Dell Wyse Management Suite
버전 3.3 관리자 가이드

2021년 7월
개정 A00

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.

목차

장 1: Wyse Management Suite 소개 9
Wyse Management Suite 에디션 9
Wyse Management Suite 기능 매트릭스 9
Wyse Management Suite 버전 3.0의 새로운 기능 13

장 2: Wyse Management Suite 시작하기 14
퍼블릭 클라우드의 Wyse Management Suite에 로그인 14
프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건 15
관리 콘솔의 기능 영역 16
씬 클라이언트 구성 및 관리 16
Wyse Device Agent 17
Dell Client Agent 17
Dell Client Agent-Enabler 18

장 3: Wyse Device Agent 설치 또는 업그레이드 19
Windows Embedded 디바이스에 수동으로 Wyse Device Agent 설치 19
Wyse Management Suite 애플리케이션 정책을 사용하여 Wyse Device Agent 업그레이드 19
ThinLinux 및 Linux 클라이언트에서 Wyse Device Agent 설치 또는 업그레이드 20

장 4: Ubuntu 디바이스에 DCA-Enabler 설치 또는 업그레이드 21
Ubuntu 디바이스에 DCA-Enabler 설치 21
Ubuntu 디바이스에서 DCA-Enabler 업그레이드 21

장 5: Wyse Management Suite를 사용하여 새 디바이스 등록 및 구성 22
Wyse Management Suite를 사용하여 새 Windows Embedded Standard 디바이스 등록 및 구성 22
Wyse Management Suite를 사용하여 새 ThinOS 8.x 디바이스 등록 및 구성 22
Wyse Management Suite를 사용하여 새 ThinOS 9.x 디바이스 등록 및 구성 23
Wyse Management Suite를 사용하여 새 Linux 또는 ThinLinux 디바이스 등록 및 구성 24
Wyse Management Suite를 사용하여 새 Wyse 소프트웨어 씬 클라이언트 등록 및 구성 24
Wyse Management Suite를 사용한 Dell Hybrid Client 등록 및 구성 25
Wyse Management Suite를 사용한 Dell Generic Client 등록 및 구성 26

장 6: Wyse Management Suite 대시보드 28
경고 보기 28
이벤트 목록 보기 29
디바이스 상태 보기 29
등록 유효성 검사 활성화 29
사용자 기본 설정 변경 29
온라인 도움말 액세스 30
암호 변경 30
관리 콘솔에서 로그아웃 30

장 7: 그룹 및 구성 관리 31
관리되지 않는 그룹 편집 32

기본 디바이스 정책 그룹 생성 32
ThinOS 선택 그룹 생성 33
기본 디바이스 정책 그룹 편집 33
ThinOS 선택 그룹 편집 33
ThinOS 선택 그룹 제거 33
사용자 정책 그룹 생성 34
사용자 정책 그룹 편집 36
전역 수준 정책 구성 36
사용자 정책 그룹 가져오기 36
그룹 제거 36
디바이스 수준 정책 구성 37
그룹 정책 내보내기 37
그룹 정책 가져오기 37
그룹 및 구성 페이지에서 그룹 정책 가져오기 37
정책 편집 페이지에서 그룹 정책 가져오기 38
ThinOS 정책 설정 편집 39
ThinOS - 마법사 모드 39
ThinOS - 고급 모드 39
ThinOS 9.x 정책 설정 편집 40
ThinOS 9.x용 BIOS 구성 41
Wyse Management Suite를 사용하여 ThinOS 9.x 이상 버전으로 업그레이드 41
BIOS 패키지 업로드 및 푸시 42
그룹 및 구성을 사용하여 ThinOS 9.x 애플리케이션 패키지 업로드 및 푸시 42
Windows Embedded Standard 정책 설정 편집 43
Windows Embedded 디바이스의 배포 설정 구성 43
Windows 10 IoT Enterprise에 대한 Edge 브라우저 설정 구성 43
Linux 정책 설정 편집 44
ThinLinux 정책 설정 편집 44
ThinLinux 디바이스의 배포 설정 구성 44
Wyse 소프트웨어 씬 클라이언트 정책 설정 편집 45
클라우드 연결 정책 설정 편집 45
Dell Hybrid Client 정책 설정 편집 45
Dell Hybrid Client에 대한 Wyse Management Suite 클라이언트 설정 구성 47
Dell Hybrid Client 디바이스의 배포 설정 구성 48
Dell Generic Client 정책 설정 편집 48
대량 디바이스 예외 파일 생성 및 가져오기 49

장 8: 디바이스 관리 53
Wyse Management Suite에 디바이스를 등록하는 방법 54
Dell Hybrid Client 수동 등록 54
수동 검색 방법을 사용하여 Dell Generic Client 등록 55
수동 검색 방법을 사용하여 Dell Hybrid Client 등록 55
Wyse Device Agent를 사용하여 ThinOS 디바이스 등록 56
Wyse Device Agent를 사용하여 Wyse Management Suite에 Windows Embedded Standard 씬 클라이언트 등록 56
Wyse Device Agent를 사용하여 Wyse Management Suite에 Wyse 소프트웨어 씬 클라이언트 등록 57
Wyse Device Agent를 사용하여 ThinLinux 씬 클라이언트 등록 57
FTP INI 메서드를 사용하여 ThinOS 디바이스 등록 57
FTP INI 메서드를 사용하여 ThinLinux 버전 2.0 디바이스 등록 58
FTP INI 메서드를 사용하여 ThinLinux 버전 1.0 디바이스 등록 58

DHCP 옵션 태그를 사용하여 디바이스 등록 ... 59
DNS SRV 레코드를 사용하여 디바이스 등록 ... 60
필터를 사용하여 디바이스 검색 ... 61
디바이스 페이지에서 필터 저장 ... 62
디바이스 상태 쿼리 ... 62
디바이스 잠금 ... 62
디바이스 재시작 ... 63
디바이스 등록 취소 ... 63
등록 유효성 검사 ... 63
디바이스 등록 유효성 검사 ... 64
디바이스를 출고 시 기본 설정으로 재설정 ... 64
디바이스 페이지에서 그룹 할당 변경 ... 64
디바이스로 메시지 전송 ... 65
Wake On LAN 명령 ... 65
디바이스 세부 정보 보기 ... 65
디스플레이 매개변수 보기 ... 65
가상 NIC 세부 정보 보기 ... 66
BIOS 세부 정보 보기 ... 66
디바이스 요약 관리 ... 67
시스템 정보 보기 ... 67
디바이스 이벤트 보기 ... 67
설치된 애플리케이션 보기 ... 67
씬 클라이언트 이름 바꾸기 ... 68
원격 섀도 연결 활성화 ... 68
Dell Hybrid Client 디바이스에 대한 원격 섀도 연결 구성 ... 69
디바이스 종료 ... 69
디바이스 태그 지정 ... 69
디바이스 규정 준수 상태 ... 69
Windows Embedded Standard 또는 ThinLinux 이미지 가져오기 ... 70
로그 파일 요청 ... 71
디바이스 문제 해결 ... 71
Dell Hybrid Client를 이미지로 다시 설치 ... 71
Dell Generic Client를 하이브리드 클라이언트로 변환 ... 72
Dell Hybrid Client용 구성 사용자 인터페이스 패키지 가져오기 ... 72
Dell Hybrid Client를 출고 시 설정으로 재설정 ... 72
디바이스의 대량 그룹 변경 ... 73

장 9: 앱 및 데이터 ... 74
애플리케이션 정책 ... 74
씬 클라이언트 애플리케이션 인벤토리 구성 ... 75
Wyse 소프트웨어 씬 클라이언트 애플리케이션 인벤토리 구성 ... 75
표준 애플리케이션 정책을 생성하여 씬 클라이언트에 배포 ... 75
표준 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포 ... 76
표준 애플리케이션 정책을 사용하여 Citrix StoreFront에 대해 SSO(Single Sign-on) 활성화 ... 77
고급 애플리케이션 정책을 생성하여 씬 클라이언트에 배포 ... 77
고급 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포 ... 79
표준 애플리케이션 정책 생성 및 Dell Hybrid Client에 배포 ... 80
고급 애플리케이션 정책 생성 및 Dell Hybrid Client에 배포 ... 81
표준 애플리케이션 정책 생성 및 Dell Generic Client에 배포 ... 82
고급 애플리케이션 정책 생성 및 Dell Generic Client에 배포 ... 83

이미지 정책 84
리포지토리에 Windows Embedded Standard 운영 체제 및 ThinLinux 이미지 추가 84
리포지토리에 ThinOS 펌웨어 추가 85
ThinOS BIOS 파일을 리포지토리에 추가 85
ThinOS 패키지 파일을 리포지토리에 추가 85
Windows Embedded Standard 및 ThinLinux 이미지 정책 생성 85
리포지토리에 ThinOS 9.x 펌웨어 추가 86
ThinOS 9.x BIOS 파일을 리포지토리에 추가 86
리포지토리에 ThinOS 애플리케이션 패키지 추가 87
Dell Hybrid Client 이미지 정책 생성 87
파일 리포지토리 관리 88

장 10: 규칙 관리 90
등록 규칙 편집 90
관리되지 않는 디바이스에 대한 자동 할당 규칙 생성 91
관리되지 않는 디바이스 자동 할당 규칙 편집 91
관리되지 않는 디바이스 자동 할당에 대한 규칙 비활성화 및 삭제 91
규칙 순서 저장 91
경고 알림에 대한 규칙 추가 92
경고 알림 규칙 편집 92
디바이스 자동 등록 취소를 위한 규칙 생성 92

장 11: 작업 관리 94
BIOS 관리자 암호 동기화 95
필터를 사용하여 예약된 작업 검색 95
디바이스 명령 작업 예약 96
이미지 정책 예약 96
애플리케이션 정책 예약 97
실패한 작업 재시작 97

장 12: 이벤트 관리 98
필터를 사용하여 이벤트 또는 경고 검색 98
이벤트 요약 보기 99
감사 로그 보기 99
최종 사용자 세션 보고 99

장 13: 사용자 관리 100
새 관리자 프로필 추가 101
Wyse Management Suite에서 WMS 맞춤 구성 역할 생성 101
가져온 AD 그룹에 WMS 맞춤 구성 역할 할당 102
할당되지 않은 관리자 또는 클라우드 연결 사용자 대량 가져오기 103
관리자 프로필 편집 103
관리자 프로필 활성화 104
관리자 프로필 비활성화 104
관리자 프로필 삭제 104
관리자 프로필 잠금 해제 105
관리자 프로필 비활성화 105
관리되지 않는 디바이스에 대한 자동 할당 규칙 생성 105
최종 사용자 추가 105

최종 사용자 편집 105
최종 사용자 정책 구성 106
최종 사용자 대량 가져오기 106
최종 사용자 삭제 106
사용자 프로파일 편집 106

장 14: 포털 관리 108
Active Directory를 통해 할당되지 않은 사용자 또는 사용자 그룹을 퍼블릭 클라우드로 가져오기 109
Active Directory 서버 정보 추가 109
퍼블릭 클라우드에서 Active Directory 페더레이션 서비스 기능 구성 110
경고 분류 111
API(Application Programming Interface) 계정 생성 111
Wyse Management Suite 파일 리포지토리 액세스 111
서브넷 매핑 112
기타 설정 구성 113
Wyse Management Suite API 활성화 114
Teradici 구성 관리 114
2단계 인증 활성화 114
다중 테넌트 계정 활성화 115
보고서 생성 115
맞춤형 브랜딩 활성화 115
시스템 설정 관리 116
보안 MQTT 구성 116
중요 정보 116
SSL을 통한 보안 LDAP 활성화 117

장 15: Dell Wyse 5070 디바이스 및 Dell Ubuntu Generic Client를 Dell Hybrid Client로 변환 119
Dell Wyse 5070 변환 119
리포지토리에 Dell Hybrid Client 이미지 추가 120
하이브리드 클라이언트 이미지 정책 생성 120
이미지 정책 예약 121
Dell Generic Client를 Dell Hybrid Client로 변환 121

장 16: 보안 구성 123
Wyse Management Suite 설치 프로그램에서 TLS 버전 구성 지원 123
퍼블릭 클라우드에서 Active Directory Federation Services 기능 구성 123
보안 LDAP 또는 LDAPS 설정 구성 124
더 이상 사용되지 않는 프로토콜 125

장 17: Teradici 디바이스 관리 126
Teradici 디바이스 검색 126
CIFS 사용 사례 시나리오 128

장 18: 라이선스 구독 관리 130
Wyse Management Suite 퍼블릭 클라우드에서 라이선스 가져오기 130
Wyse Management Suite 프라이빗 클라우드로 라이선스 내보내기 130
씬 클라이언트 라이선스 할당 131
라이선스 주문 131
라이선스 만료 이메일 알림 구성 131

장 19: Firmware upgrade 133
ThinLinux 1.x를 2.1 이상 버전으로 업그레이드 133
ThinLinux 2.x 이미지 준비 133
ThinLinux 1.x를 2.x로 업그레이드 134
ThinOS 8.x를 9.0으로 업그레이드 134
리포지토리에 ThinOS 9.x 펌웨어 추가 135
ThinLinux 8.6을 ThinOS 9.x로 업그레이드 135
Wyse Management Suite를 사용하여 ThinOS 9.x 이상 버전으로 업그레이드 136

장 20: 원격 리포지토리 137
Wyse Management Suite 리포지토리 서비스 관리 142
Wyse Management Suite 원격 리포지토리에 대한 프록시 지원 142

장 21: Windows Embedded Standard WDA 및 Dell Hybrid Client DCA에 대한 프록시 지원 144
Windows Embedded Standard WDA용 WININET 프록시를 사용하여 프록시 서버 정보 구성 144
Windows Embedded Standard WDA 및 Dell Hybrid Client DCA용 DHCP 옵션 태그를 사용하여 프록시 서버 정보 구성 144

장 22: 디바이스 문제 해결 146
Wyse Management Suite를 사용하여 로그 파일 요청 146
Wyse Management Suite를 사용하여 감사 로그 보기 146
WinHTTP 프록시가 구성되어 있을 때 디바이스가 Wyse Management Suite에 등록하지 못함 147
RemoteFX USB 리디렉션 정책은 USB 대용량 스토리지 디바이스에 적용되지 않음 147
Wyse Management Suite에서 구성된 WiFi 설정은 여러 Wyse 5070 씬 클라이언트에서 지속적이지 않음 147

장 23: FAQ(자주하는 질문) 149
설정이 충돌하는 경우 Wyse Management Suite와 ThinOS UI 간의 우선 순위는 어떻게 됩니까? 149
Wyse Management Suite 파일 리포지토리 사용 방법 149
.csv 파일에서 사용자를 가져오는 방법 150
Wyse Management Suite의 버전 확인 방법 150
DHCP 옵션 태그 생성 및 구성 방법 150
DNS SRV 레코드 생성 및 구성 방법 151
호스트 이름을 IP 주소로 변경하는 방법 152
자체 서명된 원격 리포지토리를 사용하여 디바이스를 이미지로 설치하는 방법 152

1

Wyse Management Suite 소개

Wyse Management Suite는 Dell Hybrid Client 기반 엔드포인트 및 Dell 씬 클라이언트를 중앙에서 구성하고 모니터링하며 관리하고 최적화할 수 있는 차세대 관리 솔루션입니다. 클라우드 및 온프레미스 배포, 모바일 애플리케이션을 사용하여 어디서나 관리, BIOS 구성 및 포트 잠금과 같은 향상된 보안과 같은 고급 기능 옵션 또한 제공합니다. 다른 기능으로는 디바이스 검색 및 등록, 자산 및 인벤토리 관리, 구성 관리, 운영 체제 및 애플리케이션 배포, 실시간 명령, 모니터링, 알림, 보고 및 엔드포인트 문제 해결이 있습니다.

주제:

- Wyse Management Suite 에디션
- Wyse Management Suite 기능 매트릭스
- Wyse Management Suite 버전 3.0의 새로운 기능

Wyse Management Suite 에디션

Wyse Management Suite는 다음 버전에서 사용할 수 있습니다.

- **Standard(무료)** - Wyse Management Suite의 Standard 버전은 기본 기능을 제공하고 프라이빗 클라우드 배포에만 사용할 수 있습니다. Standard 버전 사용에는 라이선스 키가 필요하지 않습니다. 이 버전은 Dell 씬 클라이언트만 관리할 수 있습니다. Standard 버전은 중소기업에 적합합니다.
- **Pro(유료)** - Wyse Management Suite의 Pro 버전은 더욱 강력한 솔루션입니다. 퍼블릭 및 프라이빗 클라우드 배포에 모두 사용할 수 있습니다. Pro 버전(구독 기반 라이선싱)을 사용하려면 라이선스 키가 필요합니다. 조직은 Pro 솔루션을 통해 하이브리드 모델을 도입하고, 필요한 경우 프라이빗 클라우드와 퍼블릭 클라우드 사이에 라이선스를 배치할 수 있습니다. 이 버전은 Teradici 기반 디바이스, PC 기반 씬 클라이언트용 Wyse Covert, Dell Hybrid Client 디바이스, 내장형 PC 및 Edge Gateway 디바이스를 관리하는 데 필요합니다. 또한 Dell 씬 클라이언트를 관리하는 고급 기능도 제공합니다. 퍼블릭 클라우드를 배포하는 경우, 홈 오피스, 타사, 파트너, 모바일 씬 클라이언트 등 비기업 네트워크에서 Pro 버전을 관리할 수 있습니다.

  노트: 클라우드와 온프레미스 설치 간에 라이선스를 쉽게 배치할 수 있습니다.

  또한 Wyse Management Suite의 Pro 버전은 다음 기능을 제공합니다.
  - 중요 경고, 알림을 확인하고 실시간으로 명령을 보낼 수 있는 모바일 애플리케이션
  - 역할 기반 관리를 위한 2단계 인증 및 Active Directory 인증을 통해 강화된 보안
  - 고급 앱 정책 및 보고

  노트: 클라우드 서비스는 미국 및 독일에서 호스팅됩니다. 데이터 상주 제한이 있는 국가의 고객은 클라우드 기반 서비스를 활용하지 못할 수 있습니다.

Wyse Management Suite 웹 콘솔은 국제화를 지원합니다. 페이지의 오른쪽 하단에 있는 드롭다운 메뉴의 다음 언어 중에서 선택합니다.

- 영어
- 프랑스어
- 이탈리아어
- 독일어
- 스페인어
- 중국어
- 일본어

Wyse Management Suite 기능 매트릭스

다음 표에는 각 구독 유형에 대한 지원 기능 정보가 나와 있습니다.

표 1. 각 구독 유형에 대한 기능 매트릭스

기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro - Cloud Edition
씬 클라이언트 관리를 위한 고확장성 솔루션	최대 1만 개의 디바이스 무료	최대 12만 개의 디바이스	최대 1백만 개의 디바이스
라이선스 약관	무료 다운로드	시트당 구독	시트당 구독
라이선스 키	필요 없음	필수	필수
아키텍처	프라이빗 클라우드	프라이빗 클라우드	퍼블릭 클라우드
유연한 배포 또는 하이브리드 클라우드	X	√	√
고급 설치 프로그램	X	√	√
멀티 테넌시	X	√	√
권한 세분화를 위한 위임된 관리	X	√	√
분산 아키텍처를 지원하는 다중 리포지토리	X	√	√
Wyse Management Suite 서버 별칭 구성 옵션	X	√	√
고가용성 참조 아키텍처	X	√	X
프록시 지원 - SOCKS5 및 HTTPS	√	√	√
API 지원	X	√	X
Dell ProSupport for Software 포함	X	√	√
Dell 엔드포인트			
Dell Hybrid Client 지원 OptiPlex 7070 Ultra	X	√	√
Dell Hybrid Client 지원 OptiPlex 3090 Ultra 및 7090 Ultra	X	√	√
Dell Hybrid Client 지원 Latitude 3320	X	√	√
Dell Hybrid Client 지원 Wyse 5070	X	√	√
ThinOS 지원 Wyse 씬 클라이언트	√	√	√
ThinLinux 지원 Wyse 씬 클라이언트	√	√	√
Windows 10 IoT Enterprise 지원 Wyse 씬 클라이언트	√	√	√
Wyse PCoIP Zero Clients(Teradici 펌웨어)	X	√	√
PC용 Wyse Converter 지원 소프트웨어 씬 클라이언트	X	√	√
보고 및 모니터링			
지역화된 관리 콘솔	X	√	√
이메일 및 모바일 애플리케이션을 사용한 알림, 이벤트 및 감사 로그	X	√	√
엔터프라이즈급 보고	X	√	√

다음 표에는 각 구독 유형에 지원되는 Dell Hybrid Client 관리 기능 정보가 나와 있습니다.

표 2. Dell Hybrid Client 관리 기능 매트릭스

Dell Hybrid Client 관리 기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro - Cloud Edition
완벽한 자산 가시성			
자동 디바이스 검색	X	√	√
자산, 인벤토리 및 시스템 관리	X	√	√
상속 후 디바이스 Wyse Management Suite 수준에서 유효 구성 보기	X	√	√
보안			
보안 통신(HTTPS)	X	√	√
보안 MQTT	X	√	√
다단계 인증	X	√	√
역할 기반 관리를 위한 Active Directory 인증	X	√	√
LDAPS를 사용한 AD 매핑	X	√	√
SSO(Single Sign On)	X	√	√
잠금 설정(지원되는 엔드포인트의 포트 활성화/비활성화)	X	√	√
포괄적인 관리			
운영 체제 패치 및 이미지 관리	X	√	√
스마트 예약	X	√	√
자동 배포	X	√	√
배포를 단순화하고 재부팅을 최소화하는 번들 애플리케이션	X	√	√
디바이스 특성을 기준으로 동적 그룹 생성 및 할당	X	√	√
애플리케이션 정책에 리포지토리 할당 및 서브넷 매핑	X	√	√
고급 앱 관리 및 앱 정책	X	√	√
사용자 그룹 상속	X	√	√
최종 사용자 예외	X	√	√
디바이스의 자동 등록 취소	X	√	√
구성			
Dell Hybrid Client 마법사 구성	X	√	√
다중 모니터 지원	X	√	√
팔로우미 프로필	X	√	√

표 2. Dell Hybrid Client 관리 기능 매트릭스 (계속)

Dell Hybrid Client 관리 기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro - Cloud Edition
파일 관계를 통해 애플리케이션 전송 모드의 우선 순위 지정	X	√	√
BIOS 설정 및 구성 지원	X	√	√
정책 구성 내보내기 및 가져오기	X	√	√
기본 사용자 그룹 정책	X	√	√
브라우저 구성	X	√	√
클라우드 공급업체 구성	X	√	√
Dell 서명 애플리케이션 자동 업데이트	X	√	√
사용자 개인화 데이터 로밍	X	√	√
VNC 구성	X	√	√
SSH 구성	X	√	√

다음 표는 각 구독에 대해 지원되는 Wyse 씬 클라이언트 및 제로 클라이언트 관리 기능에 대한 정보를 제공합니다.

