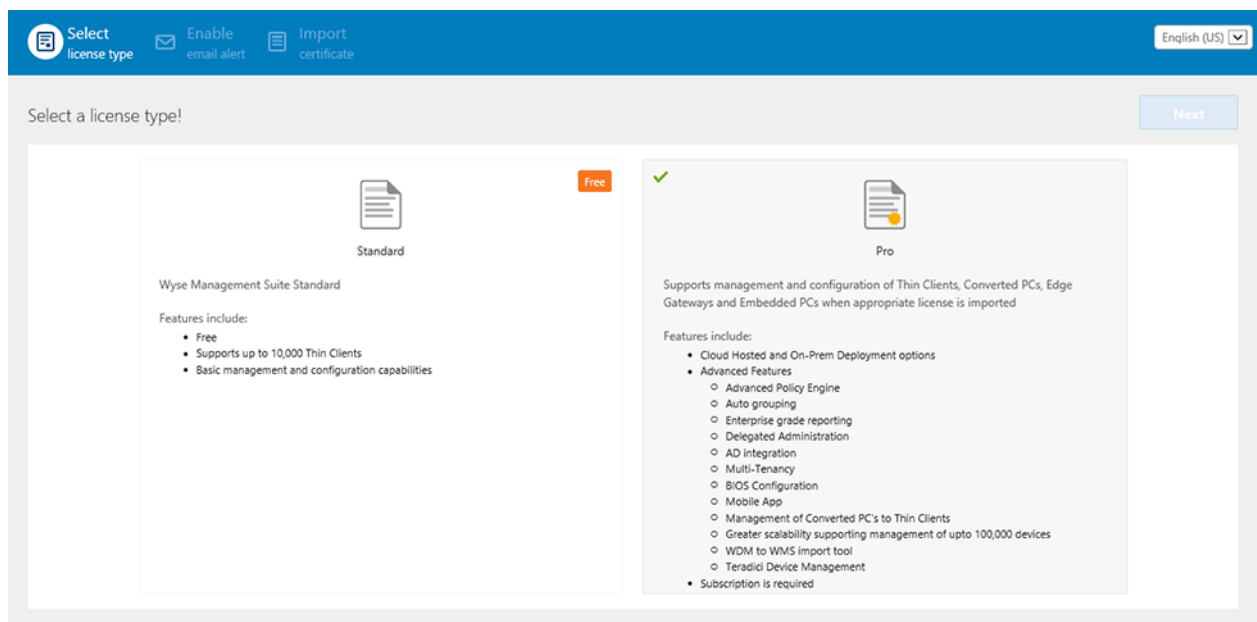


그림 2. 라이선스 유형

Enter license information ?

Enter your credentials to import licensing information ?

Username

Password

Data center

Number of TC seats ?

Number of Edge Gateway & Embedded PC seats ?

Number of Wyse Software Thin Client seats ?

Import

OR

Input your WMS Pro license key

License Key ?

Import

그림 3. 라이선스 정보

Wyse Management Suite 클라우드 포털에서 라이선스 키를 내보내려면 다음을 수행합니다.

- a. 다음 링크 중 하나를 사용하여 Wyse Management Suite 클라우드 포털에 로그인합니다.
 - 미국 데이터 센터 - us1.wysemanagementsuite.com/ccm-web
 - EU 데이터 센터 - eu1.wysemanagementsuite.com/ccm-web
- b. **포털 관리 > 구독**으로 이동합니다.

Console Settings

- Active Directory (AD)
- Alert Classification
- Edge Gateway & Embedded PC Registration
- External App Services
- File Repository
- Other Settings
- Thin Clients
- Two-Factor Authentication
- Reports

Account

- Custom Branding
- Subscription

License Subscription

License Type: Production
 Thin Client (Type/Exp): Production / Jun 1, 2019
 Wyse Software Thin Client (Type/Exp): Production / Jan 1, 2020
 Edge Gateway & Embedded PC (Type/Exp): Production / Dec 1, 2019

License Usage

Registered Thin Client devices

50 Manageable	24 In-Use	45 Used in Public Cloud WMS	5 Used in Private Cloud WMS
---------------	-----------	-----------------------------	-----------------------------

Registered Edge Gateways & Embedded PC devices

50 Manageable	0 In-Use	50 Used in Public Cloud WMS	0 Used in Private Cloud WMS
---------------	----------	-----------------------------	-----------------------------

Registered Wyse Software Thin Client devices

50 Manageable	0 In-Use	50 Used in Public Cloud WMS	0 Used in Private Cloud WMS
---------------	----------	-----------------------------	-----------------------------

Server Information:

Version: WMS 1.3.0 40874

Export License For Private Cloud

	Private Cloud	Public Cloud	Manageable
Number of TC seats		45	50
Number of Edge Gateway & Embedded PC seats		50	50
Number of Wyse Software Thin Client seats		50	50

Export WMS 1.1+

그림 4. 포털 관리

- 씬 클라이언트 시트의 수를 입력합니다.
- 내보내기를 클릭합니다.

노트: 라이선스를 내보내려면 드롭다운 목록에서 **WMS 1.1** 또는 **WMS 1.0**을 선택합니다.

라이선스를 가져온 이후에 요약 페이지에 라이선스 세부 정보가 표시됩니다.

- SMTP 서버 정보를 입력하고 **저장**을 클릭합니다.

노트: 이 화면을 건너뛰고 나중에 콘솔에서 변경할 수 있습니다.

그림 5. 이메일 알림

노트: Wyse Management Suite에서 이메일 알림을 수신하려면 유효한 SMTP 서버 정보를 입력해야 합니다.

- SSL 인증서를 가져와서 Wyse Management Suite 서버와의 통신을 보호합니다. 퍼블릭, 프라이빗 및 Apache 인증서를 입력하고 가져오기 버튼을 클릭합니다. 인증서를 가져오기 위해 Tomcat 서비스를 구성하고 다시 시작하는 데 3분이 소요됩니다. 이 화면을 건너뛰고 나중에 Wyse Management Suite 프라이빗 클라우드에 로그인한 후 포털 관리 페이지에서 가져와서 콘솔에서 변경할 수 있습니다.

노트:

기본적으로 Wyse Management Suite는 설치 중에 생성되는 자체 서명된 SSL 인증서를 가져와서 클라이언트와 Wyse Management Suite 서버 간의 통신을 보호합니다. Wyse Management Suite 서버에 유효한 인증서를 가져오지 않은 경우 설치된 서버 이외의 시스템에서 Wyse Management Suite에 액세스하면 보안 경고 메시지가 표시됩니다. 설치 중에 생성되는 자체 서명된 인증서는 인증 기관([geotrust.com](https://www.geotrust.com))의 서명이 없으므로 경고 메시지가 표시됩니다. .pem 또는 .pfx 인증서를 가져올 수 있습니다.

그림 6. 키 또는 인증서 값 쌍

Import certificate ? You can complete this setup or make changes later in the console.

PKCS-12 (.pfx or .p12)
Use this option when you have a .pfx or .p12 file that has the domain certificate, private key, and complete certificate chain (root and potentially intermediate certificates). This is the option you would normally use when using IIS to request the domain certificate.

Key/Certificate Pair
Use this option when the domain certificate, private key, and certificate chain (root and potentially intermediate certificates) are separate files. This is the option you would normally use when using a Public CA to request the certificate. When using this method make sure to choose Apache as the certificate type when requesting the certificate. Also note that some Public CA's don't include the intermediate certificate in the chain so you have to download them from the Public CA's website separately.

PKCS-12 (.pfx or .p12) *

Password for PKCS *

Intermediate certificate ?

그림 7. PKCS-12

14. 디바이스 페이지에서 관리자가 그룹에 대한 씬 클라이언트의 수동 및 자동 등록을 제어할 수 있도록 **등록 유효성 검사**를 활성화할 수 있습니다.

Select device type | Enable email alert | Import certificate | **Device Enrollment Validation** | English (US)

Configure Device Enrollment Validation You can complete this setup or make changes later in the console.

Enrollment Validation(Unmanaged Group) ? ☒

그림 8. 등록 유효성 검사

15. **저장**을 클릭한 후 **다음**을 클릭합니다.
16. **WMS**에 로그인을 클릭합니다.
Dell Management Portal 로그인 페이지가 표시됩니다.

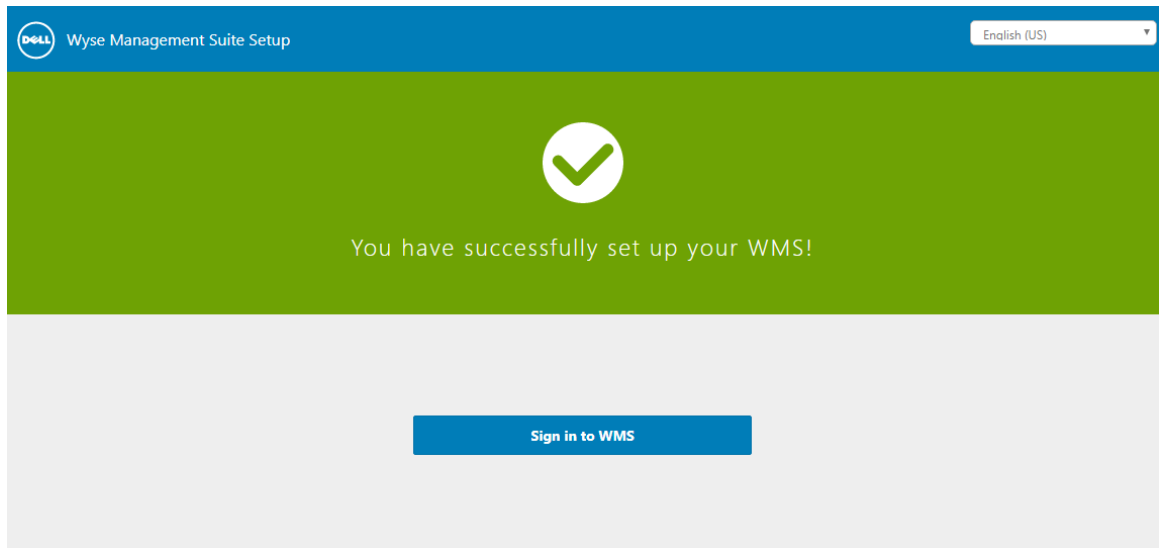


그림 9 . 로그인 페이지

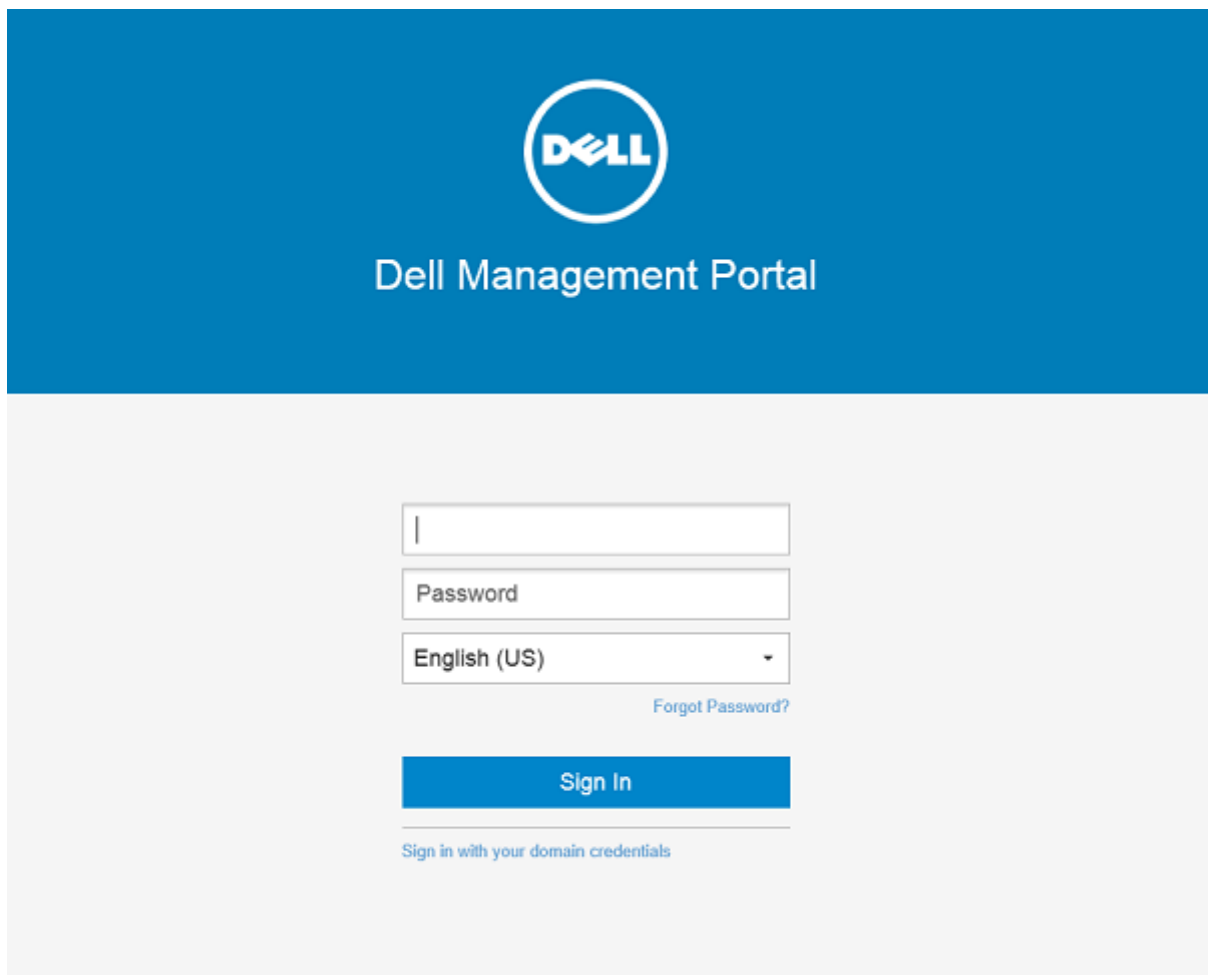


그림 10 . Dell Management Portal

① **노트:** 이후에 포털 관리 페이지에서 라이선스를 업그레이드하거나 확장할 수 있습니다.