표 3. Wyse 씬 클라이언트 및 제로 클라이언트 관리 기능 매트릭스

Wyse 씬 클라이언트 및 제로 클라이언트 관리 기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro - Cloud Edition
완벽한 자산 가시성			
자동 디바이스 검색	√	√	√
자산, 인벤토리 및 시스템 관리	√	√	√
상속 후 디바이스 수준에서 유효 구성 보기	√	√	√
보고 및 모니터링			
VNC를 사용한 원격 섀도	√	√	
구성 가능한 하트비트 및 체크인 간격	√	√	√
보안			
보안 통신(HTTPS)	√	√	√
802.1x 인증서 배포	√	√	√
보안 MQTT	√	√	√
2단계 인증	X	√	√
역할 기반 관리를 위한 Active Directory 인증	X	√	√
도메인 가입 기능(Windows 10 IoT Enterprise)	X	√	√
LDAPS를 사용한 AD 매핑	X	√	√

표 3. Wyse 씬 클라이언트 및 제로 클라이언트 관리 기능 매트릭스 (계속)

Wyse 씬 클라이언트 및 제로 클라이언트 관리 기능	Wyse Management Suite Standard	Wyse Management Suite Pro - 프라이빗 클라우드	Wyse Management Suite Pro - Cloud Edition
잠금 설정(지원되는 엔드포인트의 포트 활성화 또는 비활성화)	X	√	√
포괄적인 관리			
운영 체제 패치 및 이미지 관리	√	√	√ **
스마트 예약	√	√	√
자동 배포	√	√	√
배포를 단순화하고 재부팅을 최소화하는 번들 애플리케이션	X	√	√
디바이스 특성을 기준으로 동적 그룹 생성 및 할당	X	√	√
애플리케이션 정책에 리포지토리 할당 및 서브넷 매핑	X	√	√
디바이스의 자동 등록 취소	√	√	√
고급 앱 정책	X	√	√
구성			
Wyse ThinOS 8.x 및 9.x 마법사 구성	√	√	√
다중 모니터 지원	√	√	√
Wyse Easy Setup 및 Wyse Overlay Optimizer	√	√	√
맞춤형 애플리케이션 설치를 위한 스크립팅 지원	X	√	√
BIOS 설정 및 구성 지원	X	√	√
정책 구성 내보내기/가져오기	X	√	√
RSP 패키지 지원	X	√	√
WDM 가져오기 툴	X	√	X
대량 디바이스 예외	X	√	√

노트: **이중 별표는 ThinLinux 및 Windows 10 IoT Enterprise 운영 체제의 경우 Wyse Management Suite 퍼블릭 클라우드 환경을 사용할 때 온프레미스 리포지토리가 필요하다는 것을 나타냅니다.

Wyse Management Suite 버전 3.0의 새로운 기능

- Dell Hybrid Client 패키지용 Wyse Management Suite 퍼블릭 클라우드 리포지토리를 지원합니다.
- Windows 10 IoT Enterprise 디바이스 설정인 Chromium에 기반한 Edge 브라우저 구성을 지원합니다.
- 라이선스 만료 전 테넌트 이메일 알림 구성을 지원합니다.

2

Wyse Management Suite 시작하기

이 섹션에서는 관리자로 시작하고 Wyse Management Suite를 사용하여 씬 클라이언트를 관리하는 일반적인 기능에 대해 설명합니다.

주제:

- 퍼블릭 클라우드의 Wyse Management Suite에 로그인
- 프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건
- 관리 콘솔의 기능 영역
- 씬 클라이언트 구성 및 관리
- Wyse Device Agent
- Dell Client Agent
- Dell Client Agent-Enabler

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. **로그인**을 클릭합니다.

   Wyse Management Suite 콘솔에 처음으로 로그인하거나 새 사용자를 추가하거나, 사용자 라이선스를 갱신하는 경우 **이용 약관** 페이지가 표시됩니다. 이용 약관을 읽고 해당 확인란을 선택한 다음 **동의**를 클릭합니다.

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.

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 다음을 수행합니다.

1. 관리 콘솔 오른쪽 상단에 있는 계정 링크를 클릭합니다.
2. **암호 변경**을 클릭합니다.

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

로그아웃

관리 콘솔에서 로그아웃하려면 다음을 수행합니다.

1. 관리 콘솔 오른쪽 상단에 있는 계정 링크를 클릭합니다.
2. **로그아웃**을 클릭합니다.

프라이빗 클라우드에서 Wyse Management Suite를 배포하기 위한 필수 조건

표 4. 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 Standard Wyse Management Suite 웹 서버에는 Apache Tomcat 웹 서버가 내장되어 있습니다. Microsoft IIS, Apache Tomcat 웹 서버를 별도로 설치하지 않도록 합니다. 지원되는 언어 팩 - 영어, 프랑스어, 이탈리아어, 독일어, 스페인어, 일본어, 중국어			
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 • TLS 443 - 보안 MQTT 통신 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.

노트: `WMS.exe` `WMS_Repo.exe`를 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 머신에 소프트웨어를 설치할 수 있습니다. 또한 소프트웨어 리포지토리와 Wyse Management Suite 서버의 운영 체제가 같을 필요는 없습니다.

노트: 10,000개의 디바이스를 설치하는 경우 보안 MQTT 통신을 위해서는 최소 메모리(RAM)가 12GB여야 합니다.

노트: Wyse Management Suite 3.3에서는 분산 설치에 MongoDB 버전 4.2.12를 사용해야 합니다. 다른 버전의 외부 MongoDB 서버를 사용하여 Wyse Management Suite 3.3을 설치하거나 업그레이드할 수 없습니다.

노트: Azure, Amazon Web Services 및 Google Cloud Platform과 같은 클라우드 호스팅 서버에서는 Wyse Management Suite 서버 및 리포지토리 설치가 지원되지 않습니다.

관리 콘솔의 기능 영역

Wyse Management Suite 콘솔은 다음과 같은 기능 영역으로 구성됩니다.

- **대시보드** 페이지에서는 시스템의 각 기능 영역에 대한 현재 상태 관련 정보를 제공합니다.
- **그룹 및 구성** 페이지에서는 디바이스 구성에 대한 계층 구조의 그룹 정책 관리를 수행합니다. 선택적으로 기업 표준에 따라 전역 그룹 정책의 하위 그룹을 생성하여 디바이스를 분류할 수 있습니다. 예를 들어 작업 기능, 디바이스 유형 등에 따라 디바이스를 그룹화할 수 있습니다.
- **사용자** 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. 또한 최종 사용자 관리를 위해 **최종 사용자** 탭이 추가됩니다.
- **디바이스** 페이지에서는 디바이스, 디바이스 유형 및 디바이스별 구성을 보고 관리할 수 있습니다.
- **앱 및 데이터** 페이지에서 디바이스 애플리케이션, 애플리케이션 인벤토리 및 파일 리포지토리를 관리할 수 있습니다.
- **규칙** 페이지에서는 자동 그룹화, 경고 알림과 같은 규칙을 추가, 편집, 활성화 또는 비활성화할 수 있습니다.
- **작업** 페이지에서는 재부팅, Wake On LAN, 등록된 디바이스에 애플리케이션 또는 이미지 정책 배포와 같은 작업을 생성할 수 있습니다.
- **이벤트** 페이지에서는 시스템 이벤트 및 알림을 보고 감사할 수 있습니다.
- **포털 관리** 페이지에서는 로컬 리포지토리 구성, Dell Hybrid Client 라이선스 구독, Active Directory 구성 및 2단계 인증 등 다양한 시스템 설정을 구성할 수 있습니다.

씬 클라이언트 구성 및 관리

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

  노트: Pro Edition에서 규칙을 추가하여 그룹을 생성할 수 있습니다. 또한 서브넷, 시간대, 위치와 같은 디바이스 특성에 따라 디바이스를 기존 그룹에 할당할 수 있습니다.

  다음도 구성할 수 있습니다.

  - 기본 정책 그룹에 설정된 테넌트 계정의 모든 디바이스에 적용되는 설정을 구성할 수 있습니다. 이러한 설정은 모든 그룹 및 하위 그룹이 상속하는 전역 매개변수 세트입니다. 하위 수준 그룹에 구성된 설정은 상위 또는 상위 수준 그룹에 구성된 설정보다 우선합니다.

    예를 들면, 다음과 같습니다.
    - 기본 정책 그룹(상위 그룹)에 대한 정책을 구성합니다. 정책을 구성한 후 맞춤형 그룹(하위 그룹) 정책을 확인합니다. 하위 그룹에도 동일한 정책 세트가 적용됩니다. 기본 정책 그룹 설정의 구성은 모든 그룹 및 하위 그룹이 상위 그룹에서 상속하는 전체 매개변수 세트입니다.
    - 맞춤형 그룹에 대해 다른 설정을 구성합니다. 맞춤형 그룹은 페이로드를 모두 수신하지만 기본 정책 그룹의 디바이스는 맞춤형 정책 그룹에 구성된 페이로드를 수신하지 않습니다.
    - 맞춤형 그룹에 대해 다른 설정을 구성합니다. 하위 수준 그룹에 구성된 설정은 상위 또는 상위 수준 그룹에 구성된 설정보다 우선합니다.

  - **디바이스 세부 정보** 페이지에서 구성할 수 있는 특정 디바이스에 고유한 설정을 구성할 수 있습니다. 하위 수준 그룹과 같은 이러한 설정은 상위 수준 그룹에 구성된 설정보다 우선합니다.

  정책을 생성하고 게시하면 구성 매개변수가 하위 그룹을 포함한 해당 그룹의 모든 디바이스에 배포됩니다.

  정책을 게시하고 디바이스로 전파한 후에는 변경할 때까지 설정이 디바이스로 다시 전송되지 않습니다. 등록된 새 디바이스는 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 변경(예: 디스플레이 설정) 시 재부팅이 실행될 수 있습니다.

- **애플리케이션 및 운영 체제 이미지 배포** - 애플리케이션 및 운영 체제 이미지 업데이트는 **앱 및 데이터** 탭에서 배포할 수 있습니다. 애플리케이션은 정책 그룹을 기준으로 배포됩니다.

  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. 애플리케이션을 설치하는 동안 디바이스가 재시작됩니다. 각 애플리케이션 설치 전과 설치 후에 디바이스를 재부팅합니다. 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.

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

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

- **디바이스의 인벤토리** - 이 옵션은 **디바이스** 탭을 클릭하여 찾을 수 있습니다. 기본적으로 이 옵션은 시스템에 있는 모든 디바이스를 페이지가 매겨진 목록으로 표시합니다. 그룹 또는 하위 그룹, 디바이스 유형, 운영 체제 유형, 상태, 서브넷, 플랫폼, 시간대 등 다양한 필터 조건을 사용하여 디바이스의 하위 집합을 표시하도록 선택할 수 있습니다.

  해당 디바이스의 **디바이스 세부 정보** 페이지로 이동하려면 이 페이지에 나열된 디바이스 항목을 클릭합니다. 디바이스의 모든 세부 정보가 표시됩니다.

  디바이스 세부 정보 페이지에는 해당 디바이스에 적용할 수 있는 모든 구성 매개변수와 각 매개변수가 적용되는 그룹 수준도 표시됩니다.

  또한 이 페이지에서 **디바이스 예외** 버튼을 활성화하여 해당 디바이스에 고유한 구성 매개변수를 설정할 수 있습니다. 이 섹션에서 구성된 매개변수는 그룹 및/또는 전역 수준에서 구성된 모든 매개변수를 재정의합니다.

- **보고서** - 보고서를 생성하고 사전 정의된 필터를 기준으로 보고서를 볼 수 있습니다. 보고서를 생성하려면 **포털 관리** 페이지에서 **보고서** 탭을 클릭합니다.

- **모바일 애플리케이션** - Android 디바이스에서 사용할 수 있는 모바일 애플리케이션인 **Dell Mobile Agent**를 사용하여 경고 알림을 수신하고 디바이스를 관리할 수 있습니다. 모바일 애플리케이션 및 **Dell Mobile Agent 시작 가이드**를 다운로드하려면 **포털 관리자** 페이지에서 **알림 및 분류** 탭을 클릭합니다.

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.

- **보안 수준이 높은 환경** - DHCP 또는 DNS 서버가 새 디바이스 검색에 실패하는 위험을 줄이기 위해 관리자가 각 디바이스에 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 디바이스에서 인증서를 수동으로 구성해야 합니다. 또한 인증서를 `Agent Configuration` 폴더에 복사하여 인증서를 보존하고, 디바이스 이미지를 재작성한 후에도 DHCP 또는 DNS 서버가 검색에 실패하는 위험을 줄여야 합니다.

  `Agent Configuration` 폴더는 다음 위치에 있습니다.
  - Windows Embedded Standard 디바이스-`%SYSTEMDRIVE%\\Wyse\\WCM\\ConfigMgmt\\Certificates`
  - ThinLinux 디바이스-`/etc/addons.d/WDA/certs`
  - ThinOS 디바이스-`wnos/cacerts/`

  노트: USB 드라이브 또는 FTP 경로를 사용하여 인증서를 ThinOS 운영 체제를 실행하는 씬 클라이언트로 가져와야 합니다.
- **안전한 환경** - DHCP 또는 DNS 서버가 새 디바이스 검색에 실패하는 위험을 줄이기 위해 관리자가 CA 서명 인증서를 사용하여 Wyse Management Suite 서버를 구성해야 합니다. 디바이스는 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 디바이스에 인증서가 없는 경우 처음 등록 후 인증서를 디바이스로 푸시해야 합니다. 이 인증서는 DHCP 또는 DNS 서버가 검색에 실패하는 위험을 줄이기 위해 디바이스 이미지를 재작성하거나 디바이스를 재시작한 후에도 보존됩니다.
- **일반 환경** - 디바이스가 CA 서명 또는 자체 서명 인증서로 구성된 Wyse Management Suite 프라이빗 클라우드에 대해 DHCP/DNS 레코드에서 Wyse Management Suite 서버 URL을 가져옵니다. 디바이스에서 CA Validation 옵션이 비활성화되어 있는 경우 디바이스를 처음 등록하면 Wyse Management Suite 관리자가 알림을 받습니다. 이 시나리오에서 Dell은 관리자가 서버가 자체 서명 인증서로 구성된 디바이스로 인증서 푸시를 수행할 것을 권장합니다. 이 환경은 퍼블릭 클라우드에 사용할 수 없습니다.

Dell Client Agent

DCA(Dell Client Agent)는 Dell Hybrid Client 관리 솔루션을 위한 통합 에이전트입니다. DCA를 설치하면 Wyse Management Suite를 사용하여 Dell Hybrid Client를 관리할 수 있습니다.

OptiPlex 7070 Ultra 디바이스에 Dell Hybrid Client를 설치하려면 다음을 수행합니다.

1. 검색 방법(DNS 또는 DHCP) 또는 **reg.json** 수동 방법을 사용하여 Wyse Management Suite에 디바이스를 등록합니다. Wyse Management Suite에 디바이스를 등록하는 방법을 참조하십시오.
2. OptiPlex 7070 Ultra 디바이스를 이미지로 다시 설치합니다. Dell Hybrid Client 이미지로 다시 설치를 참조하십시오.

Dell Client Agent-Enabler

DCA-Enabler(Dell Client Agent-Enabler)는 Dell Ubuntu 디바이스에서 Ubuntu 버전 18.04 및 20.04 LTS 64비트를 관리하기 위한 클라이언트 에이전트입니다. Dell Hybrid Client 소프트웨어에는 DCA-Enabler(Dell Client Agent-Enabler)가 사전 로드되어 있습니다. DCA-Enabler는 Wyse Management Suite에서 관리하는 다음 작업을 수행하도록 지원합니다.

- Ubuntu 디바이스 등록
- Query, Restart, Shutdown, Wake On LAN 등의 실시간 명령 배포
- Device Pull Log 명령
- 서버에서 등록 취소
- 작업, 디바이스 또는 디바이스 세부 정보 페이지를 사용한 Convert to Hybrid Client 명령
- 표준 애플리케이션 정책 배포
- 고급 애플리케이션 정책 배포
- 일반 클라이언트를 Dell Hybrid Client로 변환 정책 배포
- 인증서 정책 배포

DCA-Enabler는 대부분의 Dell Ubuntu 플랫폼에 사전 로드되어 있습니다. DCA-Enabler 폴더와 관련 파일은 다음 위치에서 찾을 수 있습니다.

- `/etc/dcae/config/`
- `/etc/dcae/certificates/`
- `/var/log/dcae/dcae.log`
- `/usr/sbin/dcae`

다음 명령을 사용하여 Dell Ubuntu 플랫폼에서 DCA-Enabler 서비스 및 패키지를 확인할 수 있습니다.

- `systemctl status dcae.service-` 실행 중인 활성 버전이 표시됩니다.
- `dpkg -l | grep dca-enabler-` DCA-Enabler 버전은 **dca-enabler 1.x.0-xx** 형식으로 표시됩니다.

3

Wyse Device Agent 설치 또는 업그레이드

이 섹션에서는 Wyse Management Suite를 사용하여 Windows Embedded Standard, Linux 및 ThinLinux 디바이스와 같은 씬 클라이언트에서 Wyse Device Agent를 설치 또는 업그레이드하는 방법에 대해 설명합니다.

- **Windows Embedded Standard 디바이스** - support.dell.com에서 Wyse Device Agent 버전 1.4.x를 다운로드할 수 있습니다. 다음 방법 중 하나를 사용하여 Windows Embedded Standard 디바이스에서 Wyse Device Agent를 설치하거나 업그레이드할 수 있습니다.
  - Wyse Device Agent 수동 설치
  - Wyse Management Suite 애플리케이션 정책을 사용하여 Wyse Device Agent 업그레이드

  노트: Wyse Device Agent .exe 파일의 최신 버전을 두 번 클릭하여 Wyse Device Agent를 수동으로 업그레이드할 수도 있습니다.

  노트: Wyse Device Agent는 KB3033929를 사용할 수 있는 경우에만 Windows Embedded Standard 7 운영 체제에 설치할 수 있습니다.
- **Linux 및 ThinLinux 디바이스** - Wyse Device Agent는 Wyse Management Suite를 사용하여 Linux 및 ThinLinux 디바이스에 설치하거나 업그레이드할 수 있습니다. 자세한 내용은 ThinLinux 및 Linux 클라이언트에서 Wyse Device Agent 설치 또는 업그레이드를 참조하십시오.

주제:

- Windows Embedded 디바이스에 수동으로 Wyse Device Agent 설치
- Wyse Management Suite 애플리케이션 정책을 사용하여 Wyse Device Agent 업그레이드
- ThinLinux 및 Linux 클라이언트에서 Wyse Device Agent 설치 또는 업그레이드

Windows Embedded 디바이스에 수동으로 Wyse Device Agent 설치

단계

1. `WDA.exe` 파일을 씬 클라이언트로 복사합니다.
2. `WDA.exe` 파일을 두 번 클릭합니다.
3. **예**를 클릭합니다.

   노트: 디바이스에 이전 버전의 Wyse Device Agent 또는 HAgent가 설치되어 있으면 경고 메시지가 표시됩니다.
4. **그룹 토큰** 필드에 그룹 토큰을 입력합니다. 이 필드는 선택 사항입니다.
   이 단계를 건너뛰려면 **다음**을 클릭합니다. 나중에 Wyse Device Agent 사용자 인터페이스에서 그룹 토큰 세부 정보를 입력할 수 있습니다.
5. **지역** 드롭다운 목록에서 Wyse Management Suite 퍼블릭 클라우드 서버의 지역을 선택합니다.
   설치가 완료되면 Wyse Management Suite 퍼블릭 클라우드 서버가 Wyse Management Suite 콘솔에 디바이스를 자동으로 등록합니다.

Wyse Management Suite 애플리케이션 정책을 사용하여 Wyse Device Agent 업그레이드

전제조건

Wyse Device Agent를 업그레이드할 때는 Wyse Management Suite 애플리케이션을 사용하는 것이 좋습니다. Wyse Management Suite 프라이빗 클라우드 설정에서, 로컬 리포지토리의 Windows Embedded Standard용 최신 Wyse Device Agent 패키지를 사용할 수 있습

니다. 퍼블릭 클라우드를 사용하거나 프라이빗 클라우드의 원격 리포지토리를 사용하는 경우, `WDA.exe` 파일을 리포지토리의 `thinClientApps` 폴더에 복사합니다.

단계

1. `WDA.exe` 파일이 리포지토리로 복사되면 **앱 및 데이터**로 이동하고 이 패키지를 사용하여 표준 애플리케이션 정책을 생성합니다. 씬 클라이언트에 표준 애플리케이션 정책 생성 및 배포를 참조하십시오.

   노트: 고급 애플리케이션 정책은 Wyse Device Agent 14.x 이상에서만 지원됩니다. Wyse Device Agent를 14.x에서 업그레이드할 때는 표준 애플리케이션 정책을 사용하는 것이 좋습니다. Wyse Device Agent를 14.x에서 최신 버전으로 업그레이드할 경우에는 고급 애플리케이션 정책을 사용할 수도 있습니다.

2. **작업** 페이지로 이동하고 Wyse Device Agent 업그레이드 작업을 예약합니다.

   노트: Windows Embedded Standard Wyse Device Agent를 13.x 버전에서 14.x 버전으로 업그레이드하는 경우 HTTP를 리포지토리 프로토콜로 사용하는 것이 좋습니다.

   설치가 완료되면 상태가 서버로 전송됩니다.

ThinLinux 및 Linux 클라이언트에서 Wyse Device Agent 설치 또는 업그레이드

전제조건

- ThinLinux 버전 2.0, 이미지 버전 2.0.14 및 Wyse Device Agent 버전 3.0.7을 사용하는 Dell Wyse 3040 씬 클라이언트에 Wyse Device Agent를 설치하려면 `wda3040_3.0.10-01_amd64.deb` 파일을 설치한 다음 `wda_3.2.12-01_amd64.tar` 파일을 설치해야 합니다.
- Linux 씬 클라이언트용 플랫폼 유틸리티 추가 기능 및 Wyse Device Agent 추가 기능을 설치해야 합니다. ThinLinux 씬 클라이언트용 `wda_x.x.x.tar` 파일을 설치할 수 있습니다.

이 작업 정보

다음 옵션 중 하나를 사용하여 애드온을 설치하거나 업그레이드할 수 있습니다.

- INI 매개변수 사용
- 추가 설정 관리자
- RPM 명령

단계

1. 퍼블릭 클라우드를 사용하거나 프라이빗 클라우드의 원격 리포지토리를 사용하는 경우에는 RPM 파일을 리포지토리의 `thinClientApps` 폴더에 복사합니다. 기본적으로 Linux 및 ThinLinux 클라이언트용 최신 Wyse Device Agent 및 플랫폼 유틸리티 RPM을 로컬 리포지토리에서 사용할 수 있습니다.
2. **Jobs** 페이지로 이동하고 플랫폼 유틸리티 애드온 업그레이드 작업을 예약합니다.

   씬 클라이언트에 플랫폼 유틸리티 애드온이 설치될 때까지 기다려야 합니다.

   노트: 먼저 플랫폼 유틸리티 애드온을 설치한 다음 Wyse Device Agent 애드온을 설치합니다. 최신 플랫폼 유틸리티 애드온을 설치하기 전에는 최신 Wyse Device Agent를 설치할 수 없습니다.

3. **Jobs** 페이지에서 클라이언트에서 Wyse Device Agent를 업그레이드하는 작업을 예약합니다.

   노트: Wyse Device Agent 추가 기능 버전 2.0.11을 설치한 후에 Linux 클라이언트가 재시작됩니다.

4

Ubuntu 디바이스에 DCA-Enabler 설치 또는 업그레이드

이 섹션에서는 Ubuntu 디바이스에 DCA-Enabler를 설치하거나 업그레이드하는 방법에 대한 정보를 제공합니다.

주제:

- Ubuntu 디바이스에 DCA-Enabler 설치
- Ubuntu 디바이스에서 DCA-Enabler 업그레이드

Ubuntu 디바이스에 DCA-Enabler 설치

DCA-Enabler는 대부분의 Dell Ubuntu 플랫폼에 사전 로드되어 있습니다. DCA-Enabler가 사전 로드되지 않은 경우 DCA-Enabler를 설치할 수 있습니다.

단계

1. www.dell.com/support에서 DCA-Enabler 패키지를 다운로드합니다.
2. 다운로드한 파일의 압축을 풉니다.
   압축을 푼 파일에 .deb 파일이 포함되어 있습니다.
3. 다음 명령을 사용하여 DCA-Enabler 패키지 및 DCA-Enabler 패키지를 설치합니다.
   - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb >"`
   - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb >"`

Ubuntu 디바이스에서 DCA-Enabler 업그레이드

다음 방법 중 하나를 사용하여 Ubuntu 디바이스에서 DCA-Enabler를 업그레이드할 수 있습니다.

- Wyse Management Suite에 디바이스를 등록하고 애플리케이션 정책을 사용하여 최신 DCA-Enabler 패키지를 배포합니다.
- 수동으로 패키지를 다운로드하여 압축을 푼 다음 디바이스에서 다음 명령을 실행합니다.
  - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb"`
  - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb"`

5

Wyse Management Suite를 사용하여 새 디바이스 등록 및 구성

주제:

- Wyse Management Suite를 사용하여 새 Windows Embedded Standard 디바이스 등록 및 구성
- Wyse Management Suite를 사용하여 새 ThinOS 8.x 디바이스 등록 및 구성
- Wyse Management Suite를 사용하여 새 ThinOS 9.x 디바이스 등록 및 구성
- Wyse Management Suite를 사용하여 새 Linux 또는 ThinLinux 디바이스 등록 및 구성
- Wyse Management Suite를 사용하여 새 Wyse 소프트웨어 씬 클라이언트 등록 및 구성
- Wyse Management Suite를 사용한 Dell Hybrid Client 등록 및 구성
- Wyse Management Suite를 사용한 Dell Generic Client 등록 및 구성

Wyse Management Suite를 사용하여 새 Windows Embedded Standard 디바이스 등록 및 구성

단계

1. 씬 클라이언트에 Wyse Device Agent 설치 - Wyse Device Agent 설치 또는 업그레이드를 참조하십시오.
2. Wyse Management Suite에 씬 클라이언트 등록 - Wyse Device Agent를 사용하여 Wyse Management Suite에 Windows Embedded Standard 씬 클라이언트 등록을 참조하십시오.

   노트: 다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.
   - DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

   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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

3. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
4. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
   - **그룹 및 구성** 페이지 사용 - Windows Embedded Standard 정책 설정 편집을 참조하십시오.
   - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용하여 새 ThinOS 8.x 디바이스 등록 및 구성

단계

1. 씬 클라이언트의 데스크탑 메뉴에서 **시스템 설정** > **중앙 구성**으로 이동합니다.
   중앙 구성 창이 표시됩니다.
2. 관리자가 원하는 그룹에 대해 구성한 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.

   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. **확인**을 클릭합니다.

   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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

   디바이스가 Wyse Management Suite에 등록됩니다.
8. Wyse Management Suite로 로그인합니다.
9. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
10. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
    - **그룹 및 구성** 페이지 사용 - ThinOS 정책 설정 편집을 참조하십시오.
    - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용하여 새 ThinOS 9.x 디바이스 등록 및 구성

단계

1. 씬 클라이언트의 데스크탑 메뉴에서 **시스템 설정** > **중앙 구성**으로 이동합니다.
   중앙 구성 창이 표시됩니다.
2. 관리자가 원하는 그룹에 대해 구성한 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.

   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.

   알림 창이 표시됩니다.
7. **확인**을 클릭합니다.
8. **중앙 구성** 창에서 **확인**을 클릭합니다.

   노트: 다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.
   - DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

   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 검사

를 수행할 수 있습니다. 디바이스의 유효성 검사가 완료되면 디바이스가 해당 그룹으로 이동됩니다. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

디바이스가 Wyse Management Suite에 등록됩니다.

9. Wyse Management Suite로 로그인합니다.
10. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
11. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
    - **그룹 및 구성** 페이지 사용 - ThinOS 9.x 정책 설정 편집을 참조하십시오.
    - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용하여 새 Linux 또는 ThinLinux 디바이스 등록 및 구성

단계

1. 씬 클라이언트에 Wyse Device Agent 설치 - Wyse Device Agent 설치 또는 업그레이드를 참조하십시오.
2. Wyse Management Suite에 씬 클라이언트 등록 - Wyse Device Agent를 사용하여 Wyse Management Suite에 Linux/ThinLinux 씬 클라이언트 등록을 참조하십시오.

   노트: 다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.
   - DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

   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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

3. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
4. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
    - **그룹 및 구성** 페이지 사용 - ThinLinux 정책 설정 편집 또는 Linux 정책 설정 편집을 참조하십시오.
    - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용하여 새 Wyse 소프트웨어 씬 클라이언트 등록 및 구성

단계

1. 씬 클라이언트에 Wyse Device Agent 설치 - Wyse Device Agent 설치 또는 업그레이드를 참조하십시오.
2. Wyse Management Suite에 씬 클라이언트 등록 - Wyse Device Agent를 사용하여 Wyse Management Suite에 Wyse 소프트웨어 씬 클라이언트 등록을 참조하십시오.

   노트: 다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.
   - DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

   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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

3. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
4. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
    - **그룹 및 구성** 페이지 사용 - Wyse 소프트웨어 씬 클라이언트 정책 설정 편집을 참조하십시오.

- **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용한 Dell Hybrid Client 등록 및 구성

전제조건

디바이스를 등록하기 전에 디바이스가 네트워크에 연결되어 있어야 Wyse Management Suite 서버에 연결할 수 있습니다.

노트: 게스트 사용자 계정에서만 디바이스를 등록하거나 등록 취소할 수 있습니다.

단계

1. Dell Hybrid Client에 게스트 사용자로 로그인합니다.
2. 위쪽 표시줄에서 을 클릭합니다.

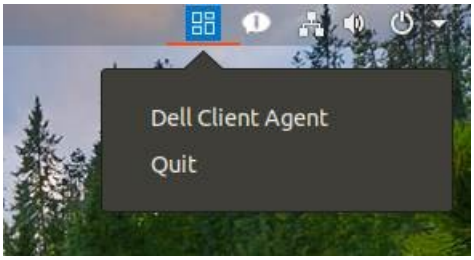


그림 1 . DCA 아이콘

3. **Dell Client Agent**를 클릭합니다.
   Dell Client Agent 대화 상자가 표시됩니다.
4. **등록**을 클릭합니다.
   기본 상태가 **검색 진행 중**으로 표시됩니다.
5. 수동으로 종료하려면, **취소** 버튼을 클릭합니다.
6. **WMS 서버** 필드에 Wyse Management Suite 서버의 URL을 입력합니다.
7. **그룹 토큰** 필드에 그룹 등록 키를 입력합니다. 그룹 토큰은 디바이스를 그룹에 직접 등록할 수 있는 고유한 키입니다.

   노트: 테넌트 및 그룹 필드가 비어 있으면 디바이스가 관리되지 않는 그룹에 등록됩니다. 그러나 디바이스를 퍼블릭 클라우드에 등록하려면 그룹 토큰이 필요합니다.

8. **서버 인증서 CA 유효성 검사** 옵션을 활성화하거나 비활성화하려면 **켜기/끄기** 버튼을 클릭합니다. 모든 디바이스 대 서버 통신에 대한 서버 인증서 유효성을 검사하려면 이 옵션을 활성화합니다.
   CA 유효성 검사 옵션은 자동으로 활성화되며 퍼블릭 클라우드 URL을 입력하면 비활성화할 수 없습니다.
9. **등록**을 클릭하여 Wyse Management Suite 서버에 하이브리드 클라이언트를 등록합니다.
   다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.
   - DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

   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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

   하이브리드 클라이언트가 성공적으로 등록되면 상태가 **등록 상태** 레이블 옆에 있는 녹색 체크 표시와 함께 **등록됨**으로 표시됩니다. **등록** 버튼의 캡션이 **등록 취소**로 변경됩니다.

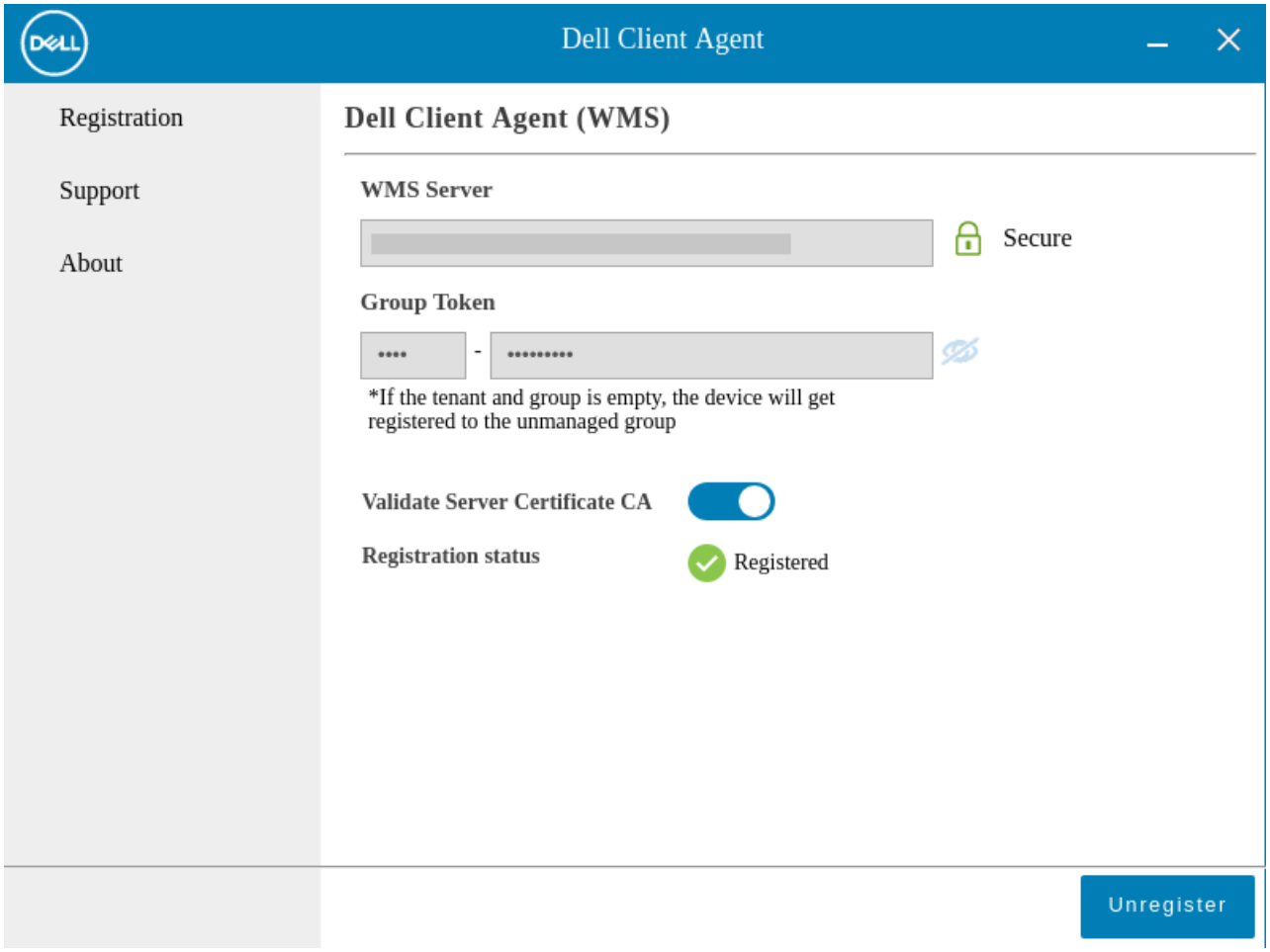


그림 2 . Dell Client Agent

10. Wyse Management Suite로 로그인합니다.
11. 원하는 그룹에 디바이스 추가(선택 사항) - 그룹 및 구성 관리를 참조하십시오.
12. 다음 옵션 중 하나를 사용하여 씬 클라이언트를 구성합니다.
    - **그룹 및 구성** 페이지 사용 - Dell Hybrid Client 정책 설정 편집을 참조하십시오.
    - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

Wyse Management Suite를 사용한 Dell Generic Client 등록 및 구성

전제조건

- 디바이스를 등록하기 전에 디바이스가 네트워크에 연결되어 있어야 Wyse Management Suite 서버에 연결할 수 있습니다.
- DCA-Enabler가 디바이스에 설치됩니다.

노트: Ubuntu 사용자 계정에서만 디바이스를 등록하거나 등록 취소할 수 있습니다.

단계

1. Ubuntu 운영 체제를 실행하는 Dell Generic Client에 로그인합니다.
2. 터미널을 엽니다.
3. 명령 `systemctl restart dcae.service`를 사용하여 dcae_service를 재시작합니다.
   DCA-Enabler 서비스는 `/etc/dcae/config` 폴더에 있는 reg.json 파일을 사용하여 디바이스를 수동으로 등록합니다.
   다음 방법 중 하나를 사용하여 디바이스를 등록할 수도 있습니다.
   - DHCP 옵션 태그 사용 - DHCP 옵션 태그를 사용하여 디바이스 등록을 참조하십시오.

- DNS SRV 레코드 사용 - DNS SRV 레코드를 사용하여 디바이스 등록을 참조하십시오.

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. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

4. Wyse Management Suite로 로그인합니다.
5. 원하는 그룹에 디바이스를 추가하거나 이동합니다(선택 사항). 그룹 및 구성 관리를 참조하십시오.
6. 다음 옵션 중 하나를 사용하여 일반 클라이언트를 구성합니다.
   - **그룹 및 구성** 페이지 사용 - Dell Generic Client 설정 편집을 참조하십시오.
   - **디바이스 페이지** 사용 - 디바이스 관리를 참조하십시오.

6

Wyse Management Suite 대시보드

Dashboard 페이지에서 시스템 상태와 시스템에서 수행한 최근 작업을 볼 수 있습니다. 특정 경고를 보려면 **경고** 섹션에서 링크를 클릭합니다. **대시보드** 페이지에서 디바이스 요약을 볼 수도 있습니다.

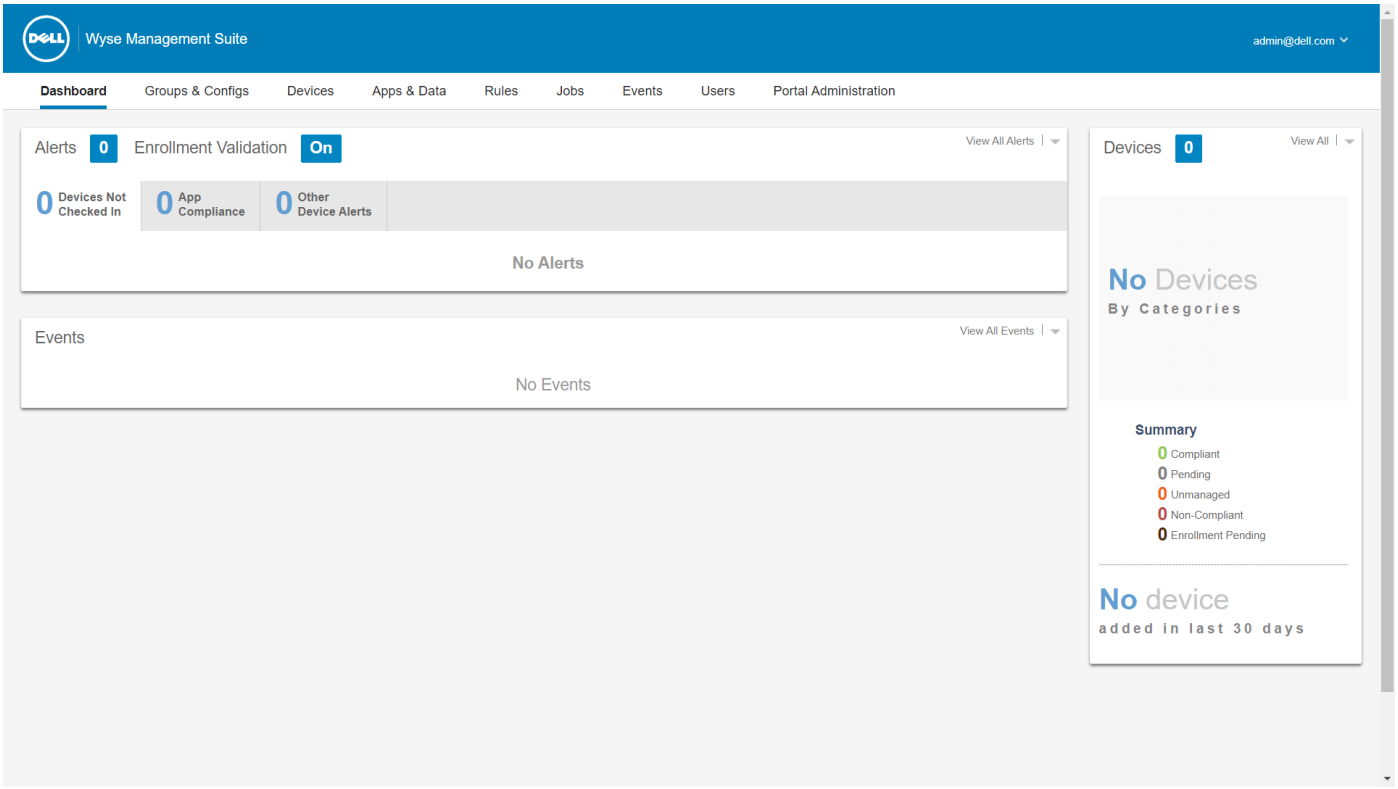


그림 3 . 대시보드

주제:

- 경고 보기
- 이벤트 목록 보기
- 디바이스 상태 보기
- 등록 유효성 검사 활성화
- 사용자 기본 설정 변경
- 온라인 도움말 액세스
- 암호 변경
- 관리 콘솔에서 로그아웃

경고 보기

경고 섹션에는 모든 경고의 요약이 표시됩니다.

단계

1. **대시보드**를 클릭합니다.
   경고 요약이 표시됩니다.
2. **모든 경고 보기**를 클릭합니다.

이벤트 페이지에 표시되는 특성은 다음과 같습니다.

- **디바이스가 체크인되지 않음**
- **앱 규정 준수**
- **기타 디바이스 경고**

이벤트 목록 보기

이벤트 섹션에는 지난 며칠 동안 발생한 이벤트의 요약이 표시됩니다.

단계

1. **대시보드**를 클릭합니다.
   이벤트 요약이 표시됩니다.
2. **모든 이벤트 보기**를 클릭합니다.
   이벤트 페이지가 모든 이벤트의 목록과 함께 표시됩니다.

디바이스 상태 보기

디스플레이 섹션에는 디바이스 상태에 대한 요약이 나와 있습니다.