주제:

- [Wyse Management Suite에 로그인](#)

- 관리 콘솔의 기능 영역
- 씬 클라이언트 구성 및 관리
- 정책 그룹 생성 및 구성 업데이트
- 새 씬 클라이언트 등록

Wyse Management Suite에 로그인

관리 콘솔에 로그인하려면 다음을 수행합니다.

1. Internet Explorer를 사용하는 경우 **Internet Explorer Enhanced Security** 및 **Compatibility View** 설정을 비활성화합니다.
2. 인터넷에 액세스할 수 있는 모든 시스템에서 지원되는 웹 브라우저를 사용하고 <https://<FQDN>/ccm-web>에서 Wyse Management Suite의 프라이빗 클라우드 버전에 액세스합니다. 예를 들어, <https://wmserver.domain.com/ccm-web>에서 wmserver.domain.com은 서버의 정규화된 도메인 이름입니다.
3. 사용자 이름과 암호를 입력합니다.
4. **Sign In**을 클릭합니다.

관리 콘솔의 기능 영역

Wyse Management Suite 콘솔은 다음과 같은 기능 영역으로 구성됩니다.

- **Dashboard** 페이지는 시스템의 각 기능 영역에 대한 정보를 제공합니다.
- **Groups & Configs** 페이지에서는 장치 구성에 대한 계층 구조의 그룹 정책 관리를 수행합니다. 선택적으로 기업 표준에 따라 전역 그룹 정책의 하위 그룹을 생성하여 장치를 분류할 수 있습니다. 예를 들어 장치를 작업 기능, 장치 유형, BYOD(Bring-Your-Own-Device) 등에 따라 그룹화할 수 있습니다.
- **Devices** 페이지에서는 장치, 장치 유형 및 장치별 구성을 보고 관리할 수 있습니다.
- **Apps & Data** 페이지에서는 장치 애플리케이션, 운영 체제 이미지, 정책, 인증서 파일, 로고 및 배경화면 이미지를 관리할 수 있습니다.
- **Rules** 페이지에서는 자동 그룹화, 경고 알림과 같은 규칙을 추가, 편집, 활성화 또는 비활성화할 수 있습니다.
- **Jobs** 페이지에서는 재부팅, WOL, 등록된 장치에 애플리케이션 또는 이미지 정책 배포와 같은 작업을 생성할 수 있습니다.
- **Events** 페이지에서는 시스템 이벤트 및 경고를 보고 감사할 수 있습니다.
- **Users** 페이지에서는 로컬 사용자와 Active Directory에서 가져온 사용자가 Wyse Management Suite에 로그인할 수 있도록 전역 관리자, 그룹 관리자 및 뷰어 역할을 할당할 수 있습니다. 할당된 역할에 따라 작업을 수행할 수 있는 권한이 사용자에게 부여됩니다.
- **Portal Administration** 페이지에서는 관리자가 로컬 리포지토리 구성, 라이선스 구독, Active Directory 구성 및 2단계 인증 등 다양한 시스템 설정을 구성할 수 있습니다. 자세한 내용은 support.dell.com의 *Dell Wyse Management Suite 관리자 안내서*를 참조하십시오.

씬 클라이언트 구성 및 관리

Configuration management - Wyse Management Suite는 그룹 및 하위 그룹의 계층 구조를 지원합니다. 그룹은 시스템 관리자가 정의한 규칙에 따라 수동 또는 자동으로 생성할 수 있습니다. 기능 그룹(예: 마케팅, 영업, 엔지니어링) 또는 위치 계층 구조(예: 국가, 시/도, 구/군/시)를 기준으로 구성할 수 있습니다.

이 노트:

Pro Edition에서 시스템 관리자는 규칙을 추가하여 그룹을 생성할 수 있습니다. 또한 서버넷, 시간대, 위치와 같은 장치 특성에 따라 장치를 기존 그룹에 할당할 수 있습니다.

다음도 구성할 수 있습니다.

- 기본 정책 그룹에 설정된 테넌트 계정의 모든 장치에 적용되는 설정 또는 정책. 이러한 설정 및 정책은 모든 그룹 및 하위 그룹이 상속하는 전역 매개변수 세트입니다.
- 하위 수준 그룹에 구성된 설정 또는 매개변수는 상위 또는 상위 수준 그룹에 구성된 설정보다 우선합니다.
- **Device Details** 페이지에서 구성할 수 있는 특정 장치에 고유한 매개변수. 하위 수준 그룹과 같은 이러한 매개변수는 상위 수준 그룹에 구성된 설정보다 우선합니다.

구성 매개변수는 관리자가 정책을 생성하고 게시할 때 해당 그룹 및 모든 하위 그룹의 모든 장치에 배포됩니다.

구성을 게시하고 장치로 전파한 후에는 관리자가 변경할 때까지 설정이 장치로 다시 전송되지 않습니다. 등록된 새 장치는 등록된 그룹에 유효한 구성 정책을 수신합니다. 여기에는 전역 그룹 및 중간 수준 그룹에서 상속된 매개변수가 포함됩니다.

구성 정책은 즉시 게시되며 나중에 예약할 수 없습니다. 일부 정책(예: 디스플레이 설정) 변경 시 재부팅이 실행될 수 있습니다.

Application and operating system image deployment - 애플리케이션 및 운영 체제 이미지 업데이트는 **Apps & Data** 탭에서 배포할 수 있습니다. 애플리케이션은 정책 그룹을 기준으로 배포됩니다.

이 노트: 고급 애플리케이션 정책을 사용하면 요구 사항에 따라 현재 및 모든 하위 그룹에 애플리케이션을 배포할 수 있습니다. 운영 체제 이미지는 현재 그룹에만 배포할 수 있습니다.

Wyse Management Suite는 표준 및 고급 애플리케이션 정책을 지원합니다. 표준 애플리케이션 정책을 사용하면 단일 애플리케이션 패키지를 설치할 수 있습니다. 각 애플리케이션 설치 전과 설치 후에 장치를 재부팅해야 합니다. 고급 애플리케이션 정책을 사용하면 두 번의 재부팅만으로 여러 애플리케이션 패키지를 설치할 수 있습니다. 이 기능은 Pro Edition에서만 사용할 수 있습니다. 고급 애플리케이션 정책은 특정 애플리케이션 설치에 필요할 수 있는 사전 설치 및 사후 설치 스크립트의 실행도 지원합니다.

장치를 Wyse Management Suite에 등록하거나 장치를 새 그룹으로 이동할 때 자동으로 적용되도록 표준 및 고급 애플리케이션 정책을 구성할 수 있습니다.

애플리케이션 정책 및 운영 체제 이미지를 씬 클라이언트에 배포하는 작업을 장치 시간대 또는 기타 지정된 시간대를 기준으로 즉시 또는 나중에 예약할 수 있습니다.

Inventory of devices - 이 옵션은 **Devices** 탭을 클릭하여 찾을 수 있습니다. 기본적으로 이 옵션은 시스템에 있는 모든 장치를 페이지가 매겨진 목록으로 표시합니다. 관리자는 그룹 또는 하위 그룹, 장치 유형, 운영 체제 유형, 상태, 서브넷, 플랫폼, 시간대 등 다양한 필터 기준을 사용하여 장치의 하위 집합을 표시하도록 선택할 수 있습니다.

해당 장치의 **Device Details** 페이지로 이동하려면 이 페이지에 나열된 장치 항목을 클릭합니다. 장치의 모든 세부 정보가 표시됩니다.

Device Details 페이지에는 해당 장치에 적용할 수 있는 모든 구성 매개변수와 각 매개변수가 적용되는 그룹 수준도 표시됩니다.

또한 이 페이지에서 관리자는 **Device Exceptions** 버튼을 활성화하여 해당 장치에 고유한 구성 매개변수를 설정할 수 있습니다. 이 섹션에서 구성된 매개변수는 그룹 및/또는 전역 수준에서 구성된 모든 매개변수를 재정의합니다.

Reports - 관리자가 형식이 지정된 보고서를 생성하고 사전 정의된 필터를 기준으로 보고서를 볼 수 있습니다. 형식이 지정된 보고서를 생성하려면 **Portal Administration** 페이지에서 **Reports** 탭을 클릭합니다.

Mobile application - 관리자가 Android 장치에서 사용할 수 있는 모바일 애플리케이션을 사용하여 경고 알림을 수신하고 장치를 관리할 수 있습니다. 모바일 애플리케이션 및 빠른 시작 설명서를 다운로드하려면 **Portal Administration** 페이지에서 **Alerts and Classification** 탭을 클릭합니다.

정책 그룹 생성 및 구성 업데이트

정책을 생성하고 구성을 업데이트하려면 다음을 수행합니다.

1. 관리자로 로그인합니다.
2. 정책 그룹을 생성하려면 다음을 수행합니다.
 - a. **Groups & Configs**를 선택하고 왼쪽 창에서 **+** 버튼을 클릭합니다.
 - b. 그룹 이름과 설명을 입력합니다.
 - c. **Enabled** 확인란을 선택합니다.
 - d. 그룹 토큰을 입력합니다.
 - e. **Save**를 클릭합니다.
3. 정책 그룹을 업데이트하거나 편집하려면 다음을 수행합니다.
 - a. **Edit Policies**를 클릭하고 정책을 관리할 운영 체제를 선택합니다.
 - b. 수정할 정책을 선택하고 구성을 완료합니다.
 - c. **Save and Publish**를 클릭합니다.

이 노트:

- Wyse Management Suite에서 지원하는 다양한 구성 정책에 대한 자세한 내용은 support.dell.com에서 *Dell Wyse Management Suite Administrator's Guide(Dell Wyse Management Suite 관리자 가이드)*를 참조하십시오.
- 서브넷, 시간대, 위치와 같은 특정 특성을 기반으로 그룹을 자동으로 생성하거나 장치를 그룹에 할당하는 규칙을 생성할 수 있습니다.

새 씬 클라이언트 등록

이 노트: 고객 보안 환경에 대한 자세한 내용은 **Wyse Device Agent**를 참조하십시오.

WDA(Wyse Device Agent)를 통해 씬 클라이언트를 Wyse Management Suite에 수동으로 등록할 수 있습니다. DHCP 서버에서 적절한 옵션 태그를 구성하거나 DNS 서버에서 적절한 DNS SRV 레코드를 구성하여 씬 클라이언트를 자동으로 등록할 수도 있습니다.

여러 서버넷의 장치가 여러 서버넷을 포함하는 다른 Wyse Management Suite 그룹에 자동으로 체크인하도록 하려면 DHCP 옵션 태그를 사용하여 쉐인 클라이언트를 등록합니다. 예를 들어, TimeZone_A의 장치는 TimeZoneA에 구성된 ProfileGroup에 체크인할 수 있습니다.

TLD에서 Wyse Management Suite 서버 정보를 입력하려는 경우 장치 규칙에 따라 자동 그룹 할당을 허용하기 위해 Wyse Management Suite Pro를 설치했다면 DNS 서버의 DNS SRV 레코드를 사용하여 쉐인 클라이언트를 등록합니다. 예를 들어, 장치가 TimeZoneA에서 체크인하는 경우 TimeZoneA용으로 구성된 ProfileGroup에 장치를 할당합니다.

Wyse Management Suite가 자체 서명된 인증서가 있는 프라이빗 클라우드에 위치한 경우 보안 통신을 위해 쉐인 클라이언트에 다음 버전의 Wyse Device Agents 또는 펌웨어가 설치되어 있어야 합니다.

- Windows Embedded 시스템 - 13.0 이상 버전
- Thin Linux - 2.0.24 이상 버전
- ThinOS - 펌웨어 8.4 이상 버전
- HTTPS 대신 HTTP URL을 사용하여 이전 버전 에이전트에 장치를 등록할 수 있습니다. 에이전트 또는 펌웨어를 최신 버전으로 업그레이드한 이후에는 Wyse Management Suite와의 통신이 자동으로 https로 전환됩니다.
- downloads.dell.com/wyse/wda에서 최신 버전 WDA를 다운로드할 수 있습니다.
- Wyse Management Suite를 프라이빗 클라우드에 설치하고 인증 기관(예: www.geotrust.com)에서 인증서를 가져온 경우 **Portal Administration > Setup**으로 이동하여 **Certification Validation** 확인란을 선택합니다. 잘 알려진 인증 기관에서 인증서를 가져오지 않은 경우 이 확인란을 선택하면 안 됩니다. 퍼블릭 클라우드의 인증서 유효성 검사는 항상 활성화되어 있으므로 퍼블릭 클라우드에서는 Wyse Management Suite에 대해 이 옵션을 사용할 수 없습니다.

수동으로 ThinOS 장치 등록

ThinOS 장치를 수동으로 등록하려면 다음을 수행합니다.

1. 데스크탑 메뉴에서 **System Setup > Central Configuration**으로 이동합니다. **Central Configuration** 창이 표시됩니다.
2. **WDA** 탭을 클릭합니다.
기본적으로 **WMS**가 선택되어 있습니다.

이 노트: WDA 서비스는 클라이언트 부팅 프로세스가 완료된 후 자동으로 실행됩니다.

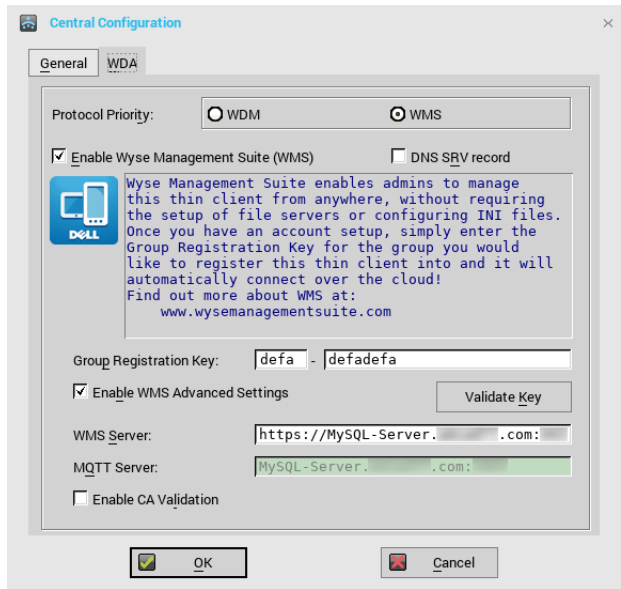


그림 11. 중앙 구성

3. Wyse Management Suite를 활성화하려면 **Enable Wyse Management Suite** 확인란을 선택합니다.
4. 원하는 그룹에 대하여 관리자가 구성한 대로 **Group Registration Key**를 입력합니다.
5. **Enable WMS Advanced Settings** 옵션을 선택하고 WMS 서버 또는 MQTT 서버 세부 정보를 입력합니다.
6. 라이선스 유형(퍼블릭 클라우드 또는 프라이빗 클라우드)에 따라 CA Validation를 활성화 또는 비활성화합니다.
 - 퍼블릭 클라우드 - 퍼블릭 클라우드에서 Wyse Management Suite에 장치를 등록한 경우 **Enable CA Validation** 확인란을 선택합니다.