단계

1. **대시보드**를 클릭합니다.
   디바이스 요약이 표시됩니다.
2. **모두 보기**를 클릭합니다.
   디바이스 페이지가 등록된 모든 디바이스의 목록과 함께 표시됩니다. **요약** 섹션에는 다음 디바이스 상태 범주를 기반으로 디바이스 개수가 표시됩니다.
   - **준수**
   - **보류 중**
   - **관리되지 않음**
   - **비준수**
   - **등록 보류 중**

등록 유효성 검사 활성화

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

단계

1. **대시보드**를 클릭합니다.
2. **등록 유효성 검사** 옵션 옆에 있는 **켜기/끄기** 버튼을 클릭합니다.
   포털 관리 페이지의 **기타 설정** 옵션으로 리디렉션됩니다.
3. **등록 유효성 검사** 옵션을 활성화 또는 비활성화합니다.

사용자 기본 설정 변경

경고 알림, 정책 설정 및 페이지 크기와 같은 사용자 기본 설정을 변경할 수 있습니다.

단계

1. **대시보드** 페이지의 오른쪽 상단에서 로그인 드롭다운 메뉴를 클릭합니다.
2. **사용자 기본 설정**을 클릭합니다.
   사용자 기본 설정 창이 표시됩니다.
3. **경고**를 클릭하고 이메일 및 모바일 애플리케이션에서 전달되는 알림의 경고 유형(위험, 경고 또는 정보)을 할당하려면 해당 확인란을 선택합니다.

4. **정책**을 클릭하고 **ThinOS 마법사 모드를 사용할 것인지 묻습니다** 확인란을 선택하여 ThinOS 정책 설정을 구성할 때마다 **ThinOS 구성 모드 선택** 창을 표시합니다.
5. **페이지 크기**를 클릭하고 **페이지당 항목 수** 텍스트 상자에 10 - 100 사이의 숫자를 입력합니다. 이 옵션을 사용하면 각 페이지에 표시되는 항목 수를 설정할 수 있습니다.

온라인 도움말 액세스

단계

1. **대시보드** 페이지의 오른쪽 상단에서 로그인 드롭다운 메뉴를 클릭합니다.
2. **WMS 도움말**을 클릭합니다.
   Wyse Management Suite 지원 페이지가 표시됩니다.

암호 변경

단계

1. **대시보드** 페이지의 오른쪽 상단에서 로그인 드롭다운 메뉴를 클릭합니다.
2. **암호 변경**을 클릭합니다.
   암호 변경 창이 표시됩니다.
3. 현재 암호를 입력합니다.
4. 새 암호를 입력합니다.
5. 확인을 위해 새 암호를 다시 입력합니다.
6. **암호 변경**을 클릭합니다.

관리 콘솔에서 로그아웃

단계

1. **대시보드** 페이지의 오른쪽 상단에서 로그인 드롭다운 메뉴를 클릭합니다.
2. **로그아웃**을 클릭합니다.

7

그룹 및 구성 관리

그룹 및 구성 페이지에서 디바이스를 구성하는 데 필요한 정책을 정의할 수 있습니다. 전역 그룹 정책의 하위 그룹을 생성하고 요구 사항에 따라 디바이스를 분류할 수 있습니다. 예를 들어 디바이스를 작업 기능, 디바이스 유형 등에 따라 그룹화할 수 있습니다.

각 그룹에서 다음 운영 체제에 대한 정책을 정의할 수 있습니다.

- **ThinOS**
  - **ThinOS**
  - **ThinOS 9.x**
- **WES**
- **Linux**
- **ThinLinux**
- **Teradici**
- **Wyse 소프트웨어 씬 클라이언트**
- **하이브리드 클라이언트**
- **일반 클라이언트**

디바이스는 생성된 순서대로 정책을 상속합니다. 기본 정책 그룹에 구성된 설정은 기본 정책 그룹에 나열된 모든 정책에서 기본 설정으로 적용됩니다. 특정 그룹에 있는 모든 디바이스는 기본 정책 그룹을 기본 설정으로 사용합니다.

디바이스 세부 정보 페이지에서 그룹 기본값과 다른 정책의 하위 집합을 갖도록 그룹의 디바이스에 대한 예외를 생성할 수 있습니다.

구성이 설정된 위치(전역, 그룹 및 디바이스 수준)에 대한 세부 정보와 함께 특정 자산에 대한 구성이 이 페이지에 표시됩니다. 예외 생성 옵션을 페이지에서 사용할 수 있습니다. **예외** 설정은 선택한 디바이스에만 적용됩니다.

노트: 하위 수준 정책을 수정하면 정책 옆에 글머리 기호가 표시됩니다. 이 기호는 해당 정책이 상위 수준 정책을 재정의한다는 것을 나타냅니다. 예를 들어 시스템 개인 설정, 네트워킹, 보안 등이 있습니다. 정책을 수정하면 정책 옆에 별표(*)가 표시됩니다. 이 기호는 저장되지 않았거나 게시되지 않은 변경 사항이 있다는 것을 나타냅니다. 이러한 변경 사항을 게시하기 전에 검토하려면 **보류 중인 변경 사항 보기** 링크를 클릭합니다.

서로 다른 수준에서 정책 구성의 우선 순위를 지정해야 하는 경우에는 최하위 수준 정책이 우선 적용됩니다.

정책 설정을 구성하면 변경 사항에 대한 알림이 씬 클라이언트에 제공됩니다. 씬 클라이언트를 구성한 직후에 변경 사항이 적용됩니다.

노트: Windows Embedded Standard에 대한 BIOS 구성과 같은 특정 설정은 시스템을 재시작해야 변경 사항이 적용됩니다. 하지만 ThinOS의 대부분의 설정은 디바이스를 재시작해야 변경 사항이 적용됩니다.

정책은 다음 우선 순위에 따라 적용됩니다.

- 전역 수준 정책
- 디바이스 그룹 수준 정책
- 디바이스 예외
- 사용자 그룹 수준 정책
- 사용자 예외
- 사용자 개인 설정

기본 디바이스 그룹에 적용된 배경 화면 또는 펌웨어 정책과 같은 구성은 기본적으로 하위 그룹에 적용됩니다. Wyse Management Suite 3.2에서 하위 그룹에 대해 이러한 구성을 재정의할 수 있습니다.

노트: Wyse Management Suite 3.3에서 클라이언트로 구성을 5,000회 동시 다운로드할 수 있습니다. 추가적인 동시 다운로드는 슬롯이 사용 가능한 상태가 될 때까지 대기 상태로 전환됩니다. 60초 후 요청 시간이 초과됩니다.

주제:

- 관리되지 않는 그룹 편집
- 기본 디바이스 정책 그룹 생성
- 사용자 정책 그룹 생성
- 전역 수준 정책 구성
- 사용자 정책 그룹 가져오기

- 그룹 제거
- 디바이스 수준 정책 구성
- 그룹 정책 내보내기
- 그룹 정책 가져오기
- ThinOS 정책 설정 편집
- ThinOS 9.x 정책 설정 편집
- Windows Embedded Standard 정책 설정 편집
- Linux 정책 설정 편집
- ThinLinux 정책 설정 편집
- Wyse 소프트웨어 씬 클라이언트 정책 설정 편집
- 클라우드 연결 정책 설정 편집
- Dell Hybrid Client 정책 설정 편집
- Dell Generic Client 정책 설정 편집
- 대량 디바이스 예외 파일 생성 및 가져오기

관리되지 않는 그룹 편집

관리되지 않는 그룹에 속하는 디바이스는 라이선스를 사용하거나 구성 또는 애플리케이션 기반 정책을 수신하지 않습니다. 관리되지 않는 그룹에 디바이스를 추가하려면 관리되지 않는 그룹 디바이스 등록 키를 자동 등록 또는 수동 디바이스 등록의 일부로 사용합니다.

단계

1. **그룹 및 구성** 페이지에서 **관리되지 않는 그룹**을 선택합니다.
2. 을 클릭합니다.
   관리되지 않는 그룹 편집 페이지가 표시됩니다. **그룹 이름**에 그룹의 이름이 표시됩니다.
3. 다음 세부 사항을 입력합니다.
   - **설명** - 그룹에 대한 간단한 설명을 표시합니다.
   - **그룹 토큰** - 그룹 토큰을 활성화하려면 이 옵션을 선택합니다.
4. **저장**을 클릭합니다.

   노트: 퍼블릭 클라우드의 경우 디바이스를 등록하려면 관리되지 않는 그룹에 대한 그룹 토큰을 활성화해야 합니다. 프라이빗 클라우드의 경우 관리되지 않는 그룹에 대한 그룹 토큰이 자동으로 활성화됩니다.

기본 디바이스 정책 그룹 생성

전역 디바이스 그룹 정책에 대한 그룹을 생성하고 요구 사항에 따라 디바이스를 분류할 수 있습니다.

단계

1. **그룹 및 구성** 페이지에서 **기본 디바이스 정책 그룹** 옵션을 클릭합니다.
2. 를 클릭합니다.
3. **새 그룹 추가** 대화 상자에서 **그룹 이름**과 **설명**을 입력합니다.
4. **ThinOS 선택 그룹 상위** 옵션을 선택하여 ThinOS 디바이스의 상위 선택 그룹을 생성합니다. 이 단계는 선택 사항입니다.
   자세한 내용은 ThinOS 선택 그룹 생성을 참조하십시오.
5. **등록** 탭의 그룹 토큰 아래에서 **활성화** 확인란을 선택합니다.
6. 그룹 토큰을 입력합니다.
7. **관리** 탭에서 이 그룹을 관리해야 하는 그룹 관리자의 이름을 선택할 수 있습니다. **사용 가능한 그룹 관리자** 상자에서 특정 그룹을 선택하고 오른쪽 화살표를 클릭하여 **할당된 그룹 관리자** 상자로 이동합니다. **할당된 그룹 관리자**에서 **사용 가능한 그룹 관리자**로 그룹을 이동하려면 그 반대로 수행합니다. 이 단계는 선택 사항입니다.
8. **저장**을 클릭합니다.
   그룹이 **그룹 및 구성** 페이지의 사용 가능한 그룹 목록에 추가됩니다.

노트: 해당 그룹에 대한 **그룹 및 구성** 페이지에서 사용할 수 있는 그룹 토큰을 입력하여 디바이스를 그룹에 등록할 수 있습니다.

노트: 상위 디바이스 정책 그룹에는 하위 디바이스 그룹을 10개만 사용할 수 있습니다.

ThinOS 선택 그룹 생성

단계

1. **그룹 및 구성** 페이지에서 **기본 디바이스 정책 그룹** 옵션을 클릭합니다.
2. +를 클릭합니다.
3. **새 그룹 추가** 대화 상자에서 **그룹 이름**과 **설명**을 입력합니다.
4. **ThinOS 선택 그룹 상위 항목** 옵션을 선택합니다.
5. 이 그룹을 관리해야 하는 그룹 관리자의 이름을 선택합니다. **사용 가능한 그룹 관리자** 상자에서 특정 그룹을 선택하고 오른쪽 화살표를 클릭하여 **할당된 그룹 관리자** 상자로 이동합니다. **할당된 그룹 관리자**에서 **사용 가능한 그룹 관리자**로 그룹을 이동하려면 그 반대로 수행합니다. 이 단계는 선택 사항입니다.
6. **저장**을 클릭합니다.

   그룹이 **그룹 및 구성** 페이지의 사용 가능한 그룹 목록에 추가됩니다.

   생성된 상위 그룹에 하위 그룹을 추가하려면 **그룹 및 구성** 페이지에서 상위 그룹을 클릭하고 디바이스 정책 그룹 생성에서 설명하는 단계를 따릅니다.

   노트: 상위 선택 그룹에는 10개의 하위 선택 그룹이 있을 수 있으며 하위 선택 그룹에 디바이스를 등록할 수 있습니다. 다른 운영 체제의 프로필을 구성할 수 있습니다. 생성된 프로필은 다른 맞춤형 그룹과 동일합니다.

   노트: 하위 그룹에서 변경된 일부 정책의 경우 변경 내용을 적용하려면 클라이언트를 재부팅해야 합니다.

기본 디바이스 정책 그룹 편집

단계

1. **그룹 및 구성** 페이지로 이동하여 **기본 디바이스 정책 그룹**을 선택합니다.
2. **기본 디바이스 정책 그룹 편집** 대화 상자에서 필요한 그룹 정보를 편집합니다.
3. **저장**을 클릭합니다.

ThinOS 선택 그룹 편집

단계

1. **그룹 및 구성** 페이지로 이동하여 편집하려는 ThinOS 선택 그룹을 클릭합니다.
2. 을 클릭합니다.
3. **기본 정책 그룹 편집** 대화 상자에서 **그룹 이름** 및 **설명**과 같은 그룹 정보를 편집합니다.
4. **관리** 탭에서 이 그룹을 관리해야 하는 그룹 관리자의 이름을 선택할 수 있습니다. **사용 가능한 그룹 관리자** 상자에서 특정 그룹을 선택하고 오른쪽 화살표를 클릭하여 **할당된 그룹 관리자** 상자로 이동합니다. **할당된 그룹 관리자**에서 **사용 가능한 그룹 관리자**로 그룹을 이동하려면 왼쪽 화살표를 클릭합니다. 이 단계는 선택 사항입니다.
5. **저장**을 클릭합니다.

ThinOS 선택 그룹 제거

관리자는 그룹 계층에서 그룹을 제거할 수 있습니다.

단계

1. **그룹 및 구성** 페이지에서 삭제하려는 ThinOS 선택 그룹을 선택합니다.

2. 를 클릭합니다.
   이 작업으로 그룹 트리 계층에서 하나 이상의 그룹이 제거되었음을 나타내는 경고 메시지가 표시됩니다.
3. 그룹 드롭다운 목록에서 현재 그룹의 사용자 및 디바이스에 대한 새 타겟 그룹을 선택합니다.
4. **그룹 제거**를 클릭합니다.

   노트: 그룹 계층에서 그룹을 제거하면 삭제된 그룹에 속하는 모든 사용자와 디바이스가 맞춤형, 기본 또는 관리되지 않는 그룹으로 이동됩니다.

   노트: 선택 그룹을 삭제하면 제거된 그룹의 디바이스를 다른 선택 그룹으로 이동할 수 없습니다.

사용자 정책 그룹 생성

전역 사용자 그룹 정책에 대한 그룹을 생성하고 사용자 그룹에 따라 사용자와 디바이스를 분류할 수 있습니다.

단계

1. **그룹 및 구성** 페이지에서 **기본 사용자 정책 그룹** 옵션을 클릭합니다.
2. +를 클릭합니다.
3. **새 그룹 추가** 대화 상자에서 AD 도메인에 있는 이름인 **그룹 이름**, **설명**, **도메인**, **AD 특성**(AD 그룹 또는 OU 그룹) 및 **AD 특성 이름**을 입력합니다. **그룹 이름**을 **AD 특성 이름**으로 사용해야 합니다.

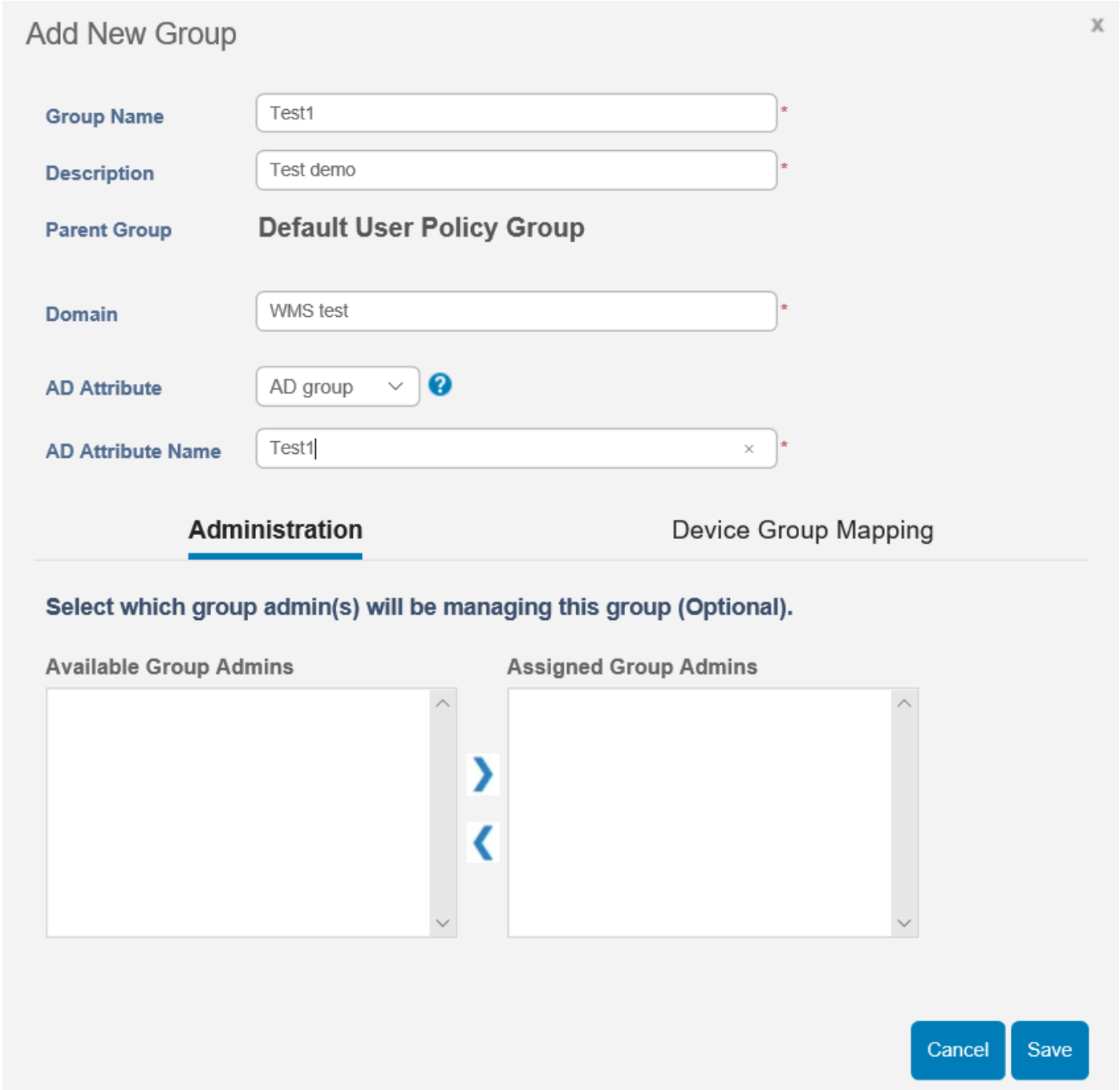


그림 4 . 새 그룹 추가

노트: AD 그룹이 도메인의 OU 그룹 안에 있으면 OU 그룹을 AD 특성으로 선택해야 합니다.

4. 이 그룹을 관리해야 하는 그룹 관리자의 이름을 선택합니다.
5. **사용 가능한 그룹 관리자** 상자에서 특정 그룹을 선택하고 오른쪽 화살표를 클릭하여 **할당된 그룹 관리자** 상자로 이동합니다.
   할당된 그룹 관리자에서 **사용 가능한 그룹 관리자**로 그룹을 이동하려면 그 반대로 수행합니다.
6. **저장**을 클릭합니다.
   그룹이 **그룹 및 구성** 페이지의 사용 가능한 그룹 목록에 추가됩니다.
   노트: 사용자 정책 그룹은 AD 그룹 또는 조직 단위에 매핑되어야 하지만 둘 다 함께 매핑할 수 없습니다.
7. **디바이스 그룹 매핑** 옵션을 선택하여 디바이스 매핑을 사용하는 사용자 그룹을 가져와서 기본적으로 모든 디바이스 그룹에 적용되는 구성을 제어합니다.

Wyse Management Suite로 가져온 AD 사용자 그룹은 해당 디바이스 그룹에 매핑할 수 있습니다. 디바이스를 매핑하면 원치 않는 사용자 그룹 정책을 수신하지 않습니다.

노트: 기본적으로 사용자 그룹은 디바이스 그룹에 매핑되지 않습니다. **기본 디바이스 그룹** 정책을 선택하면 모든 하위 디바이스 그룹이 선택됩니다. 이 기능은 Wyse Management Suite Pro 라이선스에서만 사용할 수 있습니다. 100개의 사용자 그룹을 Wyse Management Suite에 가져올 수 있습니다.

노트: 사용자 그룹 및 디바이스 그룹 매핑은 최대 25,000개의 디바이스를 지원합니다.

사용자 정책 그룹 편집

단계

1. **그룹 및 구성** 페이지로 이동하여 기본 사용자 정책 그룹을 선택합니다.
2. 을 클릭합니다.
3. **기본 사용자 정책 그룹 편집** 대화 상자에서 필요한 그룹 정보를 편집합니다.
4. **저장**을 클릭합니다.

전역 수준 정책 구성

단계

1. **그룹 및 구성** 페이지의 **정책 편집** 드롭다운 메뉴에서 디바이스 유형을 선택합니다.
   각 디바이스 유형의 정책 설정이 표시됩니다.
2. 구성할 정책 설정을 선택한 다음 **이 항목 구성**을 클릭합니다.
3. 옵션을 구성한 후에 **저장 및 게시**를 클릭합니다.

사용자 정책 그룹 가져오기

단계

1. **그룹 및 구성** 페이지에서 **기본 사용자 정책 그룹** 옵션을 클릭합니다.
2. 를 클릭합니다.
3. **대량 가져오기** 대화 상자에서 **찾아보기**를 클릭하고 .csv 파일을 찾습니다.
   .csv 파일에는 다음 순서로 세부 정보가 포함되어 있어야 합니다.
   - 그룹 이름 - 표시 이름
   - 설명
   - 도메인 - 도메인 이름
   - AD 특성 - AD 그룹 또는 OU 그룹
   - AD 특성 이름 - AD 도메인에 있는 그룹 이름

   노트: 그룹 이름을 AD 특성 이름으로 사용해야 합니다. 또한 AD 그룹이 도메인의 OU 그룹 안에 있는 경우 **OU 그룹**을 **AD 특성**으로 선택해야 합니다.
4. .csv 파일에 헤더 줄이 있는 경우 **CSV 파일에 헤더 줄 있음** 확인란을 선택합니다.
5. **가져오기**를 클릭합니다.

그룹 제거

관리자는 그룹 계층에서 그룹을 제거할 수 있습니다.

단계

1. **그룹 및 구성** 페이지에서 삭제하려는 그룹을 선택합니다.
2.  를 클릭합니다.
   이 작업으로 그룹 트리 계층에서 하나 이상의 그룹이 제거되었음을 나타내는 경고 메시지가 표시됩니다.
3. 드롭다운 목록에서 새 그룹을 선택하여 현재 그룹의 사용자 및 디바이스를 이동합니다.
4. **그룹 제거**를 클릭합니다.

   노트: 디바이스 그룹이 삭제되면 그룹의 모든 디바이스가 선택된 디바이스 그룹으로 이동합니다. 사용자 그룹이 삭제되면 연결된 디바이스 또는 사용자가 없습니다.

디바이스 수준 정책 구성

단계

1. **디바이스** 페이지에서 구성하려는 디바이스를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.
2. **디바이스 구성** 섹션에서 **예외 생성/편집**을 클릭합니다.

그룹 정책 내보내기

정책 내보내기 옵션을 사용하면 현재 그룹에서 정책을 내보낼 수 있습니다. 이 옵션은 Wyse Management Suite Pro 라이선스 사용자가 사용할 수 있습니다.

단계

1. **그룹 및 구성** 페이지에서 정책을 내보낼 그룹을 선택합니다. 그룹에 구성된 정책이 있어야 합니다.
2. **정책 내보내기**를 클릭합니다.
   정책 내보내기 화면이 표시됩니다.
3. 내보낼 디바이스 유형 정책을 선택합니다.
   다음과 같은 옵션을 사용할 수 있습니다.
   - 모든 디바이스 유형 정책 – 모든 디바이스 유형 정책을 내보냅니다.
   - 특정 디바이스 유형 정책 – 드롭다운 목록에서 디바이스 유형을 하나 이상 선택합니다. 선택한 디바이스 유형 정책만 내보냅니다.
4. 선택한 디바이스 유형 정책을 내보내려면 **예** 버튼을 클릭합니다.
   상위 그룹 정책은 내보내지 않습니다. 선택 또는 대상 그룹 수준에 구성된 정책만 내보냅니다.
5. 다운로드 링크를 클릭하거나 파일을 마우스 오른쪽 버튼으로 클릭하고 **다른 이름으로 저장**을 클릭하여 `JSON` 파일을 저장합니다.

   노트: 암호는 내보낸 파일에서 암호화됩니다. 파일 이름은 `[Group Name]-[ALL]-[Exported Date & Time]UTC.json` 형식입니다.

   노트: 정책 가져오기 오류를 방지하려면 파일로 내보내기 전에 인증서, 배경 화면, 펌웨어, 로고 등의 파일에 대한 암호 및 참조를 제거해야 합니다.

그룹 정책 가져오기

정책 가져오기 옵션을 사용하면 정책을 가져올 수 있습니다. 이 옵션은 Wyse Management Suite PRO 라이선스 사용자가 사용할 수 있습니다. **그룹 및 구성** 페이지 또는 **정책 편집** 페이지에서 그룹 정책을 가져올 수 있습니다.

그룹 및 구성 페이지에서 그룹 정책 가져오기

단계

1. **그룹 및 구성** 페이지에서 기본 설정 그룹을 선택합니다.

대상 그룹에 가져온 것과 동일한 디바이스 유형의 정책이 포함되어 있으면 해당 정책이 제거되고 새 정책이 추가됩니다.

2. **정책 가져오기**를 클릭합니다.
   정책 가져오기 마법사 화면이 표시됩니다.
3. 선택한 그룹에서 그룹 정책을 가져오기 위한 모드를 선택합니다.
   다음과 같은 옵션을 사용할 수 있습니다.
   - 기존 그룹에서 - 드롭다운 목록에서 그룹을 선택합니다. 해당 그룹의 정책이 현재 그룹에 복사됩니다.
   - 내보낸 파일에서 - `.json` 파일을 검색합니다. 해당 파일의 정책이 현재 그룹에 복사됩니다.
4. **다음**을 클릭합니다.
5. 가져올 디바이스 유형 구성을 선택합니다.
   다음과 같은 옵션을 사용할 수 있습니다.
   - 모든 디바이스 유형 정책 - 구성된 모든 디바이스 유형 정책을 현재 그룹으로 가져옵니다.
   - 특정 디바이스 유형 정책 - 드롭다운 목록에서 하나 이상의 디바이스 유형을 선택합니다. 선택한 디바이스 유형 정책만 현재 그룹으로 가져옵니다.
6. **다음**을 클릭합니다.
   선택한 그룹에 있는 정책의 미리 보기가 표시됩니다.
7. **다음**을 클릭합니다.
   가져오기 프로세스의 요약이 표시됩니다. 다음 유형의 경고가 표시될 수 있습니다.
   - **가져온 <운영 체제 유형> 정책이 <그룹 이름> 그룹에 적용됩니다** - 어떤 구성도 없는 그룹으로 운영 체제 구성을 가져오는 경우.
   - **<그룹 이름> 그룹에 대한 <운영 체제 유형> 정책이 이미 있습니다. 제거된 정책인 기존 <운영 체제 유형> 정책이 적용됩니다** - 운영 체제 유형 구성이 있는 그룹으로 새 운영 체제 유형 구성을 가져오는 경우.
   - **인벤토리 파일에 대한 종속성이 포함된 파일에서 정책을 가져올 수 없습니다. 이 가져오기를 허용하려면 "정책 편집" 창에서 가져오기 옵션을 사용합니다** - 인벤토리 파일에 대한 참조가 있는 파일에서 디바이스 유형 구성을 가져오는 경우.
8. **가져오기**를 클릭합니다.

   노트: 선택한 디바이스 유형 구성만 가져올 수 있습니다. 선택한 디바이스 유형에 대해 타겟 그룹에 정의된 정책은 동일한 디바이스 유형의 새 정책을 적용하기 전에 제거됩니다.

   노트: 그룹 정책을 가져오는 동안 암호 및 참조 파일을 가져오지 않습니다. 정책을 게시하기 전에 관리자가 해당 정책을 선택해야 합니다.

정책 편집 페이지에서 그룹 정책 가져오기

단계

1. **그룹 및 구성** 페이지에서 기본 설정 그룹을 선택합니다.
2. **정책 편집**을 클릭하고 기본 설정 옵션을 선택합니다.
3. **가져오기**를 클릭합니다.
   정책 가져오기 마법사 화면이 표시됩니다.
4. 선택한 그룹에서 그룹 정책을 가져오기 위한 모드를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.
   - 기존 그룹에서 - 드롭다운 목록에서 그룹을 선택합니다. 해당 그룹의 정책이 현재 그룹에 복사됩니다.
   - 내보낸 파일에서 - **찾아보기**를 클릭하고 `.JSON` 파일을 선택합니다. 해당 파일의 정책이 현재 그룹에 복사됩니다.
5. **다음**을 클릭합니다.
   선택한 그룹에 있는 정책의 미리 보기가 표시됩니다.
6. **다음**을 클릭합니다. 가져오기 프로세스의 요약이 표시됩니다. 다음 유형의 경고가 표시될 수 있습니다.
   - **가져온 <디바이스 유형> 정책이 <그룹 이름> 그룹에 적용됩니다** - 디바이스 유형 구성을 해당 디바이스 유형 구성이 없는 그룹으로 가져오는 경우.
   - **<그룹 이름> 그룹에 대한 <디바이스 유형> 정책이 이미 있습니다. 기존 <디바이스 유형> 정책이 제거되고 가져온 정책이 적용됩니다** - 디바이스 유형 구성을 해당 디바이스 유형 구성이 있는 그룹으로 가져오는 경우.
   - **인벤토리 파일에 대한 종속성이 포함된 파일에서 정책을 가져올 수 없습니다. 이 가져오기를 허용하려면 정책 편집 창에서 가져오기 옵션을 사용합니다** - 인벤토리 파일에 대한 참조가 있는 파일에서 디바이스 유형 구성을 가져오는 경우.
7. **가져오기**를 클릭합니다.

   노트: 파일에서 정책을 가져올 때 참조 또는 잘못된 종속성이 있으면 가져오기가 실패하고 오류 메시지가 표시됩니다. 또한 가져올 파일에 참조 또는 종속성 파일이 있는 경우 해당 디바이스 유형의 **정책 편집** 페이지로 이동하여 그룹 정책을 가져옵니다.

노트: 파일을 사용하거나 한 그룹에서 다른 그룹으로 그룹 정책을 디바이스에서 사용자 그룹으로 또는 그 반대로 가져오거나 내보낼 수 있습니다. BIOS, 도메인 가입 등과 같은 지원되지 않는 구성은 사용자 그룹으로 구성을 가져올 때 무시됩니다.

결과

대상 그룹에 가져온 것과 동일한 디바이스 유형의 정책이 포함되어 있으면 해당 정책이 제거되고 새 정책이 추가됩니다.

노트: 그룹 정책을 가져오는 동안에는 암호를 가져오지 않습니다. 관리자는 모든 암호 필드에 암호를 다시 입력해야 합니다.

ThinOS 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **ThinOS**를 클릭합니다.
   ThinOS 구성 모드 선택 창이 표시됩니다.
4. 정책 설정을 구성하려면 원하는 모드를 선택합니다. 사용 가능한 모드는 다음과 같습니다.
   - 마법사 모드
   - 고급 구성 모드

   노트: ThinOS 고급 구성을 기본 모드로 설정하려면 확인란을 선택합니다.
5. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

   노트: 다음 설정을 변경하면 씬 클라이언트가 재부팅됩니다.
   - BIOS 설정
   - DP 오디오
   - 잭 팝업
   - 터미널 이름
   - 이더넷 속도
   - 디스플레이 변경 - 해상도, 회전, 새로 고침, 듀얼 디스플레이 및 다중 디스플레이
   - 시스템 모드 - VDI, Storefront 및 클래식
   - LPT 포트 바인딩

ThinOS - 마법사 모드

이 페이지를 사용하여 ThinOS 디바이스에 가장 자주 사용되는 매개변수를 구성합니다.

단계

1. 구성 모드로 **마법사**를 선택합니다.
2. 필요에 따라 옵션을 구성합니다.
3. **다음**을 클릭하여 다음 정책 설정으로 이동합니다.
4. 옵션을 구성한 후 **저장 및 게시**를 클릭합니다.

   노트: ThinOS 고급 구성 모드로 이동하려면 **계속**을 클릭합니다.

ThinOS - 고급 모드

이 페이지를 사용하여 ThinOS 디바이스에 대한 고급 정책 설정을 구성합니다.

단계

1. 구성 모드로 **고급 구성**을 선택합니다.
2. 필요에 따라 옵션을 구성합니다.
3. **저장 및 게시**를 클릭하여 구성을 저장하고 게시합니다.

   노트: **ThinOS** 페이지로 돌아가려면 **정책 제거**를 클릭합니다.

ThinOS 9.x 정책 설정 편집

전제조건

- 애플리케이션 패키지를 푸시할 디바이스에 대한 그룹 토큰이 있는 그룹을 생성합니다.
- Wyse Management Suite에 씬 클라이언트를 등록합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
   구성 제어 | ThinOS 창이 표시됩니다.

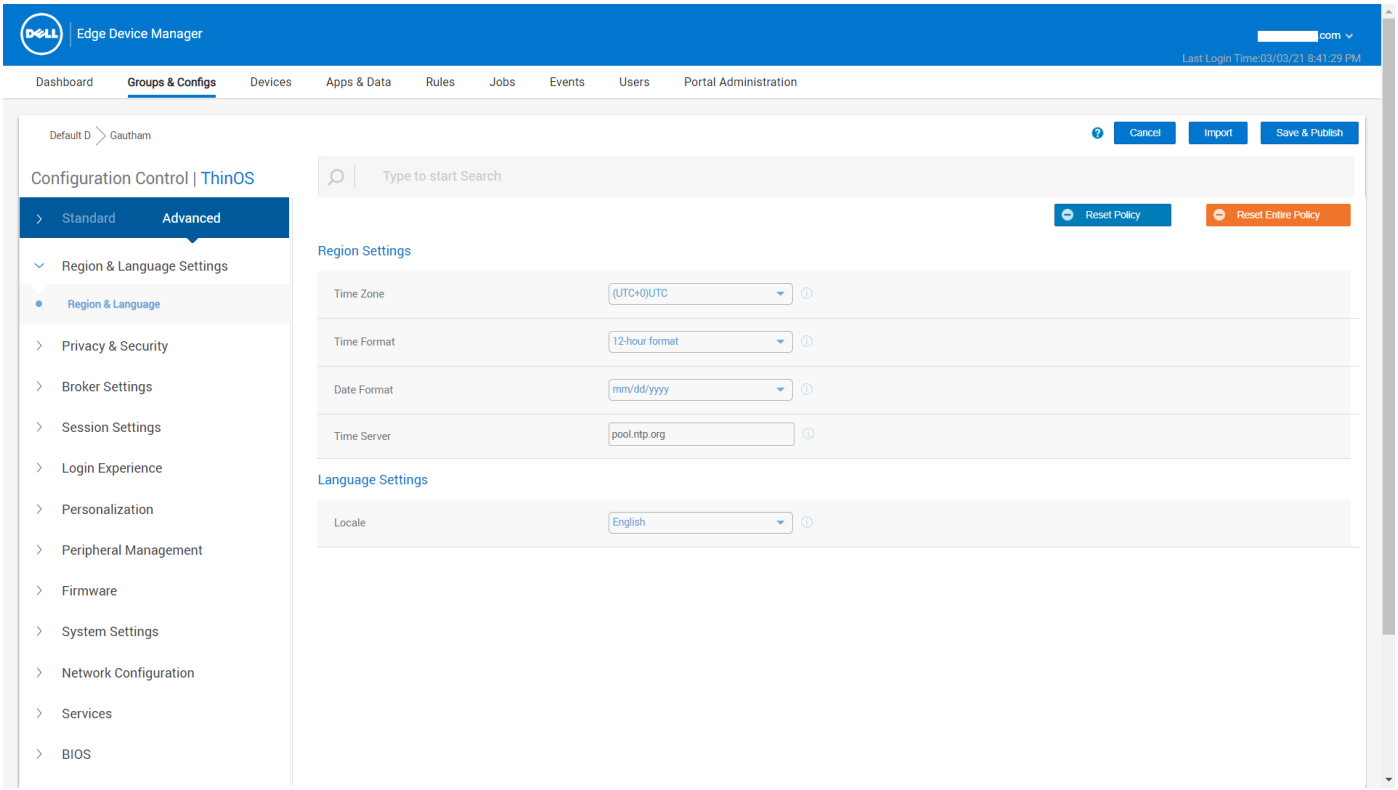


그림 5 . 구성 제어 | ThinOS

3. **고급** 또는 **표준** 옵션을 클릭합니다.
4. 구성하려는 옵션을 선택합니다.
5. 해당 필드에서 구성하려는 옵션을 클릭합니다.

   글로벌 검색 옵션을 사용하여 정책 설정에서 이용할 수 있는 관련 설정 또는 매개변수를 확인할 수 있습니다. 검색 결과에 다음 순서로 설정이 표시됩니다.
   - 설정
   - 매개변수 그룹
   - 매개변수 하위 그룹
   - 매개변수
6. 필요에 따라 옵션을 구성합니다.

노트: Wyse Management Suite 3.2에서 정책을 기본 구성으로 재설정하려면 **정책 재설정** 옵션을 클릭할 수 있습니다. 모든 구성을 지우려면 **전체 정책 재설정** 옵션을 클릭할 수도 있습니다.

7. **저장 및 게시**를 클릭합니다.

노트: ThinOS 구성의 변경 또는 업데이트에 대한 자세한 내용은 www.dell.com/support의 *ThinOS 9.x 관리자 가이드 및 릴리스 노트*를 참조하십시오.

노트: **저장 및 게시**를 클릭하면 구성된 설정이 **표준** 탭에도 표시됩니다.

노트: 펌웨어, 패키지, 배경 화면 등과 같은 참조 파일이 상위 그룹에 적용된 정책 구성(예: 기본 디바이스 그룹)은 기본적으로 하위 그룹에 적용됩니다. Wyse Management Suite 3.2에서 이러한 구성을 재정의하고 하위 그룹에서 제거할 수 있습니다.

노트: **구성 제어 | ThinOS** 창에서 10개의 인증서, 배경 화면 및 참조 파일만 업로드하고 배포할 수 있습니다.

ThinOS 9.x용 BIOS 구성

이 작업 정보

BIOS 구성 설정은 Wyse Management Suite 2.1을 사용하여 ThinOS 9.x 디바이스로 구성할 수 있습니다. **그룹 및 구성** 페이지를 사용하거나 서브넷 매핑 옵션을 사용하여 BIOS 패키지를 배포할 수 있습니다.

노트: 이 기능은 Wyse Management Suite Pro 라이선스에서만 사용할 수 있습니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
   구성 제어 | ThinOS 창이 표시됩니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
3. **고급**을 클릭합니다.
4. **BIOS** 필드에서 **플랫폼 선택**을 클릭하여 BIOS 설정을 구성할 플랫폼을 선택합니다.

Wyse Management Suite를 사용하여 ThinOS 9.x 이상 버전으로 업그레이드

전제조건

- 그룹 토큰으로 그룹을 생성해야 합니다. 이 그룹 토큰을 사용하여 ThinOS 9.x 디바이스를 등록합니다.
- 씬 클라이언트를 Wyse Management Suite에 등록해야 합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
   구성 제어 | ThinOS 창이 표시됩니다.
3. **고급**을 클릭합니다.
4. **펌웨어** 필드에서 **OS 펌웨어 업데이트**를 클릭합니다.
5. **찾아보기**를 클릭하여 펌웨어를 찾아 업로드합니다.
   패키지의 EULA 세부 정보와 공급업체 이름이 표시됩니다.
6. 파일을 선택하려면 **찾아보기**를 클릭하고 펌웨어가 있는 위치로 이동합니다.
   - EULA가 패키지에 포함된 경우 패키지의 EULA 세부 정보와 공급업체 이름이 표시됩니다. 공급업체 이름을 클릭하여 각 공급업체의 라이선스 계약을 읽을 수 있습니다. **수락**을 클릭하여 패키지를 업로드합니다. 여러 패키지를 업로드하면 각 패키지의 EULA 세부 정보가 표시됩니다. 패키지의 라이선스 계약에 개별적으로 동의해야 합니다.
   - EULA를 수락하지 않으면 펌웨어가 설치되지 않습니다.

   노트: 원격 리포지토리, 테넌트 클라우드 리포지토리 또는 운영자 클라우드 리포지토리에서 여러 펌웨어 패키지를 업로드하고 배포할 수 있습니다.

7. **배포할 ThinOS 펌웨어 선택** 드롭다운 메뉴에서 업로드된 펌웨어를 선택합니다.

   노트: 원격 리포지토리, 테넌트 클라우드 리포지토리 또는 운영자 클라우드 리포지토리에서 여러 펌웨어 패키지를 업로드하고 배포할 수 있습니다.

8. **저장 및 게시**를 클릭합니다.
   씬 클라이언트는 펌웨어를 다운로드하고 재시작됩니다. 펌웨어 버전이 업그레이드됩니다.

BIOS 패키지 업로드 및 푸시

전제조건

- Wyse Management Suite에서 그룹 토큰으로 그룹을 생성합니다. 이 그룹 토큰을 사용하여 ThinOS 9.x 디바이스를 등록합니다.
- Wyse Management Suite에 씬 클라이언트를 등록합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
   구성 제어 | ThinOS 창이 표시됩니다.
3. **고급**을 클릭합니다.
4. **펌웨어** 필드에서 **BIOS 펌웨어 업데이트**를 클릭합니다.
5. **배포할 ThinOS BIOS 선택** 드롭다운 메뉴에서 패키지를 선택합니다.

   노트: 원격 리포지토리, 테넌트 클라우드 리포지토리 또는 운영자 클라우드 리포지토리에서 여러 펌웨어 패키지를 업로드하고 배포할 수 있습니다. 테넌트 클라우드 리포지토리에서 10개의 패키지를 업로드할 수 있습니다.

6. **저장 및 게시**를 클릭합니다.
   씬 클라이언트가 재시작되고 애플리케이션 패키지가 설치됩니다.

   다음 단계에서 언급한 대로 Wyse Management Suite 2.1의 **앱 및 데이터**에서 BIOS 펌웨어를 업로드할 수도 있습니다.
   a. **앱 및 데이터** 페이지로 이동합니다.
   b. **OS 이미지 리포지토리**를 클릭하고 **ThinOS 9.x**를 선택합니다.
   c. 리포지토리에 추가할 파일을 찾아보고 추가하려면 **BIOS 파일 추가**를 클릭합니다.

      노트: 이 기능은 Wyse Management Suite Pro 라이선스에서만 사용할 수 있습니다.

그룹 및 구성을 사용하여 ThinOS 9.x 애플리케이션 패키지 업로드 및 푸시

전제조건

- 그룹 토큰으로 그룹을 생성해야 합니다. 이 그룹 토큰을 사용하여 ThinOS 9.x 디바이스를 등록합니다.
- Wyse Management Suite에 씬 클라이언트를 등록합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
   구성 제어 | ThinOS 창이 표시됩니다.
3. **고급**을 클릭합니다.
4. **펌웨어** 필드에서 **애플리케이션 패키지 업데이트**를 클릭합니다.
5. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
   - EULA가 패키지에 포함된 경우 패키지의 EULA 세부 정보와 공급업체 이름이 표시됩니다. 공급업체 이름을 클릭하여 각 공급업체의 라이선스 계약을 읽을 수 있습니다. **수락**을 클릭하여 패키지를 업로드합니다. 여러 패키지를 업로드하면 각 패키지의 EULA 세부 정보가 표시됩니다. 패키지의 라이선스 계약에 개별적으로 동의해야 합니다.
   - EULA가 패키지에 포함되어 있지 않은 경우 6단계로 이동합니다.