- 프라이빗 클라우드 - 잘 알려진 인증 기관의 인증서를 Wyse Management Suite 서버로 가져온 경우 **Enable CA Validation** 확인란을 선택합니다.

노트:

미국 Wyse Management Suite Pro 클라우드 버전의 경우 기본 WMS 서버 및 MQTT 서버 세부 정보를 변경하지 마십시오. 유럽 Wyse Management Suite Pro 클라우드 버전의 경우 다음을 사용합니다.

- CCM 서버 - eu1.wysemanagementsuite.com
- MQTT 서버 - eu1-pns.wysemanagementsuite.com:1883

7. 설정을 확인하려면 **Validate Key**를 클릭합니다. 키가 확인되면 장치가 자동으로 다시 시작됩니다.

노트:

키가 확인되지 않는 경우 제공된 자격 증명을 확인합니다. 포트 443 및 1883이 네트워크에 의해 차단되지 않았는지 확인합니다.

8. **OK(확인)**를 클릭합니다.

장치가 Wyse Management Suite 콘솔에 등록됩니다.

Windows Embedded Standard 장치 및 Linux 장치를 등록하는 방법에 대한 자세한 내용은 [수동으로 Windows Embedded 장치 등록](#) 및 [수동으로 Linux 장치 등록](#)을 참조하십시오.

INI 파일을 사용하여 ThinOS 장치 등록

wynos.ini 또는 xen.ini를 사용하여 ThinOS 장치를 구성하려는 경우 추가 정보를 .ini 파일에 게시하여 장치가 Wyse Management Suite 서버에 체크인하도록 알릴 수 있습니다.

예:

- ThinOS 8.5의 예:
WDAService=yes \
Priority=WMS
WMSEnable=yes \
Server=<서버 URL> \
CAValidation=no \
Override=yes
- ThinOS 8.4의 예:
WDAService=yes \
Priority=CCM
CCMEnable=yes \
CCMServer=<서버 URL> \
GroupPrefix=<접두사> \
GroupKey=<키> \
MQTTServer=<서버 URL> \
Override=yes \
CAValidation=no

자세한 내용은 support.dell.com의 최신 *Dell Wyse ThinOS INI 가이드*를 참조하십시오.

노트:

- ThinOS 8.3(ThinOS Lite 2.3) 이상 버전의 경우 `WDA Service Priority` 명령을 사용하여 관리 프로토콜을 지정할 수 있습니다. 이 명령은 관리 서버를 검색하는 데 사용됩니다.
- ThinOS 버전 8.3, 8.4 및 8.5의 CCM 태그는 서로 다릅니다.

DHCP 옵션 태그를 사용하여 디바이스 등록

노트:

- Windows 서버에서 DHCP 옵션 태그를 추가하는 방법에 대한 자세한 지침은 [DHCP 옵션 태그 생성 및 구성](#)을 참조하십시오. 고객 보안 환경에 대한 자세한 내용은 [Wyse Device Agent](#)를 참조하십시오.

다음 DHCP 옵션 태그를 사용하여 디바이스를 등록할 수 있습니다.

표 2. DHCP 옵션 태그를 사용하여 디바이스 등록

옵션 태그	설명
이름 - WMS 데이터 유형 - 문자열 코드 - 165 설명 - WMS 서버 FQDN	이 태그는 Wyse Management Suite 서버 URL을 가리킵니다. 예: <code>wmserver.acme.com:443</code>. 여기서 <code>wmserver.acme.com</code>은 Wyse Management Suite가 설치된 서버의 정규화된 도메인 이름입니다. 퍼블릭 클라우드의 Wyse Management Suite에 장치를 등록하기 위한 링크는 퍼블릭 클라우드의 Wyse Management Suite 시작하기를 참조하십시오. ① 노트: 서버 URL에 <code>https://</code>를 사용하지 마십시오. 그렇지 않으면 쉘 클라이언트가 Wyse Management Suite에 등록되지 않습니다.
이름 - MQTT 데이터 유형 - 문자열 코드 - 166 설명 - MQTT 서버	이 태그는 디바이스를 Wyse Management Suite PNS(Push Notification Server)로 연결합니다. 프라이빗 클라우드 설치의 경우 디바이스가 Wyse Management Suite 서버의 MQTT 서비스로 연결됩니다. 예: <code>wmservername.domain.com:1883</code>. Wyse Management Suite 퍼블릭 클라우드에서 디바이스를 등록하려면 디바이스가 퍼블릭 클라우드의 PNS(MQTT) 서버를 가리켜야 합니다. 예를 들면, 다음과 같습니다. US1: us1-pns.wysemanagementsuite.com EU1: eu1-pns.wysemanagementsuite.com
이름 - CA 유효성 검사 데이터 유형 - 문자열 코드 - 167 설명 - 인증 기관 검증	Wyse Management Suite가 프라이빗 클라우드의 시스템에 설치되어 있는 경우 이 태그가 필요합니다. 퍼블릭 클라우드에서 Wyse Management Suite로 장치를 등록하는 경우 이 옵션 태그를 추가하지 마십시오. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져온 경우 True를 입력합니다. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져오지 않은 경우 False를 입력합니다.
이름 - GroupToken 데이터 유형 - 문자열 코드 - 199 설명 - 그룹 토큰	이 태그는 ThinOS 디바이스를 퍼블릭 또는 프라이빗 클라우드의 Wyse Management Suite에 등록하는 경우에 필수입니다. 이 태그는 Windows Embedded Standard 또는 ThinLinux 디바이스를 프라이빗 클라우드의 Wyse Management Suite에 등록하는 경우에 선택 사항입니다. 태그를 사용할 수 없는 경우 온프레미스 설치 중에 디바이스가 관리되지 않는 그룹에 자동으로 등록됩니다.

DNS SRV 레코드를 사용하여 디바이스 등록

① 노트: 고객 보안 환경에 대한 자세한 내용은 [Wyse Device Agent](#)를 참조하십시오.

DNS 기반 장치 등록은 다음 Wyse Device Agent 버전에서 지원됩니다.

- Windows Embedded 시스템 - 13.0 이상 버전
- ThinLinux - 2.0.24 이상 버전
- ThinOS - 펌웨어 8.4 이상 버전

DNS SRV 레코드 필드가 유효한 값으로 설정된 경우 Wyse Management Suite 서버에 디바이스를 등록할 수 있습니다.

① 노트: Windows 서버에서 DNS SRV 레코드를 추가하는 방법에 대한 자세한 지침은 [DNS SRV 레코드 생성 및 구성](#)을 참조하십시오.

다음 표에는 DNS SRV 레코드의 유효한 값이 나열되어 있습니다.

표 3. DNS SRV 레코드를 사용하여 디바이스 구성

URL/태그	설명
레코드 이름 - _WMS_MGMT 레코드 FQDN - _WMS_MGMT._tcp.<도메인 이름> 레코드 유형 - SRV	이 레코드는 Wyse Management Suite 서버 URL을 가리킵니다. 예: <code>wmserver.acme.com:443</code>. 여기서 <code>wmserver.acme.com</code>은 Wyse Management Suite가 설치된 서버의 정규화된 도메인 이름입니다. 퍼블릭 클라우드의 Wyse Management Suite에 장치를 등록하기 위한 링크는 퍼블릭 클라우드의 Wyse Management Suite 시작하기를 참조하십시오. ❗ 노트: 서버 URL에 <code>https://</code>를 사용하지 마십시오. 그렇지 않으면 쉘 클라이언트가 Wyse Management Suite에 등록되지 않습니다.
레코드 이름 - _WMS_MQTT 레코드 FQDN - _WMS_MQTT._tcp.<도메인 이름> 레코드 유형 - SRV	이 레코드는 디바이스를 Wyse Management Suite PNS(Push Notification Server)로 연결합니다. 프라이빗 클라우드 설치의 경우 디바이스가 Wyse Management Suite 서버의 MQTT 서비스로 연결됩니다. 예: <code>wmservername.domain.com:1883</code>. ❗ 노트: MQTT는 최신 Wyse Management Suite 버전에 대해 선택 사항입니다. Wyse Management Suite 퍼블릭 클라우드에서 디바이스를 등록하려면 디바이스가 퍼블릭 클라우드의 PNS(MQTT) 서버를 가리켜야 합니다. 예를 들면, 다음과 같습니다. US1 - us1-pns.wysemanagementsuite.com EU1 - eu1-pns.wysemanagementsuite.com
레코드 이름 - _WMS_GROUPTOKEN 레코드 FQDN - _WMS_GROUPTOKEN.<Domain> 레코드 유형 - TEXT	이 레코드는 ThinOS 디바이스를 퍼블릭 또는 프라이빗 클라우드의 Wyse Management Suite에 등록하는 경우 필수입니다. 이 레코드는 Windows Embedded Standard 또는 ThinLinux 디바이스를 프라이빗 클라우드의 Wyse Management Suite에 등록하는 경우 선택 사항입니다. 레코드를 사용할 수 없는 경우 온프레미스 설치 중에 디바이스가 관리되지 않는 그룹에 자동으로 등록됩니다. ❗ 노트: 그룹 토큰은 프라이빗 클라우드의 최신 Wyse Management Suite 버전에서 선택 사항입니다.
레코드 이름 - _WMS_CAVVALIDATION 레코드 FQDN - _WMS_CAVVALIDATION.<Domain> 레코드 유형 - TEXT	Wyse Management Suite가 프라이빗 클라우드의 시스템에 설치되어 있는 경우 이 레코드가 필요합니다. 장치를 퍼블릭 클라우드의 Wyse Management Suite에 등록하는 경우 이 선택 사항 레코드를 추가하지 마십시오. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져온 경우 True를 입력합니다. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져오지 않은 경우 False를 입력합니다. ❗ 노트: CA 유효성 검사는 최신 Wyse Management Suite 버전에 대해 선택 사항입니다.

썬 클라이언트에 애플리케이션 배포

표준 애플리케이션 정책을 사용하면 단일 애플리케이션 패키지를 설치할 수 있으며 애플리케이션 설치 후에도 재부팅해야 합니다. 고급 애플리케이션 정책을 사용하면 두 번의 재부팅만으로 여러 애플리케이션 패키지를 설치할 수 있습니다. 또한 고급 애플리케이션 정책은 특정 애플리케이션을 설치하는 데 필요할 수 있는 사전 및 사후 설치 스크립트 실행을 지원합니다. 자세한 내용은 [부록 B](#)를 참조하십시오.

주제:

- [ThinOS 펌웨어 이미지 인벤토리 업로드 및 배포](#)
- [표준 애플리케이션 정책 생성 및 썬 클라이언트에 배포](#)

ThinOS 펌웨어 이미지 인벤토리 업로드 및 배포

ThinOS 이미지 인벤토리에 파일을 추가하려면 다음을 수행합니다.

1. **Apps & Data** 탭의 OS Image Repository에서 **ThinOS**를 클릭합니다.
2. **Add Firmware File**을 클릭합니다.
Add File 화면이 표시됩니다.
3. 파일을 선택하려면 **Browse**를 클릭하고 파일이 있는 위치로 이동합니다.
4. 파일에 대한 설명을 입력합니다.
5. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
6. **Upload**를 클릭합니다.

노트: 확인란을 선택하면 파일이 리포지토리에 추가되지만 그룹 또는 장치에 할당되지 않습니다. 파일을 할당하려면 해당 장치 구성 페이지로 이동합니다.

표준 애플리케이션 정책 생성 및 썬 클라이언트에 배포

썬 클라이언트에 표준 애플리케이션 정책을 배포하려면 다음을 수행합니다.

1. 로컬 리포지토리에서 **thinClientApps**로 이동하고 애플리케이션을 폴더에 복사합니다.
2. **Apps & Data** 탭으로 이동하고 **App Inventory**에서 **Thin Client**를 선택하여 애플리케이션이 등록되어 있는지 확인합니다.

노트: 앱 인벤토리 인터페이스에서 최근에 추가된 프로그램을 채우는 데 약 2분이 걸립니다.

3. **App Policies**에서 **Thin Client**를 클릭합니다.
4. **Add Policy**를 클릭합니다.
5. 애플리케이션 정책을 생성하려면 Add Standard App Policy 창에 적절한 정보를 입력합니다.

- a. **Policy Name, Group, Task, Device Type** 및 **TC Application**을 선택합니다.
- b. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS Subtype Filter** 또는 **Platform Filter**를 선택합니다.
시간 초과를 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
- c. 이 정책을 Wyse Management Suite에 등록된 장치에 자동으로 적용하려면 **Apply Policy Automatically** 드롭다운 목록에서 **Apply the policy to new devices**를 선택합니다.

노트:

- 장치가 정의된 그룹으로 이동하거나 그룹에 직접 등록되면 앱 정책이 적용됩니다.
 - **Apply the policy to devices on check in**을 선택한 경우 Wyse Management Suite 서버에 체크인할 때 정책이 장치에 자동으로 적용됩니다.
6. 정책 실행 시 지연을 허용하려면 **Allow delay of policy execution** 확인란을 선택합니다. 이 옵션을 선택한 경우 다음 드롭다운 메뉴가 활성화됩니다.