   노트: 원격 리포지토리, 테넌트 클라우드 리포지토리 또는 운영자 클라우드 리포지토리에서 여러 펌웨어 패키지를 업로드하고 배포할 수 있습니다.

6. **배포할 ThinOS 패키지 선택** 드롭다운 메뉴에서 패키지를 선택합니다.

7. **저장 및 게시**를 클릭합니다.
   씬 클라이언트가 재시작되고 애플리케이션 패키지가 설치됩니다.

Windows Embedded Standard 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **WES**를 클릭합니다.
   WES 페이지가 표시됩니다.
4. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

Windows Embedded 디바이스의 배포 설정 구성

Wyse Management Suite 3.1에서 Windows Embedded 디바이스의 배포 설정을 구성할 수 있습니다. 디바이스에 구성을 자동으로 배포하도록 설정을 구성할 수 있습니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **WES** 또는 **ThinLinux**를 클릭합니다.
3. **배포 설정**을 클릭합니다.
4. **이 항목 구성**을 클릭합니다.
5. 다음 옵션을 구성합니다.
   - **모든 알림 활성화/비활성화** - 이 옵션을 비활성화하면 모든 옵션과 알림이 비활성화됩니다.
   - **업데이트 알림 구성** - 이 옵션을 비활성화하면 디바이스에 구성 업데이트 대화 상자가 표시되지 않습니다.
   - **애플리케이션 업데이트 알림** - 이 옵션을 비활성화하면 애플리케이션 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **이미지 업데이트 알림** - 이 옵션을 비활성화하면 이미지 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **로그오프 알림** - 이 옵션을 비활성화하면 사용자가 디바이스에서 로그오프할 수 있도록 사용자 알림이 표시되지 않습니다.
   - **재부팅 알림** - 이 옵션을 비활성화하면 디바이스 재부팅 구성이 배포될 때 사용자 알림이 표시되지 않습니다.
   - **잠금 화면 표시** - 이 옵션을 비활성화하면 애플리케이션 및 이미지 업데이트 중에 잠금 화면이 표시되지 않습니다.

   노트: 기본적으로 모든 옵션이 활성화됩니다.

6. **저장 및 게시**를 클릭합니다.

Windows 10 IoT Enterprise에 대한 Edge 브라우저 설정 구성

Wyse Management Suite 3.3에서 Windows 10 IoT Enterprise에서 실행되는 씬 클라이언트에 대한 Edge 브라우저 설정을 구성할 수 있습니다.

전제조건

Wyse Management Suite 설정에서 Edge 브라우저 설정을 구성하려면 클라이언트에 Edge 브라우저를 설치해야 합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **WES**를 클릭합니다.
3. **원격 연결 Chromium 브라우저** 를 클릭합니다.
4. 필요에 따라 해당 필드에서 옵션을 구성합니다.
5. **저장 및 게시**를 클릭합니다.

   다음 표에는 **원격 연결 Chromium 브라우저** 창에서 구성할 수 있는 기능 세트가 나열되어 있습니다.

표 5. 원격 연결 Chromium 브라우저

필드 이름	옵션
원격 연결 Chromium 브라우저	연결 이름
	로그온 시 자동 시작
	URL
	시작 시
즐겨찾기	즐겨찾기, 신뢰할 수 있는 사이트 및 바로 가기 추가
	이 영역의 모든 사이트에 대하여 서버 확인(https:)을 요구
개인 정보	추적 금지 요청
	추적 방지
표시	홈 버튼
	즐겨찾기 모음
	수집 버튼
	사용자 피드백 버튼
	공유 버튼
시스템	하드웨어 가속

Linux 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **Linux**를 클릭합니다.
4. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

ThinLinux 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **ThinLinux**를 클릭합니다.
4. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

ThinLinux 디바이스의 배포 설정 구성

Wyse Management Suite 3.1에서 ThinLinux 디바이스의 배포 설정을 구성할 수 있습니다. 디바이스에 구성을 자동으로 배포하도록 설정을 구성할 수 있습니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinLinux**를 클릭합니다.
3. **배포 설정**을 클릭합니다.

4. **이 항목 구성**을 클릭합니다.
5. 다음 옵션 중에서 구성합니다.
   - **모든 알림 활성화/비활성화** - 이 옵션을 비활성화하면 모든 옵션과 알림이 비활성화됩니다.
   - **업데이트 알림 구성** - 이 옵션을 비활성화하면 디바이스에 구성 업데이트 대화 상자가 표시되지 않습니다.
   - **애플리케이션 업데이트 알림** - 이 옵션을 비활성화하면 애플리케이션 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **이미지 업데이트 알림** - 이 옵션을 비활성화하면 이미지 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **로그오프 알림** - 이 옵션을 비활성화하면 사용자가 디바이스에서 로그오프할 수 있도록 사용자 알림이 표시되지 않습니다.
   - **재부팅 알림** - 이 옵션을 비활성화하면 디바이스 재부팅 구성이 배포될 때 사용자 알림이 표시되지 않습니다.
   - **잠금 화면 표시** - 이 옵션을 비활성화하면 애플리케이션 및 이미지 업데이트 중에 잠금 화면이 표시되지 않습니다.

   노트: 기본적으로 모든 옵션이 활성화됩니다.
6. **저장 및 게시**를 클릭합니다.

Wyse 소프트웨어 씬 클라이언트 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **Wyse 소프트웨어 씬 클라이언트**를 클릭합니다.
   Wyse 소프트웨어 씬 클라이언트 페이지가 표시됩니다.
4. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

클라우드 연결 정책 설정 편집

단계

1. **그룹 및 구성**을 클릭합니다.
   그룹 및 구성 페이지가 표시됩니다.
2. **정책 편집** 드롭다운 메뉴를 클릭합니다.
3. **클라우드 연결**을 클릭합니다.
4. 정책 설정을 구성한 후 **저장 및 게시**를 클릭합니다.

Dell Hybrid Client 정책 설정 편집

전제조건

- 애플리케이션 패키지를 푸시할 디바이스에 대한 그룹 토큰이 있는 그룹을 생성합니다.
- Wyse Management Suite에 Dell Hybrid Client를 등록합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **하이브리드 클라이언트**를 클릭합니다.
   구성 제어 | 하이브리드 클라이언트 창이 표시됩니다.
3. **고급** 옵션을 클릭합니다.
4. 구성하려는 옵션을 선택합니다.
5. 해당 필드에서 설정을 클릭하고 필요에 따라 옵션을 구성합니다.

   노트: Wyse Management Suite 3.2에서 정책을 기본 구성으로 재설정하려면 **정책 재설정** 옵션을 클릭할 수 있습니다. 모든 구성을 지우려면 **전체 정책 재설정** 옵션을 클릭할 수도 있습니다.
6. **저장 및 게시**를 클릭합니다.

노트: **저장 및 게시**를 클릭하면 구성된 설정이 **표준** 탭에도 표시됩니다.

다음 표에는 **구성 제어 | 하이브리드 클라이언트** 창에서 구성할 수 있는 기능 세트가 나열되어 있습니다.

표 6. 하이브리드 클라이언트 정책 설정

기능	하위 기능 - 사용자 정책 그룹	하위 기능 - 디바이스 정책 그룹
주변 기기 관리	디스플레이 설정	디스플레이 설정
	프린터	프린터
	오디오	오디오
	마우스	마우스
	키보드	키보드
네트워크 구성	무선	무선
		프록시
		Bluetooth
브라우저 설정	Google Chrome 설정	브라우저 바로 가기
	Firefox 설정	
	브라우저 바로 가기	
	기본 브라우저	
지역 및 언어 설정	지역	지역
		시간 서버
		언어
개인화	데스크탑	데스크탑
		디바이스 정보
사인온	적용되지 않음	도메인 연결
		이전에 로그인한 사용자 목록
개인 정보 보호 및 보안	적용되지 않음	인증서
		게스트 사용자 계정 속성
		USB Lockdown
		GRUB 암호
		Bremen 암호
		VNC 서버
		SSH 서버
전원 설정	절전	절전
	일시 중단 및 전원 버튼	일시 중단 및 전원 버튼
Citrix Workspace	Citrix 브로커 세션	Citrix 브로커 세션
	Citrix 전역 설정	Citrix 전역 설정
VMware ViewClient	VMware ViewClient 브로커 세션	VMware ViewClient 브로커 세션
	VMware 전역 설정	VMware 전역 설정
RDP	RDP 브로커 세션	RDP 브로커 세션
Dell Hybrid Client 모드	Dell Hybrid Client 모드	Dell Hybrid Client 모드
WMS 설정	적용되지 않음	WMS 클라이언트 설정

표 6. 하이브리드 클라이언트 정책 설정 (계속)

기능	하위 기능 - 사용자 정책 그룹	하위 기능 - 디바이스 정책 그룹
		배포 설정
애플리케이션 보안	VLC 미디어 플레이어	VLC 미디어 플레이어
	이미지 뷰어	이미지 뷰어
	Libre Office	Libre Office
네트워크 드라이브	네트워크 드라이브 목록	네트워크 드라이브 목록
BIOS	적용되지 않음	플랫폼 선택: • DHC 3090 • DHC 3320 • DHC 5070 • DHC 7070 • DHC 7090

노트: Dell Hybrid Client 구성의 변경 또는 업데이트에 대한 자세한 내용은 www.dell.com/support 의 *Dell Hybrid Client 관리자 가이드 및 릴리스 노트*를 참조하십시오.

노트: 배경 화면, 인증서, 광고 로고 파일과 같은 리소스 파일 이름에 특수 문자를 사용하거나 공백을 추가하지 마십시오.

Dell Hybrid Client 구성 방법에 대한 자세한 내용은 www.dell.com/support의 *Dell Hybrid Client 관리자 가이드*를 참조하십시오.

Dell Hybrid Client에 대한 Wyse Management Suite 클라이언트 설정 구성

관리자는 Dell Hybrid Client 구성과 관련하여 Wyse Management Suite 에이전트 동작을 구성할 수 있습니다. 관리자는 업무 시간 이외의 시간에 구성을 적용하도록 디바이스를 구성할 수도 있습니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **하이브리드 클라이언트**를 클릭합니다.
   구성 제어 | 하이브리드 클라이언트 창이 표시됩니다.
3. **표준** 옵션을 클릭합니다.
4. **WMS 설정** > **WMS 클라이언트 설정**으로 이동합니다.
5. 디바이스 그룹의 업무 시간 및 영업일을 구성하려면 **업무 시간** 필드에서 **행 추가**를 클릭하고 **영업일** 드롭다운 메뉴에서 요일을 클릭합니다.
6. 에이전트가 사용자 세션을 보고할 수 있도록 하려면 **세션 보고 활성화** 옵션을 활성화하고 **보고서 세션** 드롭다운 메뉴에서 타이밍을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
   - **실행 시 사용자 세션 전송** - Dell Client Agent는 사용자가 디바이스에서 로그오프할 때마다 사용자 세션 보고서를 보냅니다.
   - **체크인 시 사용자 세션 전송** - Dell Client Agent는 8시간마다 사용자 세션 보고서를 보냅니다.
   - **업무 시간 이외의 시간에 사용자 세션 전송** - Dell Client Agent는 5단계에서 구성한 업무 시간 이외의 시간에 사용자 세션 보고서를 보냅니다.
7. 사용자 수준 구성을 기반으로 모든 디바이스에 구성을 배포하려면 **사용자 개인 설정 로밍 활성화** 옵션을 활성화합니다. 이 옵션이 활성화된 경우 사용자가 Google Chrome 브라우저 데이터, Firefox 브라우저 데이터, 데스크탑 맞춤 구성, 맞춤 구성 배경 화면, 브라우저 애플리케이션 상태, 클라우드 데이터 및 VDI 세션 세부 정보와 같은 디바이스에서 구성한 설정이 Wyse Management Suite 서버에 저장됩니다. 이러한 구성은 사용자가 다른 디바이스에 로그인할 때 자동으로 적용됩니다. 구성된 설정이 다른 모든 구성보다 우선합니다. 또한 이 설정은 사용자 정책 그룹에서 구성할 수 있습니다.
8. 디바이스에서 알림을 활성화하려면 **푸시 알림 활성화** 옵션을 활성화합니다. 이 옵션을 활성화하면 **저장 및 게시**를 클릭한 직후 구성된 설정이 적용됩니다. 이 옵션을 비활성화하면 디바이스가 하트비트 신호를 보낼 때 구성이 적용됩니다.

   노트: 이 옵션을 비활성화하면 Wyse Management Suite가 Dell Hybrid Client로 푸시 알림을 보내지 않으므로 애플리케이션 배포에서 오류 상태로 전환될 수 있습니다.

9. 지정된 업무 시간 이외의 시간에 구성을 적용하려면 드롭다운 메뉴에서 옵션을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
   - **즉시** - 이 옵션을 선택하면 **저장 및 게시**를 클릭한 직후 설정이 적용됩니다.
   - **지정된 업무 시간 이외의 시간** - 이 옵션을 선택하면 5단계에서 구성된 업무 시간 이외의 시간에 구성이 적용됩니다.
   - **일정 기간 동안 디바이스에 로그인한 사용자가 없는 경우** - 이 옵션을 선택하면 정의된 시간 동안 디바이스에 로그인한 사용자가 없을 때 구성이 적용됩니다. 구성이 디바이스에 적용된 후 유휴 시간을 지정할 수 있습니다.

   노트: 디바이스 페이지에서 특정 디바이스에 대해 이러한 설정을 구성할 수도 있습니다. 자세한 내용은 디바이스 수준 정책 구성을 참조하십시오.

10. 사용자 구성을 저장하고 여러 디바이스에 배포하려면 **사용자 데이터 로밍** 옵션을 활성화합니다. 지정된 기능을 수행한 후, 설정을 선택한 리포지토리에 저장하거나 저장해야 하는 구성을 리포지토리에 저장하도록 구성할 수 있습니다. 이 구성은 Dell Hybrid Client 버전 1.5 이상에서 지원됩니다.
11. Dell Hybrid Client 디바이스가 Wyse Management Suite에 체크인한 후 Dell 서명 애플리케이션의 자동 업데이트를 활성화하려면 **자동 업데이트** 옵션을 활성화합니다. Wyse Management Suite 리포지토리의 애플리케이션 패키지 버전이 Dell Hybrid Client 기반 디바이스에 설치된 버전보다 높을 경우 애플리케이션이 자동으로 업데이트됩니다. 애플리케이션을 선택하고 자동 업데이트를 수행해야 하는 빈도를 구성할 수도 있습니다.

    노트: Dell Hybrid Client 지원 디바이스를 켜야 디바이스에 구성을 적용할 수 있습니다.

12. Dell Client Agent 로그에 대해 디버그 모드를 활성화하려면 **지원 모드** 옵션을 활성화합니다.

Dell Hybrid Client 디바이스의 배포 설정 구성

Wyse Management Suite 3.1에서 Dell Hybrid Client 디바이스의 배포 설정을 구성할 수 있습니다. 디바이스에 구성을 자동으로 배포하도록 설정을 구성할 수 있습니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **하이브리드 클라이언트**를 클릭합니다.
3. **WMS 설정** > **배포 설정**으로 이동합니다.
4. 다음 옵션 중에서 구성합니다.
   - **업데이트 알림 구성** - 이 옵션을 비활성화하면 디바이스에 구성 업데이트 대화 상자가 표시되지 않습니다.
   - **애플리케이션 업데이트 알림** - 이 옵션을 비활성화하면 애플리케이션 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **이미지 업데이트 알림** - 이 옵션을 비활성화하면 이미지 정책을 배포할 때 사용자 알림이 표시되지 않습니다.
   - **로그오프 알림** - 이 옵션을 비활성화하면 사용자가 디바이스에서 로그오프할 수 있도록 사용자 알림이 표시되지 않습니다.
   - **재부팅 알림** - 이 옵션을 비활성화하면 디바이스 재부팅 구성이 배포될 때 사용자 알림이 표시되지 않습니다.
   - **잠금 화면 표시** - 이 옵션을 비활성화하면 애플리케이션 및 이미지 업데이트 중에 잠금 화면이 표시되지 않습니다.

   노트: 모든 옵션 및 알림을 활성화하려면 **모든 알림 활성화/비활성화** 옵션을 활성화할 수 있습니다.

   노트: 업데이트 알림 구성 및 **잠금 화면 표시**는 기본적으로 비활성화되어 있습니다.

5. **저장 및 게시**를 클릭합니다.

Dell Generic Client 정책 설정 편집

전제조건

- 디바이스에 대한 그룹 토큰을 사용하여 그룹을 생성합니다.
- Wyse Management Suite에 Dell Generic Client를 등록합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **일반 클라이언트**를 클릭합니다.
   구성 제어 | 일반 클라이언트 창이 표시됩니다.
3. **고급** 옵션을 클릭합니다.

4. 구성하려는 옵션을 선택합니다.
5. 해당 필드에서 설정을 클릭하고 필요에 따라 옵션을 구성합니다.

   노트: Wyse Management Suite 3.2에서 정책을 기본 구성으로 재설정하려면 **정책 재설정** 옵션을 클릭할 수 있습니다.

6. **저장 및 게시**를 클릭합니다.

   노트: **저장 및 게시**를 클릭하면 구성된 설정이 **표준** 탭에도 표시됩니다.

   다음 표에는 **구성 제어 | 일반 클라이언트** 창에서 구성할 수 있는 기능 세트가 나열되어 있습니다.

표 7. 일반 클라이언트 정책 설정

기능	하위 기능 - 사용자 정책 그룹	하위 기능 - 디바이스 정책 그룹
개인 정보 보호 및 보안	인증서	인증서
에이전트 로깅 수준	로깅 수준	로깅 수준

대량 디바이스 예외 파일 생성 및 가져오기

Wyse Management Suite 3.1에서 여러 ThinOS 9.x 디바이스에 디바이스 예외 구성을 배포할 수 있습니다.

단계

1. 대량 디바이스 예외 파일을 생성합니다. 파일을 생성하려면 다음 중 하나를 수행합니다.
   - 테스트 그룹에 대한 그룹 정책을 생성한 다음 해당 정책을 파일로 내보냅니다. 구성에 암호가 포함되어 있으면 내보낸 파일에서 *로 대체됩니다. 예를 들어, 다음과 같습니다.

```
{
    "WMSVersion": "4.6.8",
    "exportedDate": "1581466633677",
    "deviceTypes": [
        {
            "type": 6,
            "configurations": {
                "version": "0.0.1",
                "sequence": 1581466506281,
                "parameters": {
                    "AdminModeUsername": {
                        "value": "admin",
                        "updatedAt": "1581466506234"
                    },
                    "AdminModePassword": {
                        "value": "********",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalName": {
                        "value": "outpatient",
                        "updatedAt": "1581466506234"
                    },
                    "TimeServer": {
                        "value": "10.10.10.10",
                        "updatedAt": "1581466506234"
                    },
                    "timeZone": {
                        "value": "America/Phoenix",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalNameCapital": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    },
                    "DeviceNICDefault": {
                        "value": "Wlan",
                        "updatedAt": "1581466506234"
                    },
                    "AdminMode": {
```

```
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    }
                }
            }
        }
    ]
}
```

- 다음 형식을 사용하여 .json 파일을 생성합니다.

```
{

"devices": {

<serialnumber>: {

"parameters": {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

},

configurations: [<configuration name>]

}

}

"configurations": {

<configurationName>: {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

  }

}

}
```

예를 들면, 다음과 같습니다.

```
{
    "devices": {
        "9EPDL900051": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 5 - Floor 3"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
```

```
            },
            configurations: ["westWingExceptions"]
        },
        "5LGDO600108": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 15 - Floor 2"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
            },
            configurations: ["westWingExceptions"]
        }
    },
    "configurations": {
        "westWingExceptions": {
            "DeviceNICDefault": {
                "value": "Wlan"
            },
            "timeZone": {
                "value": "America/Phoenix"
            },
            "TimeServer": {
                "value": "10.10.10.10"
            },
            "TerminalNameCapital": {
                "value": "yes"
            },
            "AdminMode": {
                "value": "yes"
            },
            "AdminModeUsername": {
                "value": "admin"
            },
            "AdminModePassword": {
                "value": "password"
            }
        }
    }
}
```

2. 파일을 압축하고 암호화합니다.

   노트: 7-zip 소프트웨어를 사용하여 파일을 압축하고 암호화할 수 있습니다.

   노트: 파일 크기가 1MB를 초과해서는 안 됩니다.

3. **그룹 및 구성**으로 이동하여 **정책 가져오기**를 클릭합니다.
   정책 가져오기 마법사 화면이 표시됩니다.
4. **대량 디바이스 예외**를 선택합니다.
5. **찾아보기**를 클릭하고 암호가 암호화된 .zip 파일을 선택합니다.
6. **다음**을 클릭합니다.
   가져올 디바이스 유형 구성 선택 페이지가 표시됩니다.
7. **다음**을 클릭합니다.

   노트: ThinOS 9.x 디바이스에 대한 디바이스 예외 파일을 대량으로 가져올 수 있으므로 페이지에서 옵션을 구성할 수 없습니다.

8. .json 파일을 압축하는 데 사용된 .zip 파일 암호를 입력합니다.
9. **다음**을 클릭합니다.
   대량 디바이스 예외 가져오기에 대한 요약이 표시됩니다.
10. **가져오기**를 클릭합니다.
    구성을 가져오면 다운로드할 수 있는 **그룹 및 구성** 페이지에 보고서 생성 링크가 생성됩니다. **그룹 및 구성** 페이지에 성공 메시지가 표시됩니다.

    노트: 디바이스가 등록되지 않고 구성을 가져오는 경우, 향후 30일 이내에 디바이스가 사전 로드된 일련 번호 디바이스 중 하나에 등록한 경우에만 이 디바이스에 예외가 적용됩니다.

노트: 디바이스가 이미 등록되어 있고 디바이스 일련번호를 사용하여 구성을 가져오는 경우 디바이스에 디바이스 예외가 적용됩니다.

노트: 가져온 파일은 암호로 보호됩니다. AES-256 및 ZipCrypto 암호화가 지원됩니다.

노트: 인증서, 배경 화면, 로고 등과 그와 연결된 리소스가 있는 구성은 가져오지 않습니다.