- **Max Hours per Delay** 드롭다운 메뉴에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
 - **Max delays** 드롭다운 메뉴에서 정책 실행을 지연할 수 있는 횟수(1~3)를 선택합니다.
7. 정의된 값 이후에 설치 프로세스를 중지하려면 **Application Installation Timeout** 필드에 시간(분)을 지정합니다.
 8. **Save**를 클릭하여 정책을 생성합니다.
관리자가 그룹을 기준으로 이 정책을 장치에 예약할 수 있는 메시지가 표시됩니다.
 9. 동일한 페이지에서 작업을 예약하려면 **Yes**를 선택합니다.
앱/이미지 정책 작업은 다음 방식으로 실행할 수 있습니다.
 - a. **Immediately** - 서버가 작업을 즉시 실행합니다.
 - b. **On device time zone** - 서버가 각 장치 시간대에 대해 하나의 작업을 생성하고 장치 시간대의 선택한 날짜/시간으로 작업을 예약합니다.
 - c. **On selected time zone** - 서버가 지정된 시간대의 날짜/시간에 실행할 하나의 작업을 생성합니다.
 10. 작업을 생성하려면 **Preview**를 클릭합니다. 그러면 일정이 다음 페이지에 표시됩니다.
 11. **Jobs** 페이지로 이동하여 작업 상태를 확인할 수 있습니다.

Wyse Management Suite 제거

Wyse Management Suite를 제거하려면 다음을 수행합니다.

1. **WMS** 아이콘을 두 번 클릭합니다.

제거 프로그램 마법사가 시작되고 **Wyse Management Suite uninstaller** 화면이 표시됩니다.

2. **Next**를 클릭합니다. 모든 Wyse Management Suite 설치 프로그램 구성 요소를 제거하는 **Remove** 라디오 버튼이 기본적으로 선택됩니다.

Wyse Management Suite 문제 해결

이 섹션에서는 Wyse Management Suite에 대한 문제 해결 정보를 제공합니다.

Wyse Management Suite 웹 콘솔 액세스 문제

- 문제: Wyse Management Suite 콘솔에 연결하려고 하면 인증 GUI가 표시되지 않고 HTTP 상태 404 페이지가 표시됩니다.

해결 방법: 다음 순서대로 서비스를 중지하고 시작합니다.

1. Dell WMS: MariaDB
2. Dell WMS: memcached
3. Dell WMS: MongoDB
4. Dell WMS: MQTT 브로커 서비스
5. Dell WMS: Tomcat 서비스

- 문제: Wyse Management Suite 콘솔에 연결하려고 하면 인증 GUI가 표시되지 않고 다음 오류 메시지가 표시됩니다.

This page can't be displayed

해결 방법: Dell WMS: Tomcat 서비스 다시 시작

- 문제: Wyse Management Suite 웹 콘솔이 응답하지 않거나 Internet Explorer를 사용할 때 웹 페이지의 정보가 올바르게 표시되지 않습니다.

해결 방법:

- 지원되는 버전의 Internet Explorer를 사용하고 있는지 확인합니다.
- Internet Explorer Enhanced Security 기능이 비활성화되어 있는지 확인합니다.
- 호환성 보기 설정이 비활성화되어 있는지 확인합니다.

Wyse Management Suite에 장치 등록

이 노트: 고객 보안 환경에 대한 자세한 내용은 [Wyse Device Agent](#)를 참조하십시오.

- 문제: 퍼블릭 클라우드에서 Wyse Management Suite에 장치를 등록할 수 없음

해결 방법:

- 포트 443 및 1883이 열려 있는지 확인합니다.
- 네트워크 연결을 확인하고 퍼블릭 클라우드용 브라우저에서 Wyse Management 웹 애플리케이션에 액세스합니다.
- **Automatic Discovery**가 활성화되어 있는 경우 DHCP 또는 DNS SVR 레코드가 올바르게 구성되어 있는지 확인합니다. 또한 서버 URL과 그룹 토큰을 확인합니다.
- 장치를 수동으로 등록할 수 있는지 확인합니다.

- 문제: 프라이빗 클라우드에서 Wyse Management Suite에 장치를 등록할 수 없음

해결 방법:

- 포트 443 및 1883이 열려 있는지 확인합니다.
- 인터넷 연결을 확인하고 브라우저에서 Wyse Management 웹 애플리케이션에 액세스할 수 있는지 확인합니다.
- Automatic Discovery가 활성화되어 있는 경우 DHCP 또는 DNS SRV 레코드가 올바르게 구성되어 있는지 확인합니다. 또한 서버 URL과 그룹 토큰을 확인합니다.
- 장치를 수동으로 등록할 수 있는지 확인합니다.
- 자체 서명되거나 잘 알려진 인증서를 사용하고 있는지 확인합니다.

이 노트: 기본적으로 Wyse Management Suite는 자체 서명된 인증서를 설치합니다. 장치가 Wyse Management Suite 서버와 통신하려면 CA Validation를 비활성화해야 합니다.

장치에 명령을 전송하는 중 오류 발생

문제: 패키지 업데이트, 장치로 재부팅 등과 같은 명령을 전송할 수 없습니다.

해결 방법:

- Dell WMS: MQTT 브로커 서비스가 Wyse Management Suite 서버에서 실행 중인지 확인합니다.
- 포트 1883이 열려 있는지 확인합니다.
- 명령을 전송하기 전에 장치가 종료되거나 절전 상태에 있지 않은지 확인합니다.

Wyse Device Agent

WDA(Wyse Device Agent)는 모든 씬 클라이언트 관리 솔루션을 위한 통합 에이전트입니다. WDA를 설치하면 Wyse Management Suite를 사용하여 씬 클라이언트를 관리할 수 있습니다.

Wyse Device Agent가 지원하는 세 가지 유형의 고객 보안 환경은 다음과 같습니다.

- **Highly secured environments** - DHCP 또는 DNS 서버가 새 장치 검색에 실패하는 위험을 줄이기 위해 관리자가 각 장치에 개별적으로 로그인하고 Wyse Management Suite 서버 URL을 구성해야 합니다. CA 서명 또는 자체 서명 인증서를 사용할 수 있습니다. 하지만 Dell은 CA 서명 인증서를 사용할 것을 권장합니다. 자체 서명 인증서가 있는 Wyse Management Suite 프라이빗 클라우드 솔루션의 경우 모든 장치에서 인증서를 수동으로 구성해야 합니다. 또한 인증서를 Agent Configuration 폴더에 복사하여 인증서를 보존하고, 장치 이미지를 재작성한 후에도 DHCP 또는 DNS 서버가 검색에 실패하는 위험을 줄여야 합니다.

Agent Configuration 폴더는 다음 위치에 있습니다.

- Windows Embedded Standard 장치 - %SYSTEMDRIVE%\Wyse\WCM\ConfigMgmt\Certificates
- ThinLinux 장치 - /etc/addons.d/WDA/certs
- ThinOS 장치 - wnos/cacerts/

❗ 노트: USB 드라이브 또는 FTP 경로를 사용하여 인증서를 ThinOS 운영 체제를 실행하는 씬 클라이언트로 가져와야 합니다.

- **Secured environments** - DHCP 또는 DNS 서버가 새 장치 검색에 실패하는 위험을 줄이기 위해 관리자가 CA 서명 인증서를 사용하여 Wyse Management Suite 서버를 구성해야 합니다. 장치는 DHCP/DNS 레코드에서 Wyse Management Suite 서버 URL을 가져오고 CA Validation를 수행할 수 있습니다. 자체 서명 인증서가 있는 Wyse Management Suite 프라이빗 클라우드 솔루션은 등록 전에 장치에 인증서가 없는 경우 처음 등록 후 인증서를 장치로 푸시해야 합니다. 이 인증서는 DHCP 또는 DNS 서버가 검색에 실패하는 위험을 줄이기 위해 장치 이미지를 재작성하거나 장치를 재시작한 후에도 보존됩니다.
- **Normal environments** - 장치가 CA 서명 또는 자체 서명 인증서로 구성된 Wyse Management Suite 프라이빗 클라우드에 대해 DHCP/DNS 레코드에서 Wyse Management Suite 서버 URL을 가져옵니다. 장치에서 CA Validation 옵션이 비활성화되어 있는 경우 장치를 처음 등록하면 Wyse Management Suite 관리자가 알림을 받습니다. 이 시나리오에서 Dell은 관리자가 서버가 자체 서명 인증서로 구성된 장치로 인증서 푸시를 수행할 것을 권장합니다. 이 환경은 퍼블릭 클라우드에 사용할 수 없습니다.

추가 자료

비디오 안내:

- Wyse Management Suite 설치에 [Wyse Management Suite 설치](#)를 참조하십시오.
- Wyse Management Suite 온-프레미스를 DHCP 옵션 태그와 함께 사용하여 ThinOS 클라이언트를 자동으로 구성하는 방법은 [Wyse Management Suite를 사용하여 ThinOS 장치 구성](#)을 참조하십시오.

원격 데이터베이스

원격 또는 클라우드 데이터베이스(DB)는 하이브리드 클라우드, 퍼블릭 클라우드, 프라이빗 클라우드와 같은 가상화된 환경을 위해 구축된 데이터베이스입니다. Wyse Management Suite에서 요구 사항에 따라 Mongo 데이터베이스(MongoDB), Maria 데이터베이스(MariaDB) 또는 두 데이터베이스 모두를 구성할 수 있습니다.

주제:

- [Configure Mongo database](#)
- [Configure Maria database](#)

Configure Mongo database

Mongo database (MongoDB) operates on the Transmission Control Protocol (TCP) port number 27017.

 **NOTE: Replace any value that is boldfaced with your environment variables, as applicable.**

To configure MongoDB, do the following:

1. Install the MongoDB version 4.2.1.
2. Copy the MongoDB files to your local system—C:\Mongo.
3. Create the following directories if they do not exist:
 - C:\data
 - C:\data\db
 - C:\data\log
4. Go to the Mongo folder (C:\Mongo), and create a file named mongod.cfg.
5. Open the mongod.cfg file in a notepad, and add the following script:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
```

6. Save and close the mongod.cfg file.
7. Open command prompt as an administrator, and run the following command:


```
mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" --install or sc.exe create
MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\" --service --config=
\"C:\ProgramFiles\MongoDB\Server\4.2\mongod.cfg\"" DisplayName= "Dell WMS: MongoDB"
start="auto"
```

 MongoDB is installed.
8. To start the MongoDB services, run the following command:


```
net start mongoDB
```
9. To start the Mongo database, run the following command:


```
mongo.exe
```
10. To open the default admin db, run the following command:


```
use admin;
```
11. After the MongoDB sheet is displayed, run the following commands:

```
db.createUser(
{
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
```

```
{role:"readWriteAnyDatabase",db:"admin"},
{role:"dbOwner",db:"stratus"}}]
}
)
```

12. To switch to the stratus database, run the following command:

```
use stratus;
```

13. To stop the MongoDB services, run the following command:

```
net stop mongoDB
```

14. Add an authentication permission to the admin DB. Modify the mongod.cfg file to the following:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
security:
authorization:enabled
```

15. To restart the MongoDB service, run the following:

```
net Start mongoDB;
```

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MongoDB. For information about setting the MongoDB on the Wyse Management Suite installer, see [Custom installation](#).

Configure Maria database

Maria database (MariaDB) operates on the Transmission Control Protocol (TCP) port number 3306.

NOTE:

- **The IP address displayed here belongs to the Wyse Management Suite server that hosts the web components.**
- **Replace any value that is boldfaced with your environment variables, as applicable.**

To configure MariaDB, do the following:

1. Install the MariaDB version 10.2.29.
2. Navigate to the MariaDB installation path—C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p.
3. Provide the root password which was created during installation
4. Create the database stratus—`DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;`
5. Create user 'stratus'@'localhost';
6. Create user 'stratus'@'**IP ADDRESS**';
7. Set a password for 'stratus'@'localhost'=password('PASSWORD');
8. Set a password for 'stratus'@'**IP ADDRESS**'=password('PASSWORD');
9. Provide all privileges on *.* to 'stratus'@'**IP ADDRESS**' identified by 'PASSWORD' with a grant option.
10. Provide all privileges on *.* to 'stratus'@'localhost' identified by 'PASSWORD' with a grant option.

 **NOTE:** To configure custom port for MariaDB, navigate to C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port> in the second step.

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MariaDB. For information about setting the MariaDB on the Wyse Management Suite installer, see [Custom installation](#).

사용자 정의 설치

사용자 정의 설치에서 Wyse Management Suite를 설정할 데이터베이스를 선택할 수 있으며 Wyse Management Suite에 대한 기본적인 기술 작업 지식이 있어야 합니다. Dell은 고급 사용자만 사용자 정의 설치를 사용하도록 권장합니다.

1. 설치 유형을 맞춤 설정으로 선택하고 다음을 클릭합니다.

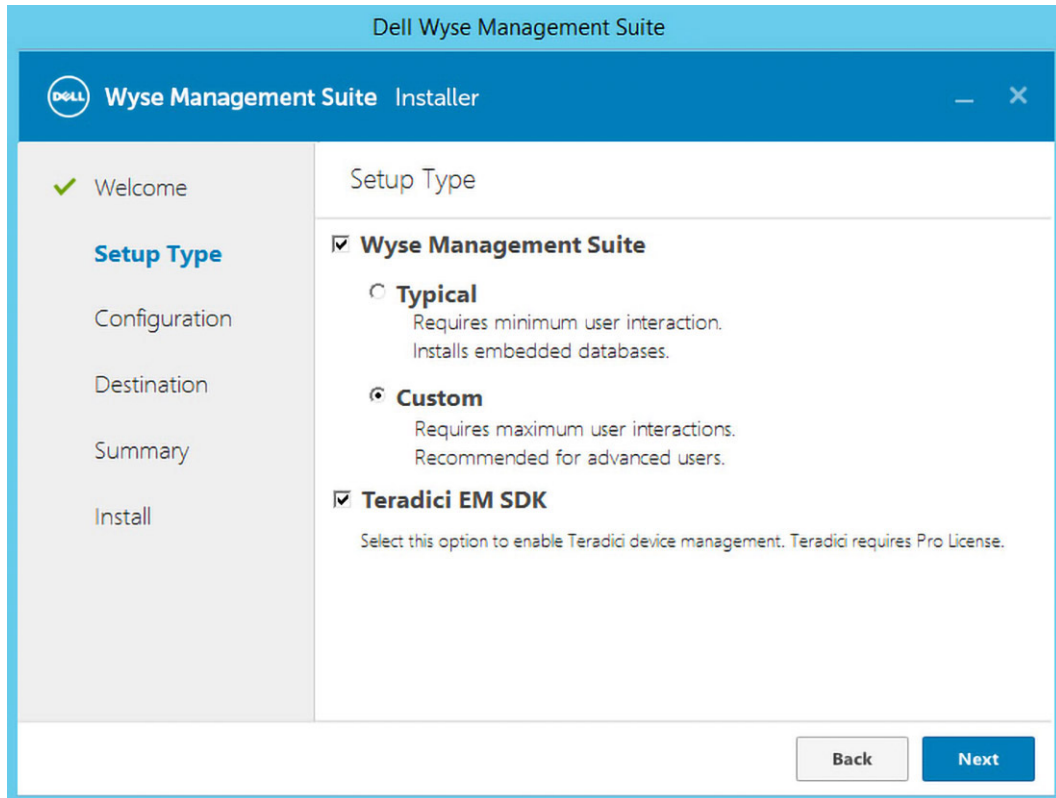


그림 12. 설치 유형

Mongo Database Server 페이지가 표시됩니다.