8

디바이스 관리

이 섹션에서는 관리 콘솔을 사용하여 일상적인 디바이스 관리 작업을 수행하는 방법을 설명합니다. 디바이스 인벤토리를 찾으려면 **디바이스** 탭을 클릭합니다. 그룹 또는 하위 그룹, 디바이스 유형, 운영 체제 유형, 상태, 서브넷, 플랫폼, 시간대 등 다양한 필터 조건을 사용하여 디바이스의 하위 집합을 볼 수 있습니다.

다음을 기준으로 디바이스 목록을 정렬할 수 있습니다.

- 유형
- 플랫폼
- 운영 체제 버전
- 일련 번호
- IP 주소
- 마지막 사용자 세부 정보
- 그룹 세부 정보
- 마지막 체크인 시간
- 등록 상태
- 쓰기 필터 상태

특정 디바이스의 **디바이스 세부 정보** 페이지를 보려면 페이지에 나열된 디바이스 항목을 클릭합니다. 디바이스의 모든 구성 매개변수와 각 매개변수가 적용되는 그룹 수준이 **디바이스 세부 정보** 페이지에 표시됩니다.

디바이스에 고유한 구성 매개변수를 설정할 수 있습니다. 이 섹션에서 구성된 매개변수는 그룹 및/또는 전역 수준에서 구성된 모든 매개변수를 재정의합니다.

노트: Wyse Management Suite 3.2에서는 **디바이스** 페이지에서 디바이스 세부 정보를 CSV 파일로 내보낼 수 없습니다. 세부 정보를 내보내려면 **포털 관리** > **보고서** > **보고서 생성**으로 이동하고 **유형** 드롭다운 목록의 **디바이스** 범주 아래에서 옵션을 선택해야 합니다.

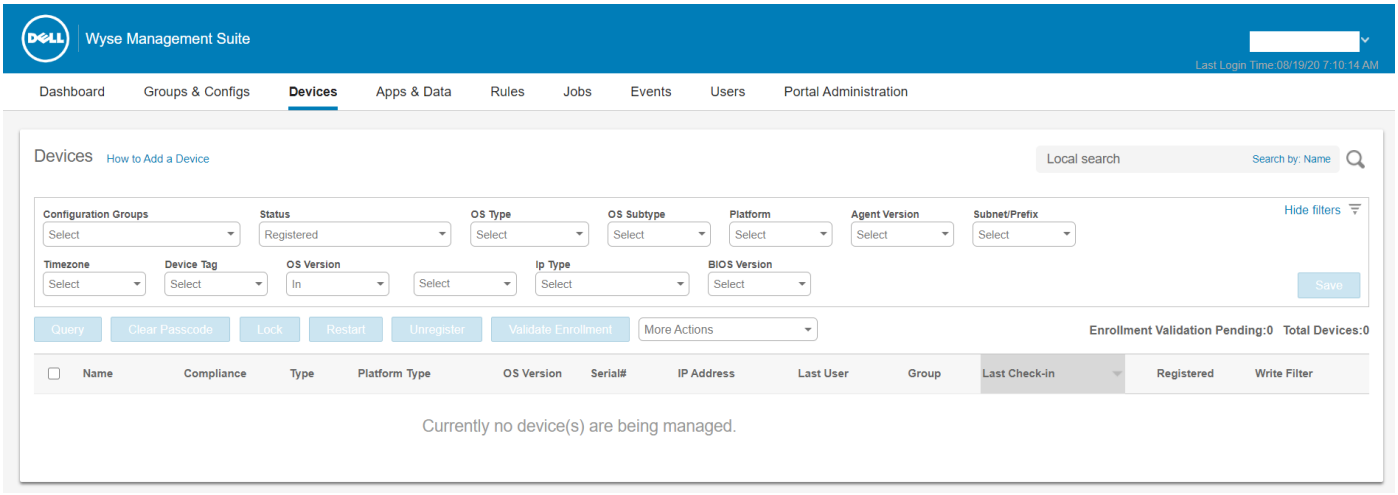


그림 6 . 디바이스 페이지

주제:

- Wyse Management Suite에 디바이스를 등록하는 방법
- 필터를 사용하여 디바이스 검색
- 디바이스 페이지에서 필터 저장
- 디바이스 상태 쿼리
- 디바이스 잠금
- 디바이스 재시작
- 디바이스 등록 취소

- 등록 유효성 검사
- 디바이스를 출고 시 기본 설정으로 재설정
- 디바이스 페이지에서 그룹 할당 변경
- 디바이스로 메시지 전송
- Wake On LAN 명령
- 디바이스 세부 정보 보기
- 디스플레이 매개변수 보기
- 가상 NIC 세부 정보 보기
- BIOS 세부 정보 보기
- 디바이스 요약 관리
- 시스템 정보 보기
- 디바이스 이벤트 보기
- 설치된 애플리케이션 보기
- 씬 클라이언트 이름 바꾸기
- 원격 섀도 연결 활성화
- Dell Hybrid Client 디바이스에 대한 원격 섀도 연결 구성
- 디바이스 종료
- 디바이스 태그 지정
- 디바이스 규정 준수 상태
- Windows Embedded Standard 또는 ThinLinux 이미지 가져오기
- 로그 파일 요청
- 디바이스 문제 해결
- Dell Hybrid Client를 이미지로 다시 설치
- Dell Generic Client를 하이브리드 클라이언트로 변환
- Dell Hybrid Client용 구성 사용자 인터페이스 패키지 가져오기
- Dell Hybrid Client를 출고 시 설정으로 재설정
- 디바이스의 대량 그룹 변경

Wyse Management Suite에 디바이스를 등록하는 방법

다음 방법 중 하나를 사용하여 Wyse Management Suite에 씬 클라이언트를 등록할 수 있습니다.

- 디바이스의 WDA(Wyse Device Agent)에서 제공하는 사용자 인터페이스를 통해 수동으로 등록합니다.
- DHCP 서버에서 적절한 옵션 태그를 구성하여 자동으로 등록합니다.
- DNS 서버에서 적절한 DNS SRV 레코드를 구성하여 자동으로 등록합니다.

노트:

- 퍼블릭 클라우드의 경우 Wyse Management Suite URL 및 디바이스를 등록할 그룹에 대한 그룹 토큰을 제공하여 씬 클라이언트를 등록합니다.
- 프라이빗 클라우드의 경우 Wyse Management Suite URL 및 그룹 토큰(이 디바이스를 등록할 그룹에 대한 선택 사항)을 제공하여 씬 클라이언트를 등록합니다. 그룹 토큰이 제공되지 않는 경우 관리되지 않는 그룹에 디바이스가 등록됩니다.

Dell Hybrid Client 수동 등록

전제조건

디바이스를 등록하기 전에 디바이스가 네트워크에 연결되어 있어야 Wyse Management Suite 서버에 연결할 수 있습니다.

노트: 게스트 사용자 계정에서만 디바이스를 등록할 수 있습니다. 게스트 사용자는 개발 모드에서만 Wyse Management Suite에서 디바이스 등록을 취소할 수 있습니다. 도메인 사용자는 Wyse Management Suite에서 디바이스 등록을 취소할 수 없습니다.

단계

1. Dell Hybrid Client에 게스트 사용자로 로그인합니다. 기본적으로 사용자 이름은 **quest**입니다.
2. 위쪽 표시줄에서 을 클릭합니다.
3. **Dell Client Agent**를 클릭합니다.

Dell Client Agent 창이 표시됩니다.

4. **등록**을 클릭합니다.
   기본 상태가 **검색 진행 중**으로 표시됩니다.
5. 수동으로 종료하려면, **취소** 버튼을 클릭합니다.
6. **WMS 서버** 필드에 Wyse Management Suite 서버의 URL을 입력합니다.
7. **그룹 토큰** 필드에 그룹 등록 키를 입력합니다. 그룹 토큰은 디바이스를 그룹에 직접 등록할 수 있는 고유한 키입니다.

   노트: 테넌트 및 그룹 필드가 비어 있으면 디바이스가 관리되지 않는 그룹에 등록됩니다. 그러나 디바이스를 퍼블릭 클라우드에 등록하려면 그룹 토큰이 필요합니다.

8. **서버 인증서 CA 유효성 검사** 옵션을 활성화하거나 비활성화하려면 **켜기/끄기** 버튼을 클릭합니다. 모든 디바이스 대 서버 통신에 대한 서버 인증서 유효성을 검사하려면 이 옵션을 활성화합니다.

   CA 유효성 검사 옵션은 자동으로 활성화되며 퍼블릭 클라우드 URL을 입력하면 비활성화할 수 없습니다.
9. **등록**을 클릭하여 Wyse Management Suite 서버에 디바이스를 등록합니다.

   디바이스가 성공적으로 등록되면 상태가 **등록 상태** 레이블 옆에 녹색 체크 표시가 있는 **등록됨**으로 표시됩니다. **등록** 버튼의 캡션이 **등록 취소**로 변경됩니다.

   노트: 관리자 또는 게스트 사용자는 **Dell Client Agent** 창에서 직접 디바이스 등록을 취소할 수 없습니다. 디바이스 등록을 취소하려면 개발 모드로 들어가거나 Wyse Management Suite 콘솔을 사용해야 합니다.

수동 검색 방법을 사용하여 Dell Generic Client 등록

수동 검색 방법을 사용하여 Ubuntu 버전 18.04 또는 20.04 LTS 64비트를 실행하는 Dell Ubuntu 디바이스(예: OptiPlex 3090 Ultra, OptiPlex 7090 Ultra, OptiPlex 7070 Ultra 및 Latitude 3320)를 Dell Client Agent-Enabler 에이전트를 활용해 Wyse Management Suite에 등록할 수 있습니다.

단계

1. 다음 템플릿을 사용하여 reg.json 파일을 작성합니다.

```
{"ccm":
{"ccmserver":"WMSServerURL.Domain.com","ccmport":"443","usessl":"true","mqttserver":"
WMSServerURL.Domain.com
","mqttport":"1883","grouptoken":"GroupToken","isCaValidationOn":"false"}}
```

2. reg.json 파일을 `/etc/dcae/config`에 복사합니다.
3. 디바이스를 다시 시작합니다.

   노트: Dell Ubuntu 디바이스는 DCA-Enabler 버전이 1.1.0-17 이하일 경우 Dell Hybrid Client로 Wyse Management Suite에 등록됩니다. DCA-Enabler 버전이 1.2.0-xx 이상인 경우 디바이스는 Dell Generic Client로 등록됩니다.

수동 검색 방법을 사용하여 Dell Hybrid Client 등록

Dell Client Agent Enabler 에이전트를 사용하여 Ubuntu 버전 18.04 LTS 64비트를 실행하는 OptiPlex 7070 Ultra 디바이스를 수동 검색 방법을 사용하여 Wyse Management Suite에 등록할 수 있습니다.

단계

1. 다음 템플릿을 사용하여 reg.json 파일을 작성합니다.

```
{"ccm":
{"ccmserver":"WMSServerURL.Domain.com","ccmport":"443","usessl":"true","mqttserver":"
WMSServerURL.Domain.com
","mqttport":"1883","grouptoken":"GroupToken","isCaValidationOn":"false"}}
```

2. reg.json 파일을 `/etc/dcae/config`에 복사합니다.
3. 디바이스를 다시 시작합니다.

Wyse Device Agent를 사용하여 ThinOS 디바이스 등록

ThinOS 디바이스를 수동으로 등록하려면 다음을 수행합니다.

단계

1. 씬 클라이언트의 데스크탑 메뉴에서 **시스템 설정** > **중앙 구성**으로 이동합니다.
   중앙 구성 창이 표시됩니다.
2. **WDA** 탭을 클릭합니다. WDA 서비스는 클라이언트 부팅 프로세스가 완료된 후 자동으로 실행됩니다.

   기본적으로 **WMS**가 선택되어 있습니다.

3. Wyse Management Suite를 활성화하려면 **Wyse Management Suite 활성화** 확인란을 선택합니다.
4. 관리자가 원하는 그룹에 대해 구성한 대로 **그룹 등록 키**를 입력합니다.
5. **WMS 고급 설정 활성화** 옵션을 선택하고 WMS 서버 또는 MQTT 서버 세부 정보를 입력합니다.
6. 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.

   노트:
   - CA 유효성 검사를 비활성화하면 경고 메시지가 표시됩니다. 확인을 클릭하여 확인해야 합니다.
   - 미국 데이터 센터의 Wyse Management Suite 퍼블릭 클라우드 버전의 경우 기본 WMS 서버 및 MQTT 서버 세부 정보를 변경하지 마십시오. 유럽 데이터 센터의 Wyse Management Suite 퍼블릭 클라우드 버전의 경우 다음을 사용하십시오.
     - CCM 서버—eu1.wysemanagementsuite.com
     - MQTT 서버—eu1-pns.wysemanagementsuite.com:1883
   - 서버 주소에 http가 포함된 경우 경고 메시지가 표시됩니다. 확인을 클릭하여 확인해야 합니다.

7. 설정을 확인하려면 **키 유효성 검사**를 클릭합니다. 키가 확인되면 디바이스가 자동으로 다시 시작됩니다.

   노트: 키가 확인되지 않은 경우 입력한 그룹 키와 WMS 서버 URL을 확인합니다. 포트 443과 1883이 네트워크에 의해 차단되지 않았는지 확인합니다.

8. **확인**을 클릭합니다.
   디바이스가 Wyse Management Suite에 등록됩니다.

Wyse Device Agent를 사용하여 Wyse Management Suite에 Windows Embedded Standard 씬 클라이언트 등록

전제조건

디바이스를 등록하려면 Wyse Management Suite에서 그룹을 생성합니다.

단계

1. Wyse Device Agent 애플리케이션을 엽니다.
   Wyse Device Agent 화면이 표시됩니다.
2. **Management Server** 드롭다운 목록에서 **Wyse Management Suite**를 선택합니다.
3. 해당 필드에 서버 주소와 포트 번호를 입력합니다.

   노트: 서버 주소에 **http**가 포함된 경우 경고 메시지가 표시됩니다. **확인**을 클릭하여 확인합니다.

4. 그룹 토큰을 입력합니다. 단일 테넌트에서 그룹 토큰은 선택적 단계입니다.

   노트: **그룹 토큰** 필드에 입력된 그룹 토큰은 일반 텍스트로 표시되지 않습니다.

5. 라이선스 유형에 따라 CA 유효성 검사를 활성화 또는 비활성화합니다.

노트: CA 유효성 검사를 비활성화하면 경고 메시지가 표시됩니다. **확인**을 클릭하여 확인합니다.

6. **등록**을 클릭합니다.

Wyse Device Agent를 사용하여 Wyse Management Suite에 Wyse 소프트웨어 씬 클라이언트 등록

전제조건

Wyse Management Suite에 디바이스를 등록하려면 그룹을 생성합니다.

단계

1. **Wyse Device Agent** 애플리케이션을 엽니다.
   Wyse Device Agent 창이 표시됩니다.
2. 디바이스 등록 세부 정보를 입력합니다.
3. **관리 서버** 드롭다운 목록에서 **Wyse Management Suite**를 선택합니다.
4. 해당 필드에 서버 주소와 포트 번호를 입력합니다.

   노트: 서버 주소에 **http**가 포함된 경우 경고 메시지가 표시됩니다. **확인**을 클릭하여 확인합니다.

5. 그룹 토큰을 입력합니다. 단일 테넌트에서 그룹 토큰은 선택적 단계입니다.
6. 라이선스 유형에 따라 CA 유효성 검사를 활성화 또는 비활성화합니다.

   노트: CA 유효성 검사를 비활성화하면 경고 메시지가 표시됩니다. **확인**을 클릭하여 확인합니다.

7. **등록**을 클릭합니다.
   등록이 완료되면 **Wyse Management Suite에 등록되었습니다** 메시지가 표시됩니다.

Wyse Device Agent를 사용하여 ThinLinux 씬 클라이언트 등록

전제조건

디바이스를 등록하려면 Wyse Management Suite에서 그룹을 생성합니다.

단계

1. Wyse Device Agent 애플리케이션을 엽니다.
   Wyse Device Agent 화면이 표시됩니다.
2. 디바이스 등록 세부 정보를 입력합니다.
3. Wyse Management Suite에서 Wyse Management Suite 서버 세부 정보를 입력합니다.
4. 그룹 토큰을 입력합니다.
   단일 테넌트에서 그룹 토큰은 선택적 단계입니다.
5. **등록**을 클릭합니다.
   등록이 완료되면 확인 메시지가 표시됩니다.

FTP INI 메서드를 사용하여 ThinOS 디바이스 등록

전제조건

Wyse Management Suite에 등록할 그룹을 생성합니다.

단계

1. `wnos.ini` 파일을 생성합니다. 다음 매개변수를 입력합니다.

   CCMEnable=yes/no **CCMServer**=FQDN of WMS Server **GroupPrefix**=The prefix of the Group Token **GroupKey**=The Group Key **CAValidation**=yes/no **Discover**=yes/no

예를 들어, ThinOS 디바이스를 그룹 토큰 defa-defadefa가 있고 CA 유효성 검사 옵션이 활성화된 Wyse Management Suite(서버 FQDN: ServerFQDN.domain.com)에 등록하려면 다음 INI 매개변수를 입력합니다.

CCMEnable=yes **CCMServer**= is ServerFQDN.domain.com **GroupPrefix**=defa **GroupKey**=defadefa **CAValidation**=yes **Discover**=yes

2. wnos.ini 파일을 임의의 FTP 경로의 wnos 폴더에 넣습니다.
3. ThinOS 디바이스의 **중앙 구성**으로 이동합니다.
4. **일반** 탭에서 파일 서버의 FTP 경로 또는 상위 폴더까지의 경로를 제공합니다.
5. 필요한 경우 FTP 자격 증명을 입력합니다. FTP에 자격 증명이 필요하지 않은 경우 사용자 이름과 암호는 익명일 수 있습니다.
6. **확인**을 클릭하고 클라이언트를 재시작합니다.
7. ThinOS 디바이스의 **중앙 구성**으로 이동합니다.
   Wyse Device Agent 탭의 해당 필드에 Wyse 관리 서버의 세부 정보가 나오고 클라이언트 항목을 Wyse Management Server>디바이스 페이지에서 볼 수 있는지 확인합니다.

FTP INI 메서드를 사용하여 ThinLinux 버전 2.0 디바이스 등록

전제조건

Wyse Management Suite에 등록할 그룹을 생성합니다.

단계

1. wlx.ini 파일을 생성합니다. 다음 매개변수를 입력합니다.

   WMSEnable=yes\no

   WMSServer=https://FQDN of the WMS Server:Port <By default 443 is used>

   GroupRegistrationKey=GroupToken present in WMS Server

   CAValidation=True/False

   예를 들어, ThinLinux 버전 2.0 디바이스를 그룹 토큰 defa-defaultfa가 있는 Wyse Management Suite(서버의 FQDN은 ServerFQDN.domain.com)에 등록하고 CA 유효성 검사 옵션을 활성화한 상태에서 다음 INI 매개변수를 입력합니다.

   WMSEnable=yes

   WMSServer=https://ServerFQDN.domain.com:443

   GroupRegistrationKey=defa-defadefa

   CAValidation=True

2. wlx ini 파일을 wyse\wlx2 폴더에 넣습니다.
3. ThinLinux 씬 클라이언트에서 **설정**으로 이동하고 관리자로 전환합니다.
4. **관리** > **INI**로 이동합니다.
5. FTP 서버 URL을 입력합니다.
6. **저장**을 클릭한 다음 씬 클라이언트를 재시작합니다.
7. **관리** > **Wyse Device Agent**로 이동합니다.
   Wyse Device Agent 탭에서 Wyse Management Server 세부 정보가 해당 필드에 나와 있고 클라이언트 항목이 Wyse Management Server>디바이스 페이지에서 볼 수 있는지 확인합니다.

FTP INI 메서드를 사용하여 ThinLinux 버전 1.0 디바이스 등록

전제조건

Wyse Management Suite에 등록할 그룹을 생성합니다.

단계

1. wlx.ini 파일을 생성하고 다음 매개변수를 입력합니다.

   WMSEnable=yes\no

   WMSServer=https://FQDN of the WMS Server:Port <By default 443 is used>

GroupRegistrationKey=GroupToken present in WMS Server

CAValidation=True/False

예를 들어, ThinLinux 버전 1.0 디바이스를 그룹 토큰 defa-defaultfa가 있는 Wyse Management Suite(서버의 FQDN은 ServerFQDN.domain.com)에 등록하고 CA 유효성 검사 옵션을 활성화한 상태에서 다음 INI 매개변수를 입력합니다.

WMSEnable=yes

WMSServer=https://ServerFQDN.domain.com:443

GroupRegistrationKey=defa-defadefa

CAValidation=True

2. wlx ini 파일을 wyse\wlx 폴더에 넣습니다.
3. ThinLinux 씬 클라이언트에서 **설정**으로 이동하고 관리자로 전환합니다.
4. **관리** > **INI**로 이동합니다.
5. FTP 서버 URL을 입력합니다.
6. **저장**을 클릭한 다음 씬 클라이언트를 재시작합니다.
7. **관리** > **Wyse Device Agent**로 이동합니다.
   Wyse Device Agent 탭에서 Wyse Management Server 세부 정보가 해당 필드에 나와 있고 클라이언트 항목이 Wyse Management Server>디바이스 페이지에서 볼 수 있는지 확인합니다.

DHCP 옵션 태그를 사용하여 디바이스 등록

DHCP 옵션 태그를 사용하여 디바이스를 등록할 수 있습니다.