2. **Embedded MongoDB** 또는 **External MongoDB**를 Mongo 데이터베이스 서버로 선택합니다.

- **Embedded MongoDB**를 선택한 경우 암호를 제공하고 **Next**를 클릭합니다.

노트: Embedded Mongo 데이터베이스를 선택한 경우에는 사용자 이름과 데이터베이스 서버 세부 정보가 필요하지 않으므로 해당 필드가 회색으로 표시됩니다.

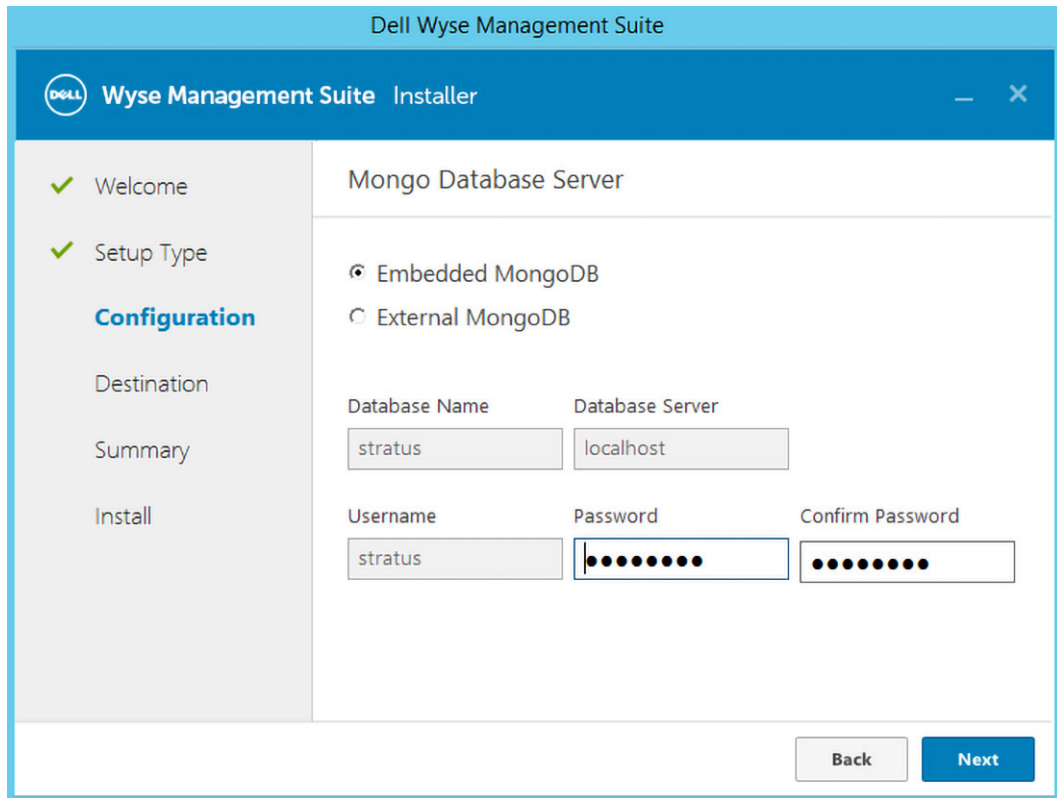


그림 13 . Embedded Mongo 데이터베이스 서버

External MongoDB를 선택한 경우 사용자 이름, 암호, 데이터베이스 서버 세부 정보 및 포트 세부 정보를 제공하고 **Next**를 클릭합니다.

노트: 포트 필드는 변경할 수 있는 기본 포트를 채웁니다.

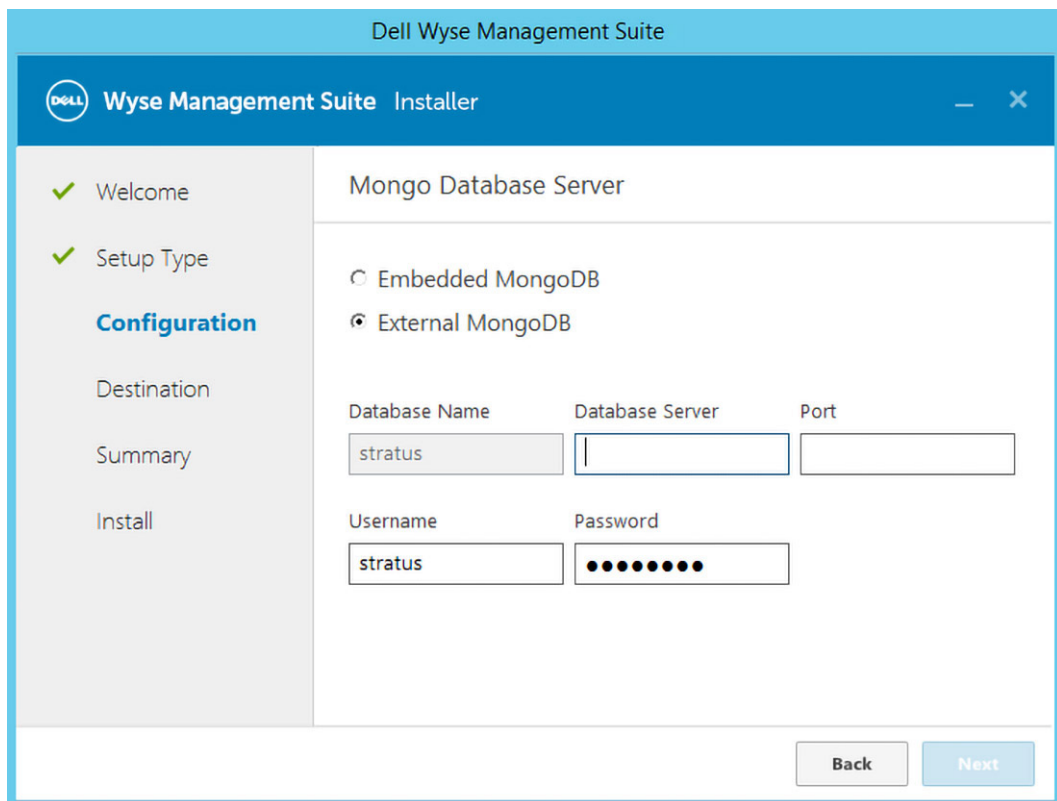


그림 14 . 외부 MongoDB

MariaDB Database Server 페이지가 표시됩니다.

3. **Embedded MariaDB** 또는 **External MariaDB**를 MariaDB 데이터베이스 서버로 선택합니다.
 - **Embedded MariaDB**를 선택한 경우 사용자 이름과 암호를 제공하고 **Next**를 클릭합니다.

The screenshot shows the 'Dell Wyse Management Suite Installer' window. On the left is a navigation pane with 'Welcome' and 'Setup Type' marked with green checkmarks, and 'Configuration' highlighted in blue. Below 'Configuration' are links for 'Destination', 'Summary', and 'Install'. The main area is titled 'MariaDB Database Server'. It has two radio buttons: 'Embedded MariaDB' (selected) and 'External MariaDB'. Below these are input fields for 'Database Name' (containing 'stratus') and 'Database Server' (containing 'localhost'). Further down are fields for 'Username' (containing 'stratus'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom right are 'Back' and 'Next' buttons, with 'Next' being the active button.

그림 15 . Embedded MariaDB

- **External MariaDB**를 선택한 경우 사용자 이름, 암호, 데이터베이스 서버 세부 정보 및 포트 세부 정보를 제공하고 **Next**를 클릭합니다.
포트 필드는 변경할 수 있는 기본 포트를 채웁니다.

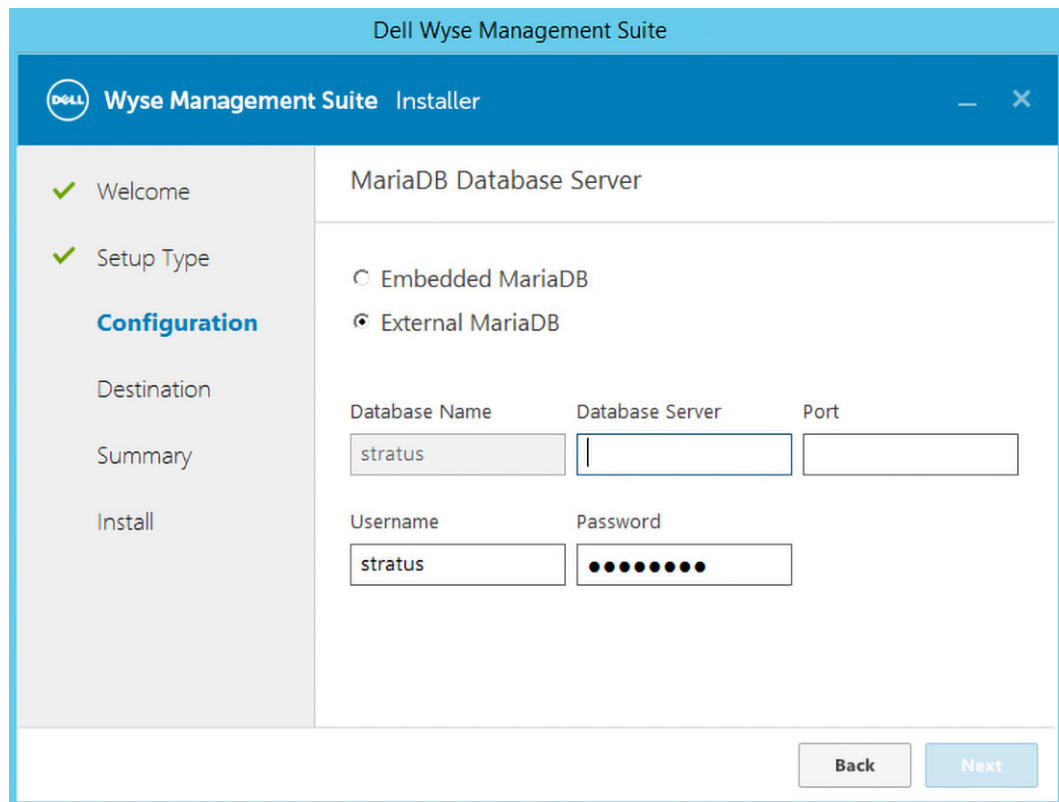


그림 16 . 외부 MariaDB

4. 다음 데이터베이스에 대해 포트를 사용자 정의할 수 있는 **Port** 페이지가 표시됩니다.

- Apache Tomcat
- MySQL 데이터베이스
- Mongo 데이터베이스
- MQTT v3.1 브로커
- Memcached

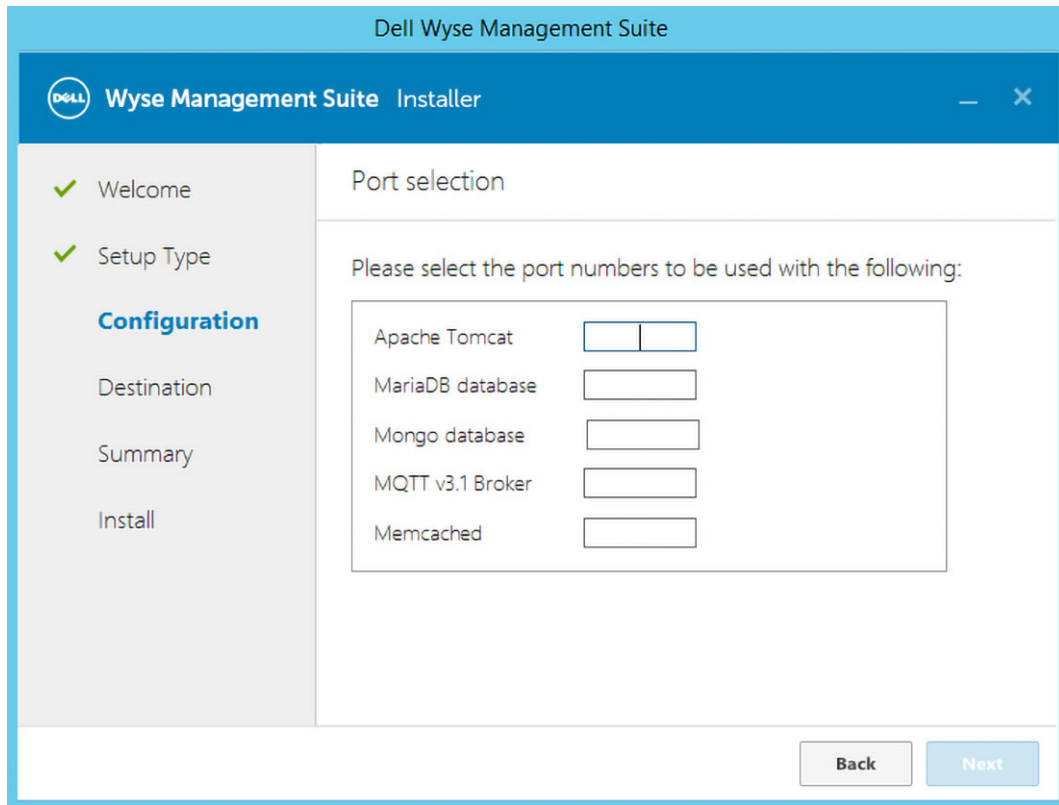


그림 17 . 포트 선택

노트: Wyse Management Suite는 다음과 같은 용도로 Maria 데이터베이스와 Mongo 데이터베이스를 사용합니다.

Maria 데이터베이스 - 잘 정의된 구조와 정규화가 필요한 데이터를 위한 관계형 데이터베이스

Mongo 데이터베이스 - 성능과 확장성을 위한 비 SQL 데이터베이스

설치를 완료하려면 [WMS 온-프레미스 설치 및 초기 설정](#) 섹션의 단계를 따릅니다.

Wyse Management Suite 아키텍처

다음 표에는 각 구독 유형에 대한 지원 기능 정보가 나와 있습니다.

표 4. 각 구독 유형에 대한 기능 매트릭스

기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro Edition
썬 클라이언트 관리를 위한 고확장성 솔루션	최대 10,000개의 장치 무료	50,000개 이상의 장치	100만 개 이상의 장치
라이선스 키	필요 없음	필수	필수
그룹 기반 관리	지원됨	지원됨	지원됨
다중 수준 그룹 및 상속	지원됨	지원됨	지원됨
구성 정책 관리	지원됨	지원됨	지원됨
운영 체제 패치 및 이미지 관리	지원됨	지원됨	지원됨
상속 후 장치 수준에서 유효 구성 보기	지원됨	지원됨	지원됨
애플리케이션 정책 관리	지원됨	지원됨	지원됨
자산, 재고 및 시스템 관리	지원됨	지원됨	지원됨
자동 장치 검색	지원됨	지원됨	지원됨
실시간 명령	지원됨	지원됨	지원됨
스마트 예약	지원됨	지원됨	지원됨
경고, 이벤트 및 감사 로그	지원됨	지원됨	지원됨
보안 통신(HTTPS)	지원됨	지원됨	지원됨
방화벽이 설정된 상태로 장치 관리	제한됨*	제한됨*	지원됨
모바일 애플리케이션	지원되지 않음	지원됨	지원됨
이메일 및 모바일 애플리케이션을 사용한 경고	지원되지 않음	지원됨	지원됨
사용자 지정 애플리케이션 설치를 위한 스크립팅 지원	지원되지 않음	지원됨	지원됨
배포를 단순화하고 재부팅을 최소화하는 번들 애플리케이션	지원되지 않음	지원됨	지원됨
위임된 관리	지원되지 않음	지원됨	지원됨
장치 특성을 기준으로 동적 그룹 생성 및 할당	지원되지 않음	지원됨	지원됨
2단계 인증	지원됨	지원됨	지원됨

기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro Edition
역할 기반 관리를 위한 Active Directory 인증	지원되지 않음	지원됨	지원됨
멀티 테넌시	지원되지 않음	지원됨	지원됨
엔터프라이즈급 보고	지원되지 않음	지원됨	지원됨
다중 리포지토리	지원되지 않음	지원됨	지원됨
지원 플랫폼에서 하드웨어 포트 활성화/비활성화	지원되지 않음	지원됨	지원됨
지원 플랫폼에서 BIOS 구성	지원되지 않음	지원됨	지원됨
정책 구성 내보내기 및 가져오기	지원되지 않음	지원됨	지원됨
애플리케이션 정책에 리포지토리 할당	지원되지 않음	지원됨	지원됨
썬 클라이언트에 대한 shutdown 명령	지원됨	지원됨	지원됨
Wyse Management Suite 콘솔 시간 초과	지원되지 않음	지원됨	지원됨
정책 순서	지원되지 않음	지원됨	지원됨
운영 체제에 따라 애플리케이션 선택 간소화	지원됨	지원됨	지원됨
별칭 구성 옵션	지원되지 않음	지원됨	지원됨

 **노트:** *별표는 보안 방화벽 작업 환경에서만 Wyse Management Suite를 사용하여 장치를 관리할 수 있음을 나타냅니다. 방화벽 설정의 범위를 벗어나는 썬 클라이언트는 관리할 수 없습니다.

Wyse Management Suite 파일 리포지토리 액세스

파일 리포지토리는 파일이 저장되고 구성되는 위치입니다. Wyse Management Suite에는 두 가지 유형의 리포지토리가 있습니다.

- **로컬 리포지토리** - Wyse Management Suite 프라이빗 클라우드 설치 중에 Wyse Management Suite 설치 프로그램에서 로컬 리포지토리 경로를 제공합니다. 설치 후에 **포털 관리자 > 파일 리포지토리**로 이동하여 로컬 리포지토리를 선택합니다. **편집** 옵션을 클릭하여 리포지토리 설정을 보고 편집합니다.
- **Wyse Management Suite 리포지토리** - Wyse Management Suite 퍼블릭 클라우드에 로그인하고 **포털 관리자 > 파일 리포지토리**로 이동하여 Wyse Management Suite 리포지토리 설치 프로그램을 다운로드합니다. 설치 후에 필수 정보를 제공하여 Wyse Management Suite 리포지토리를 Wyse Management Suite 관리 서버에 등록합니다.

자동 복제 옵션을 활성화하여 파일 리포지토리에 추가된 파일을 다른 리포지토리에 복제할 수 있습니다. 이 옵션을 활성화하면 경고 메시지가 표시됩니다. **기존 파일 복제** 확인란을 선택하여 기존 파일을 파일 리포지토리에 복제할 수 있습니다.

리포지토리가 이미 등록된 경우 **기존 파일 복제** 옵션을 적용할 수 있습니다. 새 리포지토리가 등록되면 모든 파일이 새 리포지토리에 복사됩니다. **이벤트** 페이지에서 파일 복제 상태를 볼 수 있습니다.

① 노트:

- □□□ □□□□ 템플릿은 다른 리포지토리에 자동으로 복제되지 않습니다. 이러한 파일은 수동으로 복사해야 합니다.
- 파일 복제 기능은 Wyse Management Suite 2.0 이상 버전의 리포지토리에서만 지원됩니다.
- 원격 리포지토리의 자체 서명 인증서는 Wyse Management Suite 서버로 가져올 수 없습니다. 원격 리포지토리에 대해 CA 유효성 검사가 활성화된 경우 원격 리포지토리에서 로컬 리포지토리로의 파일 복제가 실패합니다.

Wyse Management Suite 리포지토리를 사용하려면 다음을 수행합니다.

1. 퍼블릭 클라우드 콘솔에서 Wyse Management Suite 리포지토리를 다운로드합니다.
2. 설치 프로세스 후에 애플리케이션을 시작합니다.
3. Wyse Management Suite Repository 페이지에서 자격 증명을 입력하여 Wyse Management Suite 리포지토리를 Wyse Management Suite 서버에 등록합니다.
4. 퍼블릭 WMS 관리 포털에 등록 옵션을 활성화하면 리포지토리를 Wyse Management Suite 퍼블릭 클라우드에 등록할 수 있습니다.
5. 파일 동기화 옵션을 클릭하여 파일 동기화 명령을 전송합니다.
6. 체크인을 클릭한 다음 명령 전송을 클릭하여 디바이스 정보 명령을 디바이스로 전송합니다.
7. 등록 취소 옵션을 클릭하여 온프레미스 서비스를 등록 취소합니다.
8. 편집을 클릭하여 파일을 편집합니다.
9. 동시 파일 다운로드 옵션의 드롭다운 목록에서 파일 수를 선택합니다.
10. Wake on LAN 옵션을 활성화 또는 비활성화합니다.
11. 빠른 파일 업로드 및 다운로드 HTTP) 옵션을 활성화 또는 비활성화합니다.
 - HTTP가 활성화되면 파일 업로드 및 다운로드가 HTTP를 통해 수행됩니다.
 - HTTP가 활성화되지 않으면 파일 업로드 및 다운로드가 HTTPS를 통해 수행됩니다.
12. 인증서 유효성 검사 확인란을 선택하여 퍼블릭 클라우드에 대한 CA 유효성 검사를 활성화합니다.

① **노트:** Wyse Management Suite 서버에서 CA 유효성 검사가 활성화되어 있으면 인증서가 클라이언트에 있어야 합니다. 앱 및 데이터, 이미지 가져오기/푸시와 같은 모든 작업이 성공적으로 완료됩니다. 인증서가 클라이언트에 없는 경우 Wyse Management Suite 서버가 이벤트 페이지에 인증 기관을 검증하지 못함이라는 하나의 일반 감사 이벤트 메시지를 제공합니다. 앱 및 데이터, 이미지 가져오기/푸시와 같은 모든 작업이 성공적으로 완료되지 않습니다. 또한 Wyse Management Suite 서버에서 CA 유효성 검사가 비활성화되어 있으면 서버 및 클라이언트의 통신이 인증서 서명 유효성 검사 없이 보안 채널에서 수행됩니다.
13. 제공된 상자에 메모를 추가합니다.
14. 설정 저장을 클릭합니다.

DHCP 옵션 태그 생성 및 구성

노트: 고객 보안 환경에 대한 자세한 내용은 [Wyse Device Agent](#)를 참조하십시오.

DHCP 옵션 태그를 생성하려면 다음을 수행합니다.

1. Server Manager를 엽니다.
2. Tools로 이동하여 **DHCP option**을 클릭합니다.
3. **FQDN > IPv4**로 이동하여 **IPv4**를 마우스 오른쪽 단추로 클릭합니다.

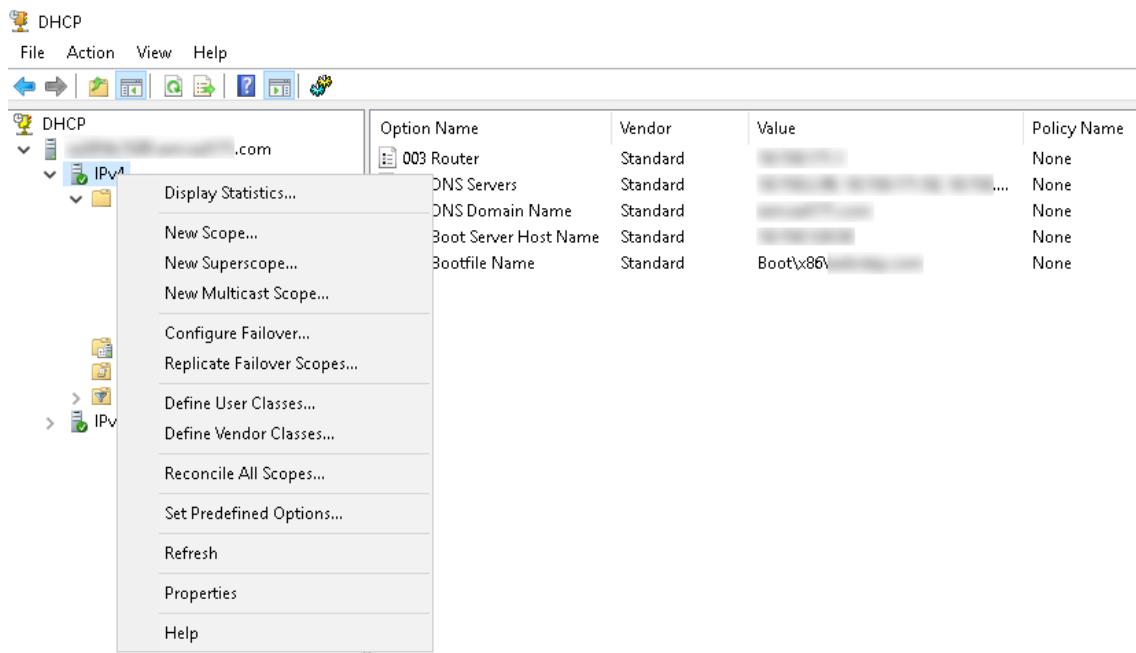


그림 18 . DHCP

4. **Set Predefined Options**을 클릭합니다.
사전 정의된 옵션 및 값
5. **Option class** 드롭다운 목록에서 **DHCP Standard Option** 값을 선택합니다.

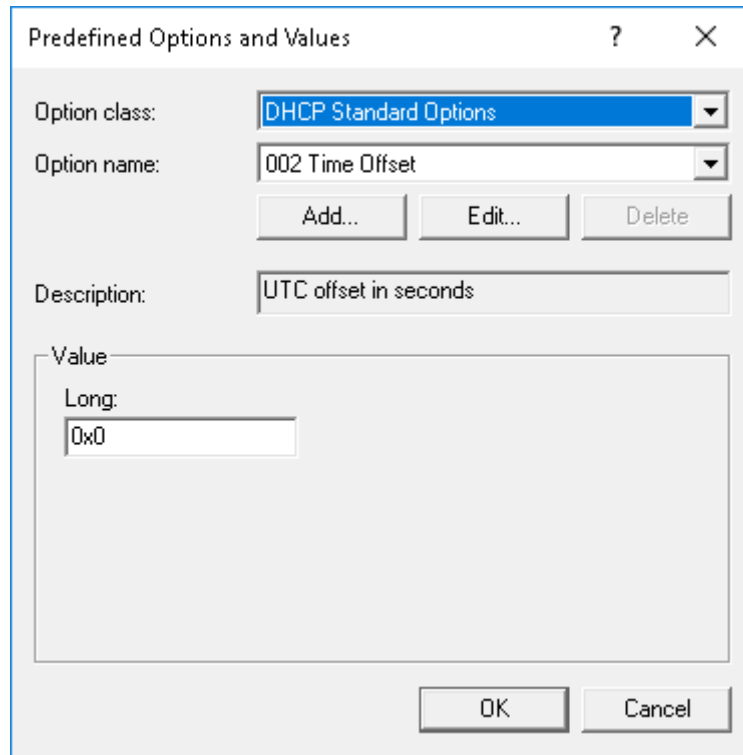


그림 19. 사전 정의된 옵션 및 값

6. **Add**를 클릭합니다.
Option Type 창이 표시됩니다.

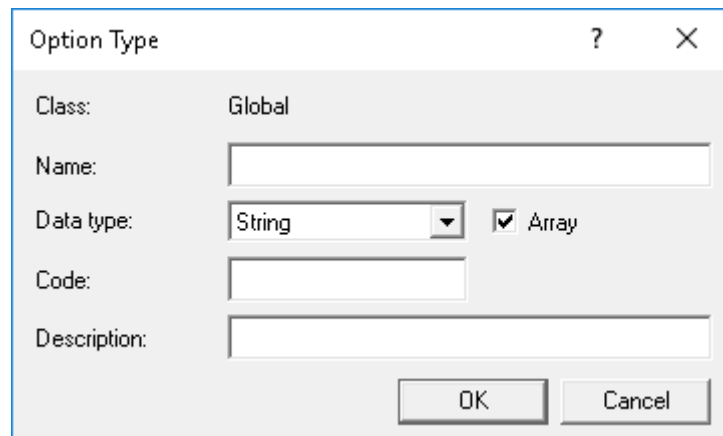


그림 20. 옵션 유형

옵션을 DHCP server 서버 옵션 또는 DHCP scope 범위 옵션에 추가해야 합니다.

DHCP 옵션 태그 구성

- 165 Wyse Management Suite 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.

- 다음 값을 입력하고 **OK**를 클릭합니다.
 - 이름 - WMS
 - 데이터 유형 - 문자열
 - 코드 - 165
 - 설명 - WMS_Server
- 다음 값을 입력한 후 **OK**를 클릭합니다.

문자열—WMS FQDN

예: WMSServerName.YourDomain.Com:443

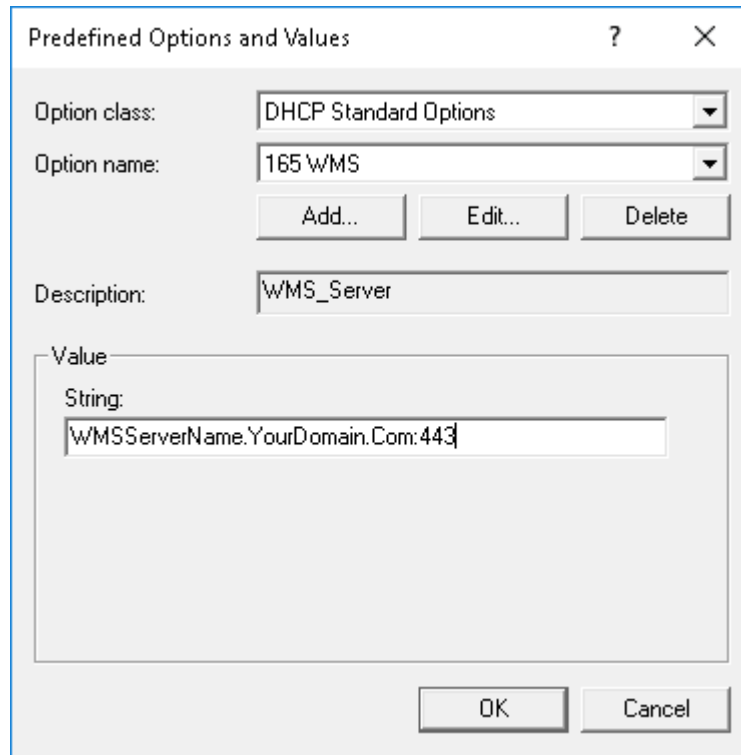


그림 21 . 165 Wyse Management Suite 서버 URL 옵션 태그

- 166 MQTT 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.

1. 다음 값을 입력하고 **OK**를 클릭합니다.

- 이름 - MQTT
- 데이터 유형 - 문자열
- 코드 - 166
- 설명 - MQTT 서버

2. 다음 값을 입력하고 **OK**를 클릭합니다.

문자열—MQTT FQDN

예: WMSServerName.YourDomain.Com:1883

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 166 MQTT Server

Add... Edit... Delete

Description: MQTT Server

Value

String: WMSServerName.YourDomain.Com:1883

OK Cancel

그림 22 . 166 Wyse Management Suite 서버 URL 옵션 태그

- 167 Wyse Management Suite CA Validation 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.

1. 다음 값을 입력하고 **OK**를 클릭합니다.

- 이름 - CA Validation
- 데이터 유형 - 문자열
- 코드 - 167
- 설명 - CA Validation

2. 다음 값을 입력하고 **OK**를 클릭합니다.

문자열—TRUE/FALSE

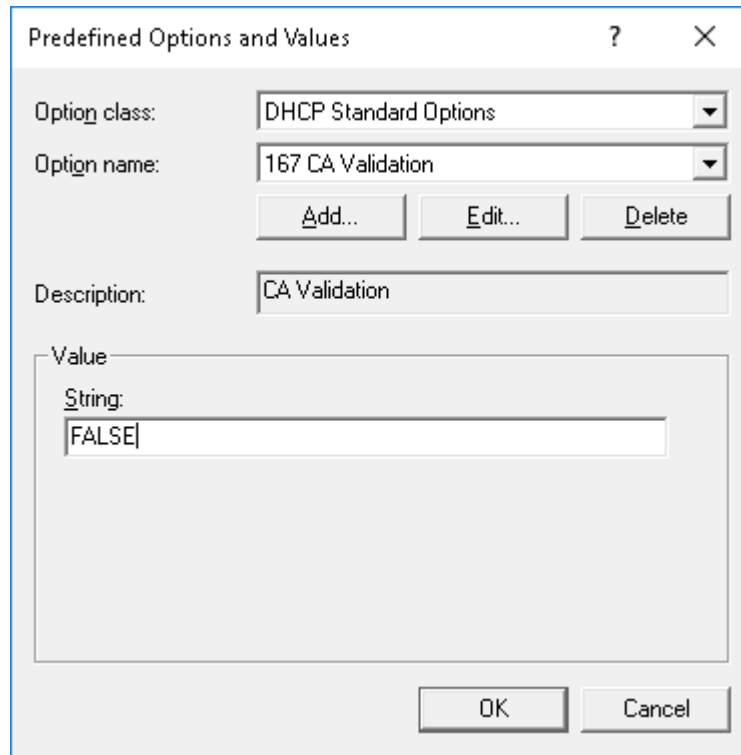


그림 23 . 167 Wyse Management Suite 서버 URL 옵션 태그

- 199 Wyse Management Suite 그룹 토큰 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.
 1. 다음 값을 입력하고 **OK**를 클릭합니다.
 - 이름 - 그룹 토큰
 - 데이터 유형 - 문자열
 - 코드 - 199
 - 설명 - 그룹 토큰
 2. 다음 값을 입력하고 **OK**를 클릭합니다.

문자열—defa-격리

Predefined Options and Values ? X

Option class: DHCP Standard Options

Option name: 199 Group token key

Add... Edit... Delete

Description: Group token key

Value

String:

defa-quarantine

OK Cancel

그림 24 . 199 Wyse Management Suite 서버 URL 옵션 태그

DNS SRV 레코드 생성 및 구성

노트: 고객 보안 환경에 대한 자세한 내용은 [Wyse Device Agent](#)를 참조하십시오.

DNS SRV 레코드를 생성하려면 다음을 수행합니다.

1. Server Manager를 엽니다.
2. **Tools**로 이동하여 **DNS option**을 클릭합니다.
3. **DNS > DNS 서버 호스트 이름 > 정방향 조회 영역 > Domain > _tcp**로 이동하고 **_tcp option**을 마우스 오른쪽 단추로 클릭.

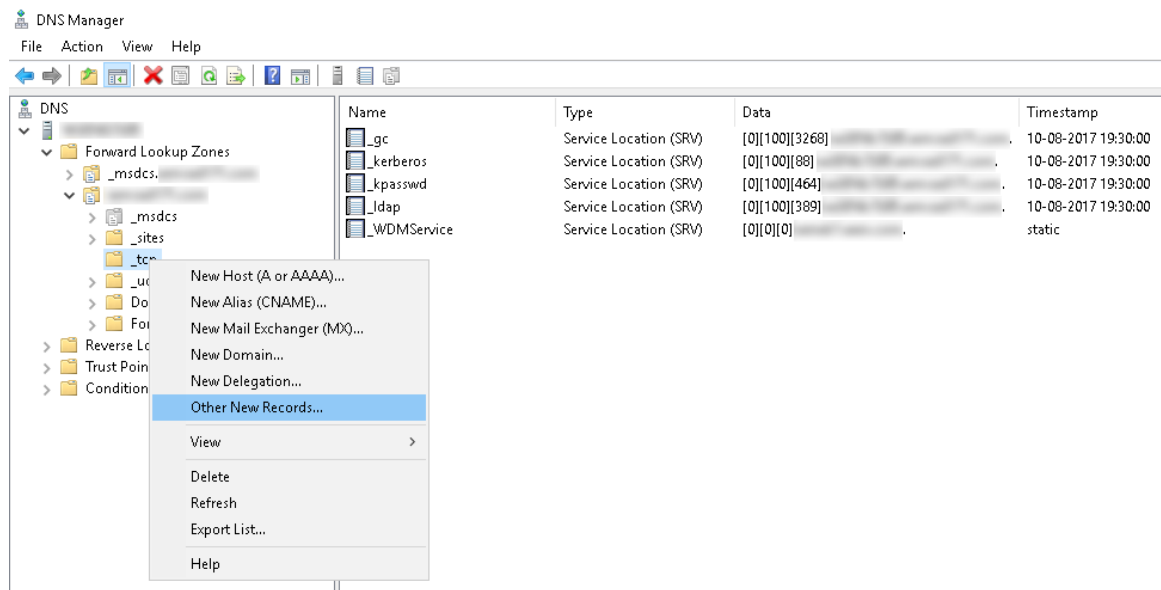


그림 25 . DNS 관리자

4. **Other New Records**를 클릭합니다.
Resource Record Type 창이 표시됩니다.
5. **Service Location(SRV)**을 선택하고 **Create Record**를 클릭한 후 다음을 수행합니다.

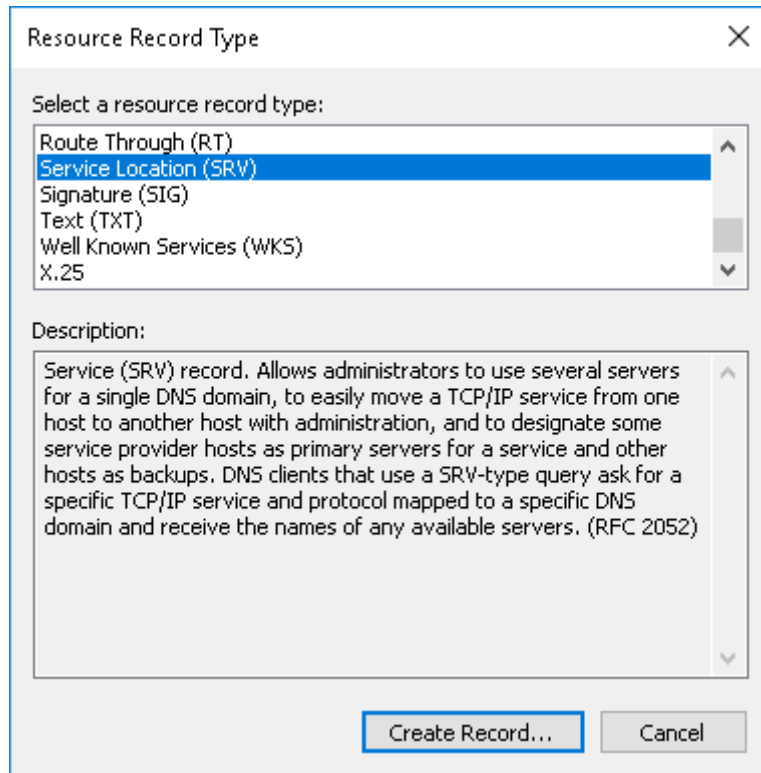


그림 26 . 리소스 기록 유형

- a) Wyse Management Suite 서버 기록을 생성하려면 다음 세부 정보를 입력하고 **OK**를 클릭합니다.
- 서비스 - _WMS_Mgmt
 - 프로토콜 - _tcp
 - 포트 번호 - 443
 - 이 서비스를 제공하는 호스트 - WMS 서버의 FQDN

New Resource Record

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

그림 27 . _WMS_MGMT 서비스

- b) MQTT 서버 기록을 생성하려면 다음 값을 입력한 다음 **OK**를 클릭합니다.
- 서비스 - _WMS_MQTT
 - 프로토콜 - _tcp
 - 포트 번호 - 1883
 - 이 서비스를 제공하는 호스트 - MQTT 서버의 FQDN

New Resource Record

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

그림 28 . _WMS_MQTT 서비스

6. **DNS > DNS Server Host Name > Forward Lookup Zones > Domain**으로 이동하고 도메인을 마우스 오른쪽 단추로 클릭합니다.
7. **Other New Records**를 클릭합니다.
8. **Text(TXT)**를 선택하고 **Create Record**를 클릭한 후 다음을 수행합니다.

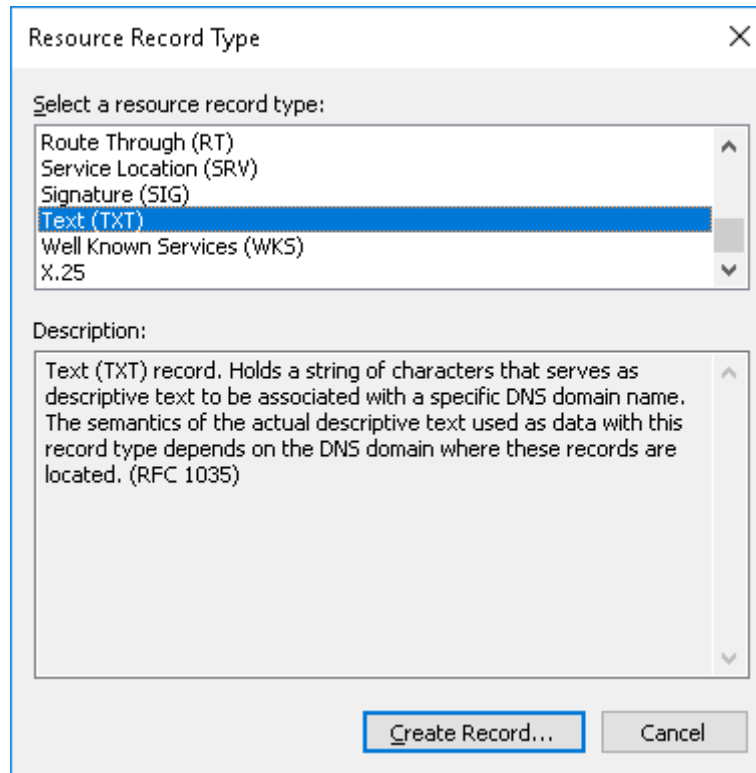


그림 29 . 리소스 기록 유형

- a) Wyse Management Suite 그룹 토큰 기록을 생성하려면 다음 값을 입력하고 **OK**를 클릭합니다.
- 기록 이름 - _WMS_GroupToken
 - 텍스트 - WMS 그룹 토큰

New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):
_WMS_GROUPTOKEN

Fully qualified domain name (FQDN):
_WMS_GROUPTOKEN.

Text:
WMS Group token

OK Cancel

그림 30 . _WMS_GROUPTOKEN 기록 이름

- b) Wyse Management Suite CA Validation 기록을 생성하려면 다음 값을 입력한 다음 **OK**를 클릭합니다.
- 기록 이름 - _WMS_CAVALIDATION
 - 텍스트 - TRUE/FALSE

New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):
_wms_cavalidation

Fully qualified domain name (FQDN):
_wms_cavalidation.

Text:
False

OK Cancel

그림 31 . _wms_cavalidation 기록 이름

고급 애플리케이션 정책 생성 및 씬 클라이언트에 배포

고급 애플리케이션 정책을 씬 클라이언트에 배포하려면 다음을 수행합니다.

1. 애플리케이션 및 사전/사후 설치 스크립트(필요한 경우)를 복사하여 로컬 리포지토리 또는 Wyse Management Suite 리포지토리의 `thinClientApps` 폴더에 있는 씬 클라이언트에 배포합니다.
 2. **Apps&Data > AppInventory**로 이동하고 **Thin Client**를 선택하여 애플리케이션이 등록되었는지 확인합니다.
 3. **App Policies**에서 **Thin Client**를 클릭합니다.
 4. **Add Advanced Policy**를 클릭합니다.
 5. 새 애플리케이션 정책을 생성하려면 다음을 수행합니다.
 - a. **Policy Name, Group, Task** 및 **Device Type**을 입력합니다.
 - b. **Add app**을 클릭하고 **TC apps**에서 하나 이상의 애플리케이션을 선택합니다. 각 애플리케이션에 대해 **Pre-Install, Post-Install** 및 **Install Parameters**에서 사전 및 사후 설치 스크립트를 선택할 수 있습니다. 애플리케이션을 설치한 후 시스템을 재부팅하려면 **Reboot**를 선택합니다.
 - c. 이 정책을 모든 하위 그룹에 적용하려면 **Include All Subgroups**를 선택합니다.
 - d. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS Subtype Filter** 또는 **Platform Filter**를 선택합니다.
 - e. 시간 초과는 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
 - f. 이 정책을 Wyse Management Suite에 등록되고 선택한 그룹에 속하거나 선택한 그룹으로 이동된 장치에 자동으로 적용하려면 **Apply Policy Automatically** 드롭다운 목록에서 **Apply the policy to new devices**를 선택합니다.
- 이 노트:** Apply the policy to devices on check in을 선택한 경우 Wyse Management Suite 서버에 체크인할 때 정책이 장치에 자동으로 적용됩니다.
- g. 정의된 값 이후에 설치 프로세스를 중지하려면 **Application Installation Timeout** 필드에 시간(분)을 지정합니다.
6. 정책 실행 시 지연을 허용하려면 **Allow delay of policy execution** 확인란을 선택합니다. 이 옵션을 선택한 경우 다음 드롭다운 메뉴가 활성화됩니다.
 - **Max Hours per Delay** 드롭다운 메뉴에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
 - **Max delays** 드롭다운 메뉴에서 정책 실행을 지연할 수 있는 횟수(1~3회)를 선택합니다.
7. 처음 장애 발생 시 애플리케이션 정책을 취소하려면 **Enable app dependency**를 선택합니다. 이 옵션을 선택하지 않으면 애플리케이션 장애가 정책 실행에 영향을 미칩니다.
8. 새 정책을 생성하려면 **Save**를 클릭합니다. 관리자가 그룹을 기준으로 이 정책을 장치에 예약할 수 있는 메시지가 표시됩니다. **Yes**를 선택하여 애플리케이션 정책을 장치에 즉시 또는 **App Policy Job** 페이지의 예약 날짜 및 시간에 예약합니다.
- 앱/이미지 정책 작업은 다음 방식으로 실행할 수 있습니다.
- a. **Immediately** - 서버가 작업을 즉시 실행합니다.
 - b. **On device time zone** - 서버가 각 장치 시간대에 대해 하나의 작업을 생성하고 장치 시간대의 선택한 날짜/시간으로 작업을 예약합니다.
 - c. **On selected time zone** - 서버가 지정된 시간대의 날짜 및 시간에 실행할 하나의 작업을 생성합니다.
9. **Preview**를 클릭하고 작업을 생성하는 다음 페이지에서 예약합니다.
 10. **Jobs** 페이지로 이동하여 작업 상태를 확인할 수 있습니다.

수동으로 Windows Embedded Standard 장치 등록

작업 표시줄에서 **WDA UI** 아이콘을 시작하여 Windows Embedded Standard 장치를 수동으로 등록할 수 있습니다.

1. **Wyse Management Suite-WMS**를 관리 서버로 선택합니다.
2. 적절한 테넌트 및 그룹 이름을 입력합니다. 이 필드를 비워두면 장치가 관리되지 않는 그룹에 등록됩니다. (선택 사항)
3. **Register**를 클릭합니다.

The image shows the 'Wyse Device Agent' application window. On the left is a sidebar with 'Registration' (highlighted), 'Support', and 'About'. The main area is titled 'Device registration' and contains the following sections:

- Select management server:** A dropdown menu currently shows 'Wyse Management Suite - WMS'. To its right, it says 'NONE is active'.
- Server settings:**
 - Management Server:** A text box with the placeholder 'Enter server url'.
 - Port:** A text box with the placeholder 'Enter Port'.
 - Tenant:** A text box with the placeholder 'Tenant'.
 - Group:** A text box with the placeholder 'Enter group'.
- A note below the Tenant and Group fields: '*If the tenant and group is empty, the device will get registered to unmanaged group'.
- Validate Server Certificate CA:** A toggle switch currently set to 'ON'.

At the bottom left, it says 'Not Registered' with a red icon. At the bottom right, there are two buttons: 'Refresh' and 'Register'.

그림 32. 장치 등록

수동으로 ThinOS 8.x 디바이스 등록

1. 썬 클라이언트의 데스크탑 메뉴에서 **시스템 설정 > 중앙 구성**으로 이동합니다.
중앙 구성 창이 표시됩니다.
2. 관리자가 원하는 그룹에 대해 구성된 대로 **그룹 등록 키**를 입력합니다.
3. **WMS 고급 설정 활성화** 확인란을 선택합니다.
4. **WMS 서버** 필드에 Wyse Management Server URL을 입력합니다.
5. 라이선스 유형에 따라 CA 유효성 검사를 활성화 또는 비활성화합니다. 퍼블릭 클라우드의 경우 **CA 유효성 검사 활성화** 확인란을 선택합니다. 프라이빗 클라우드의 경우, 잘 알려진 인증 기관의 인증서를 Wyse Management Suite 서버로 가져온 경우 **CA 유효성 검사 활성화** 확인란을 선택합니다.
프라이빗 클라우드에서 CA 유효성 검사 옵션을 활성화하려면 ThinOS 디바이스에도 동일하게 자체 서명된 인증서를 설치해야 합니다. ThinOS 디바이스에 자체 서명된 인증서를 설치하지 않은 경우 **CA 유효성 검사 활성화** 확인란을 선택하지 마십시오. 등록 후 Wyse Management Suite를 사용하여 디바이스에 인증서를 설치한 다음 CA 유효성 검사 옵션을 활성화하면 됩니다.
6. 설정을 확인하려면 **키 유효성 검사**를 클릭합니다.
① 노트: 키가 확인되지 않은 경우 입력한 그룹 키와 WMS 서버 URL을 확인합니다. 설명되어 있는 포트가 네트워크에 의해 차단되지 않았는지 확인합니다. 기본 포트는 443 및 1883입니다.
7. 확인을 클릭합니다.
① 노트: 등록 유효성 검사 옵션이 활성화되면 수동 또는 자동 검색된 디바이스가 디바이스 페이지에서 등록 유효성 검사 보류 중 상태로 있습니다. 테넌트는 디바이스 페이지에서 단일 디바이스 또는 여러 디바이스를 선택하고 등록에 대한 유효성 검사를 수행할 수 있습니다. 디바이스의 유효성 검사가 완료되면 디바이스가 해당 그룹으로 이동됩니다.

디바이스가 Wyse Management Suite에 등록됩니다.

수동으로 ThinOS 9.x 디바이스 등록

1. 쉘 클라이언트의 데스크탑 메뉴에서 **시스템 설정 > 중앙 구성**으로 이동합니다.
중앙 구성 창이 표시됩니다.
2. 관리자가 원하는 그룹에 대해 구성된 대로 **그룹 등록 키**를 입력합니다.
3. **WMS 고급 설정 활성화** 확인란을 선택합니다.
4. **WMS 서버** 필드에 Wyse Management Server URL을 입력합니다.
5. 라이선스 유형에 따라 CA 유효성 검사를 활성화 또는 비활성화합니다. 퍼블릭 클라우드의 경우 **CA 유효성 검사 활성화** 확인란을 선택하고 프라이빗 클라우드의 경우 잘 알려진 인증 기관에서 Wyse Management Suite 서버로 인증서를 가져온 경우 **CA 유효성 검사 활성화** 확인란을 선택합니다.
프라이빗 클라우드에서 CA 유효성 검사 옵션을 활성화하려면 ThinOS 디바이스에도 동일하게 자체 서명된 인증서를 설치해야 합니다. ThinOS 디바이스에 자체 서명된 인증서를 설치하지 않은 경우 **CA 유효성 검사 활성화** 확인란을 선택하지 마십시오. 등록 후 Wyse Management Suite를 사용하여 디바이스에 인증서를 설치한 다음 CA 유효성 검사 옵션을 활성화하면 됩니다.
6. 설정을 확인하려면 **키 유효성 검사**를 클릭합니다.
이 노트: 키가 확인되지 않은 경우 입력한 그룹 키와 WMS 서버 URL을 확인합니다. 설명되어 있는 포트가 네트워크에 의해 차단되지 않았는지 확인합니다. 기본 포트는 443 및 1883입니다.
경고 창이 표시됩니다.
7. **확인**을 클릭합니다.
8. **중앙 구성** 창에서 **확인**을 클릭합니다.
이 노트: 등록 유효성 검사 옵션이 활성화되면 수동 또는 자동 검색된 디바이스가 디바이스 페이지에서 등록 유효성 검사 보류 중 상태로 있습니다. 테넌트는 디바이스 페이지에서 단일 디바이스 또는 여러 디바이스를 선택하고 등록에 대한 유효성 검사를 수행할 수 있습니다. 디바이스의 유효성 검사가 완료되면 디바이스가 해당 그룹으로 이동됩니다.

디바이스가 Wyse Management Suite에 등록됩니다.

수동으로 Linux 장치 등록

System Settings에서 **WDA UI** 아이콘을 실행하여 Linux 장치를 수동으로 등록할 수 있습니다.

1. **WMS Server** 세부 정보를 입력합니다.
2. 적절한 테넌트 및 그룹 이름을 입력합니다. 이 필드를 비워두면 장치가 관리되지 않는 그룹에 등록됩니다. (선택 사항)
3. **Register**를 클릭합니다.

장치가 Wyse Management Suite 콘솔에 등록됩니다.

The screenshot shows the 'System Settings' window for 'Wyse Device Agent (WMS)'. The left sidebar has a 'Management' section with sub-items: Configuration, INI, Wyse Device Agent (highlighted), SCEP, Logs and Tools, and HAgent. The main panel displays the following configuration:

- Version: 2.0.24-00.01
- WMS Server: [Empty text field]
- Group Token: [Empty text field]
- Validate server Certificate CA: [ON] (toggle switch)
- Registration Status: [Red X icon] Not Registered

At the bottom right, there are 'Cancel' and 'Register' buttons.

그림 33. 장치 등록

용어 및 정의

다음 표에는 이 문서에 사용된 용어와 정의가 나와 있습니다.

표 5. 용어 및 정의

용어	정의
프라이빗 클라우드	조직의 데이터센터 전용 클라우드에 설치된 Wyse Management Suite 서버입니다.
WDA	장치에 상주하고 서버와 클라이언트 간의 통신을 위한 에이전트 역할을 하는 Wyse Device Agent입니다.
로컬 리포지토리	Wyse Management Suite 서버와 함께 기본적으로 설치되는 애플리케이션, 운영 체제 이미지 및 파일 리포지토리입니다.
원격 리포지토리	여러 지역에 걸친 확장성과 안정성을 위해 선택적으로 설치하여 콘텐츠를 전송할 수 있는 애플리케이션, 운영 체제 이미지 및 파일 리포지토리입니다.
퍼블릭 클라우드	인프라와 소프트웨어를 설정하고 유지 관리할 필요 없이 퍼블릭 클라우드에 편리하고 경제적으로 호스팅되는 Wyse Management Suite입니다.
애드온/앱	기본 빌드의 일부가 아니며 선택적 구성 요소로 제공되는 구성 요소 또는 패키지입니다. 관리 소프트웨어에서 구성 요소 또는 패키지를 배포할 수 있습니다. 예 - VMware 및 Citrix의 최신 연결 브로커
온-프레미스	조직의 데이터센터 전용 온-프레미스에 설치된 Wyse Management Suite 서버입니다.
테넌트	Wyse Management Suite에 대한 특정 권한으로 공통 액세스를 공유하는 사용자 그룹입니다. Management Suite에 액세스할 수 있도록 특정 고객에게 할당된 고유한 키입니다.
사용자	로컬 관리자, 전역 관리자 및 뷰어일 수 있습니다. Active Directory에서 가져온 그룹 사용자 및 사용자에게 Wyse Management Suite에 로그인할 수 있는 전역 관리자, 그룹 관리자 및 뷰어 역할을 할당할 수 있습니다. 사용자에게 할당된 역할에 따라 작업을 수행할 수 있는 권한이 부여됩니다.