표 8. 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: wmsserver.acme.com. 여기서 wmsserver.acme.com은 Wyse Management Suite가 설치된 서버의 정규화된 도메인 이름입니다. **노트:** 서버 URL에 https://FQDN 또는 FQDN:443을 사용하지 마십시오. 그렇지 않으면 씬 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: wmsservername.domain.com:1883. 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 이전 버전의 ThinOS 및 Windows Embedded 디바이스에서 Wyse Device Agent 세부 정보를 구성할 때 MQTT 서버 세부 정보를 입력해야 합니다. MQTT는 씬 클라이언트에 알리는 데 필요한 WMS의 구성 요소입니다. MQTT 세부 정보를 포함 및 포함하지 않은 URL은 Wyse Management Suite 퍼블릭 클라우드 환경의 허용 목록에 추가해야 합니다. **노트:** MQTT URL을 사용하여 Wyse Management Suite에 로그인할 수 없습니다.
이름 – CA 유효성 검사 **데이터 유형** – 문자열 **코드** - 167 **설명** – 인증 기관 검증	프라이빗 클라우드에서 Wyse Management Suite를 사용하여 디바이스를 등록하는 경우 CA 유효성 검사 옵션을 활성화 또는 비활성화할 수 있습니다. 기본적으로 CA 유효성 검사는 퍼블릭 클라우드에서 활성화됩니다. 퍼블릭 클라우드에서도 CA 유효성 검사를 비활성화할 수 있습니다. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져온 경우 **참**을 입력합니다.

표 8. DHCP 옵션 태그를 사용하여 디바이스 등록 (계속)

옵션 태그	설명
	클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져오지 않은 경우 **거짓**을 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.

노트: Windows 서버에서 DHCP 옵션 태그를 추가하는 방법에 대한 자세한 지침은 DHCP 옵션 태그 생성 및 구성 방법을 참조하십시오.

DNS SRV 레코드를 사용하여 디바이스 등록

DNS 기반 디바이스 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.

노트: Windows 서버에서 DNS SRV 레코드를 추가하는 방법에 대한 자세한 지침은 DNS SRV 레코드 생성 및 구성 방법을 참조하십시오.

다음 표에는 DNS SRV 레코드의 유효한 값이 나열되어 있습니다.

표 9. 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: `wmsserver.acme.com`. 여기서 wmsserver.acme.com은 Wyse Management Suite가 설치된 서버의 정규화된 도메인 이름입니다. **노트:** 서버 URL에 https://FQDN 또는 FQDN:443을 사용하지 마십시오. 그렇지 않으면 씬 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: `wmsservername.domain.com:1883`. **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 이전 버전의 ThinOS 및 Windows Embedded 디바이스에서 Wyse Device Agent 세부 정보를 구성할 때 MQTT 서버 세부 정보를 입력해야 합니다. MQTT는 씬 클라이언트에 알리는 데 필요한 WMS의 구성 요소입니다. MQTT 세부 정보를 포함 및 포함하지

표 9. DNS SRV 레코드를 사용하여 디바이스 구성 (계속)

URL/태그	설명
	않은 URL은 Wyse Management Suite 퍼블릭 클라우드 환경의 허용 목록에 추가해야 합니다. **노트:** MQTT URL을 사용하여 Wyse Management Suite에 로그인할 수 없습니다.
레코드 이름—_WMS_GROUPTOKEN **레코드 FQDN**—_WMS_GROUPTOKEN._tcp.<도메인 이름> **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_CAVALIDATION **레코드 FQDN** - _WMS_CAVALIDATION._tcp.<도메인 이름> **레코드 유형**—TEXT	프라이빗 클라우드에서 Wyse Management Suite를 사용하여 디바이스를 등록하는 경우 CA 유효성 검사 옵션을 활성화 또는 비활성화할 수 있습니다. 기본적으로 CA 유효성 검사는 퍼블릭 클라우드에서 활성화됩니다. 퍼블릭 클라우드에서도 CA 유효성 검사를 비활성화할 수 있습니다. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져온 경우 **참**을 입력합니다. 클라이언트와 Wyse Management Suite 서버 간의 HTTPS 통신을 위해 잘 알려진 기관에서 SSL 인증서를 가져오지 않은 경우 **거짓**을 입력합니다. **노트:** CA 유효성 검사는 최신 Wyse Management Suite 버전에 대해 선택 사항입니다.

필터를 사용하여 디바이스 검색

단계

1. **구성 그룹** 드롭다운 목록에서 기본 정책 그룹 또는 관리자가 추가한 그룹을 선택합니다.
2. **상태** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
   - **등록**
     - 등록됨
     - 미리 등록됨
     - 등록되지 않음
     - 준수
     - 등록 유효성 검사 보류 중
     - 보류 중
     - 비준수
   - **온라인 상태**
     - 온라인
     - 오프라인
     - 알 수 없음
   - **기타**
     - 최근 추가됨
3. **OS 유형** 드롭다운 목록의 다음 운영 체제 중에서 선택합니다.
   - **씬 클라이언트**

    - Linux
    - ThinLinux
    - ThinOS
    - WES
    - Teradici(프라이빗 클라우드)
    - Wyse 소프트웨어 씬 클라이언트
- **하이브리드 클라이언트**
    - 하이브리드 클라이언트

4. **OS 하위 유형** 드롭다운 목록에서 사용 중인 운영 체제의 하위 유형을 선택합니다.
5. **플랫폼** 드롭다운 목록에서 플랫폼을 선택합니다.
6. **OS 버전** 드롭다운 목록에서 운영 체제 버전을 선택합니다.
7. **에이전트 버전** 드롭다운 목록에서 에이전트 버전을 선택합니다.
8. **서브넷/접두사** 드롭다운 목록에서 서브넷을 선택합니다.
9. **시간대** 드롭다운 목록에서 시간대를 선택합니다.
10. **디바이스 태그** 드롭다운 목록에서 디바이스 태그를 선택합니다.
11. **IP 유형** 드롭다운 목록에서 IP 유형을 선택합니다.
12. **BIOS 버전** 드롭다운 목록에서 BIOS 버전을 선택합니다.

디바이스 페이지에서 필터 저장

필수 필터 옵션을 구성하여 현재 필터를 그룹으로 저장할 수 있습니다.

단계

1. 필터의 **이름**을 입력합니다.
2. **설명** 상자에 필터에 대한 설명을 입력합니다.
3. 확인란을 선택하여 현재 필터를 기본 옵션으로 설정합니다.
4. **필터 저장**을 클릭합니다.

디바이스 상태 쿼리

시스템의 디바이스 정보 및 상태를 업데이트하는 명령을 보낼 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **쿼리**를 클릭합니다.
   경고 창이 표시됩니다.
5. **명령 전송**을 클릭하여 쿼리 명령을 전송합니다.

디바이스 잠금

VDI 세션에 연결된 디바이스 그룹에 대해 등록된 디바이스를 잠그는 명령을 보낼 수 있습니다. 이 옵션은 ThinOS 운영 체제를 실행하는 씬 클라이언트에만 적용됩니다.

전제조건

디바이스가 VDI 연결에 연결되어 있어야 하며 사용자가 디바이스에 로그인해야 합니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **잠금**을 클릭합니다.
   알림 창이 표시됩니다.
5. **명령 전송**을 클릭하여 잠금 명령을 전송합니다.
   Wyse Management Suite 3.2의 **작업** 페이지에서 디바이스 잠금 명령을 보낼 수도 있습니다. 자세한 내용은 디바이스 명령 작업 예약을 참조하십시오.

디바이스 재시작

명령을 보내서 등록된 디바이스를 재시작할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **재시작**을 클릭합니다.
   경고 창이 표시됩니다.
5. 다시 시작 명령을 전송하려면 **명령 전송**을 클릭합니다.

디바이스 등록 취소

명령을 보내서 Wyse Management Suite에서 디바이스의 등록을 취소할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **등록 취소**를 클릭합니다.
   경고 창이 표시됩니다.
5. **강제 등록 취소** 확인란을 선택합니다.
6. **명령 전송**을 클릭하여 등록 취소 명령을 전송합니다.

   노트: 강제 등록 취소 옵션은 서버와 클라이언트 사이에 통신이 없는 경우 디바이스를 제거하는 데 사용할 수 있습니다. 디바이스가 관리되지 않는 상태로 이동되며 서버 항목에서 제거될 수 있습니다. WES WDA UI에서도 등록 취소 및 강제 등록 취소 작업을 수행할 수 있습니다.

등록 유효성 검사

디바이스를 수동으로 등록하거나 DHCP/DNS 자동 검색 방법을 사용하는 경우 그룹 토큰이 정의되어 있으면 디바이스가 특정 그룹에 등록됩니다. 그룹 토큰이 정의되어 있지 않으면 디바이스가 관리되지 않는 그룹에 등록됩니다.

Wyse Management Suite에서는 디바이스가 그룹에 등록되기 전에 테넌트를 수동으로 승인해야 하는 **등록 유효성 검사** 옵션이 도입되었습니다.

등록 유효성 검사 옵션이 활성화되면 자동 검색된 디바이스가 **디바이스** 페이지에서 **유효성 검사 보류 중** 상태로 있습니다. 테넌트는 **디바이스** 페이지에서 단일 디바이스 또는 여러 디바이스를 선택하고 등록에 대한 유효성 검사를 수행할 수 있습니다. 디바이스의 유

효성 검사가 완료되면 디바이스가 해당 그룹으로 이동됩니다. 디바이스의 유효성을 검사하는 방법에 대한 자세한 내용은 등록 유효성 검사를 참조하십시오.

노트: 퍼블릭 클라우드의 기존 테넌트의 경우 또는 온프레미스 테넌트를 업그레이드하는 경우 **등록 유효성 검사** 옵션이 비활성화되어 있습니다.

대시보드 페이지의 **디바이스** 섹션에는 디바이스의 유효성 검사 상태도 표시됩니다.

디바이스 등록 유효성 검사

관리자가 그룹에 대한 씬 클라이언트의 수동 및 자동 등록을 제어할 수 있도록 **등록 유효성 검사**를 활성화할 수 있습니다. **대시보드** 페이지에서 **보류 중** 상태 수를 클릭하거나 **디바이스** 페이지의 **상태** 드롭다운 목록에서 **등록 유효성 검사 보류 중**을 선택하여 **유효성 검사 보류 중**을 선택하여 디바이스를 필터링할 수 있습니다.

전제조건

- Wyse Management Suite를 설치하거나 **포털 관리** 페이지에서 **등록 유효성 검사** 옵션을 활성화해야 합니다.
- 디바이스는 등록 보류 중 상태이어야 합니다.

단계

1. 유효성 검사를 수행하려는 디바이스의 확인란을 선택합니다.
2. **등록 유효성 검사** 옵션을 클릭합니다.
   경고 창이 표시됩니다.
3. **명령 전송**을 클릭합니다.
   디바이스가 원하는 그룹으로 이동하고 디바이스가 등록됩니다.

디바이스를 출고 시 기본 설정으로 재설정

명령을 보내서 디바이스를 출고 시 기본 설정으로 재설정할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **출고 시 설정으로 재설정**을 클릭합니다.
   알림 창이 표시됩니다.
5. 클라이언트 재설정 이유를 입력합니다.
6. **명령 전송**을 클릭합니다.

   Wyse Management Suite 3.2의 **작업** 페이지에서 디바이스 잠금 명령을 보낼 수도 있습니다. 자세한 내용은 디바이스 명령 작업 예약을 참조하십시오.

디바이스 페이지에서 그룹 할당 변경

디바이스 페이지를 사용하여 디바이스의 그룹 할당을 변경할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **그룹 변경**을 클릭합니다.
   그룹 할당 변경 창이 표시됩니다.
5. 드롭다운 메뉴에서 디바이스에 대한 새 그룹을 선택합니다.

6. **저장**을 클릭합니다.

디바이스로 메시지 전송

디바이스 페이지를 사용하여 등록된 디바이스에 메시지를 보낼 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **메시지 전송**을 클릭합니다.
   메시지 전송 창이 표시됩니다.
5. 메시지를 입력합니다.
6. **전송**을 클릭합니다.

   Wyse Management Suite 3.2의 **작업** 페이지에서 디바이스로 메시지를 보낼 수도 있습니다. 자세한 내용은 디바이스 명령 작업 예약을 참조하십시오.

Wake On LAN 명령

디바이스 전원이 꺼져 있거나 절전 모드에 있는 경우 명령을 보내서 디바이스를 활성화할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **Wake On LAN**을 클릭합니다.
   알림 창이 표시됩니다.
5. **명령 전송**을 클릭합니다.

디바이스 세부 정보 보기

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.

디스플레이 매개변수 보기

Wyse Management Suite 3.1에서 Windows Embedded 및 ThinLinux 운영 체제를 실행하는 디바이스의 디스플레이 설정을 볼 수 있습니다. 디스플레이 설정의 공급업체 이름, 모델 번호, 일련번호, 해상도, 화면 종횡비, 모드, 정렬 및 회전 세부 정보를 볼 수 있습니다.

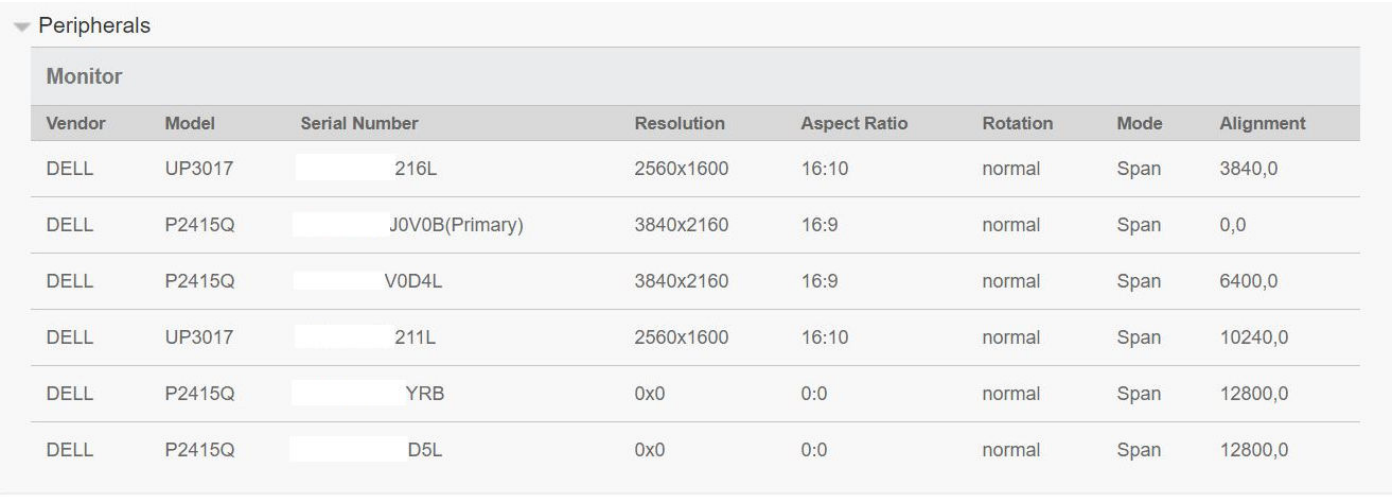
단계

1. **디바이스** 페이지로 이동합니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.

3. 표시된 디바이스 중 하나를 클릭합니다.

   디바이스 세부 정보 페이지가 표시됩니다.

4. **시스템 정보** > **주변 기기**로 이동합니다.
   디스플레이 설정 세부 정보를 볼 수 있습니다.



Peripherals

Monitor

Vendor	Model	Serial Number	Resolution	Aspect Ratio	Rotation	Mode	Alignment
DELL	UP3017	216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	D5L	0x0	0:0	normal	Span	12800,0

그림 7 . 디스플레이 매개변수

가상 NIC 세부 정보 보기

Wyse Management Suite 3.1에서 Windows Embedded 및 ThinLinux 운영 체제를 실행하는 디바이스의 네트워크 어댑터 세부 정보를 볼 수 있습니다. 네트워크 어댑터의 어댑터 이름, MAC 주소, IP 주소, 게이트웨이 IP 주소 및 DNS 서버 세부 정보를 볼 수 있습니다.

단계

1. **디바이스** 페이지로 이동합니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.

   디바이스 세부 정보 페이지가 표시됩니다.

4. **시스템 정보** > **네트워크 세부 정보 - 네트워크 어댑터**로 이동합니다.
   네트워크 세부 정보 - 네트워크 어댑터 섹션에서 가상 NIC 세부 정보를 볼 수 있습니다.

Network Details – Network Adapters

Adapter Name	MAC Address	IP Address	IPV6 Address	Gateway IP Address	DNS Server
eth0	E8:B0	10.150.		10.150.	10.150. , 10.150.
eth1	E8:B0	10.150.		10.150.	10.150. , 10.150.

그림 8 . 네트워크 세부 정보 - 네트워크 어댑터

BIOS 세부 정보 보기

Wyse Management Suite 3.1에서 **디바이스 세부 정보** 페이지에서 BIOS 매개변수 값을 볼 수 있습니다.

단계

1. **디바이스** 페이지로 이동합니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.

디바이스 세부 정보 페이지가 표시됩니다. **시스템 정보** 탭의 **BIOS 설정** 섹션에서 BIOS 세부 정보를 볼 수 있습니다.

디바이스 요약 관리

디바이스 페이지를 사용하여 메모, 그룹 할당, 경고 및 디바이스 구성에 대한 정보를 보고 관리할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
2. **디바이스 세부 정보** 페이지에서 **요약** 탭을 클릭합니다.
   디바이스 요약이 표시됩니다.
3. 오른쪽 창에서 **메모 추가**를 클릭합니다.
   메모 추가 창이 표시됩니다.
4. 제공된 필드에 메시지를 입력하고 **저장**을 클릭합니다.
5. 오른쪽 창에서 **그룹 할당 변경**을 클릭합니다.
   그룹 할당 변경 창이 표시됩니다.
6. 드롭다운 메뉴에서 디바이스에 대한 새 그룹을 선택합니다.
7. **저장**을 클릭합니다.
8. **예외 생성/편집**을 클릭하여 디바이스 수준 예외를 생성하거나 편집하고 **디바이스** 페이지에서 특정 디바이스 정책을 구성합니다.

시스템 정보 보기

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.
4. **시스템 정보**를 클릭합니다.
   시스템 정보가 표시됩니다.

디바이스 이벤트 보기

디바이스와 관련된 시스템 이벤트에 대한 정보를 보고 관리할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.
4. **디바이스 세부 정보** 페이지에서 **이벤트** 탭을 클릭합니다.
   디바이스의 이벤트가 표시됩니다.

설치된 애플리케이션 보기

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.

2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 표시된 디바이스 중 하나를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.
4. **설치된 앱** 탭을 클릭합니다.
   디바이스에 설치된 애플리케이션 목록이 표시됩니다.

   이 옵션은 Windows Embedded Standard, Linux 및 ThinLinux 디바이스에서 사용할 수 있습니다. 페이지에 표시되는 특성은 다음과 같습니다.
   - 이름
   - 게시자
   - 버전
   - 설치된 위치

   노트:

   설치된 애플리케이션 수는 애플리케이션 설치 또는 제거에 따라 증가하거나 감소합니다. 이 목록은 디바이스를 체크인하거나 다음에 쿼리될 때 업데이트됩니다.

씬 클라이언트 이름 바꾸기

이 페이지를 사용하여 Windows Embedded Standard, ThinLinux 및 ThinOS 운영 체제에서 실행되는 씬 클라이언트의 호스트 이름을 변경할 수 있습니다.

단계

1. **디바이스** 페이지에서 디바이스를 클릭합니다.
2. **기타 옵션** 드롭다운 목록에서 **호스트 이름 변경** 옵션을 선택합니다.
3. 메시지가 나타나면 새 호스트 이름을 입력합니다.

   노트: 호스트 이름에는 영숫자와 하이픈만 사용할 수 있습니다.

4. Windows Embedded Standard 디바이스에서 **재부팅** 드롭다운 목록은 **경고** 창에 있습니다. 시스템을 재시작하려면 **재부팅** 옵션을 선택합니다. **나중에 재부팅** 옵션을 선택하면 디바이스가 구성된 시간에 재시작되고 호스트 이름이 업데이트됩니다.

   노트: 호스트 이름을 업데이트하기 위해 ThinLinux 디바이스를 재시작할 필요는 없습니다.

5. **명령 전송**을 클릭합니다.
   확인 메시지가 표시됩니다.

원격 섀도 연결 활성화

이 페이지를 사용하여 전역 및 그룹 관리자가 Windows Embedded Standard, ThinLinux 및 ThinOS 씬 클라이언트 세션에 원격으로 액세스할 수 있습니다. 이 기능은 프라이빗 클라우드에만 적용되며 Standard 및 Pro 라이선스 모두에서 사용할 수 있습니다.

단계

1. **디바이스** 페이지에서 디바이스를 클릭합니다.
2. **기타 옵션** 드롭다운 목록에서 **원격 섀도(VNC)** 옵션을 선택합니다.
   타겟 씬 클라이언트의 IP 주소 및 포트 번호가 **원격 섀도(VNC)** 대화 상자에 표시됩니다.

   노트: 기본 포트 번호는 5900입니다.
3. 타겟 씬 클라이언트의 포트 번호를 변경합니다(선택 사항).
4. **연결**을 클릭하여 타겟 씬 클라이언트에 대한 원격 세션을 시작합니다.

   노트: Wyse Management Suite 포털은 테넌트당 최대 5개의 원격 섀도 세션을 지원합니다.

Dell Hybrid Client 디바이스에 대한 원격 섀도 연결 구성

이 페이지를 사용하여 전역 및 그룹 관리자가 Dell Hybrid Client 디바이스 세션에 원격으로 액세스할 수 있습니다. 이 기능은 프라이빗 클라우드에만 적용되며 Standard 및 Pro 라이선스 모두에서 사용할 수 있습니다.

단계

1. 표준 또는 고급 애플리케이션 정책을 사용하여 Wyse Management Suite에서 VNC 추가 기능 패키지를 배포합니다. 애플리케이션 정책을 참조하십시오.
   추가 기능이 설치되고 디바이스가 재부팅됩니다.
2. Wyse Management Suite에서 VNC 서버 옵션을 구성하고 배포합니다. VNC 서버 옵션을 구성하려면 다음을 수행합니다.
   a. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
   b. **정책 편집** 드롭다운 메뉴에서 **하이브리드 클라이언트**를 클릭합니다.
      구성 제어 | 하이브리드 클라이언트 창이 표시됩니다.
   c. **표준** 또는 **고급** 옵션을 클릭합니다.
   d. **개인 정보 보호 및 보안** > **VNC 서버**로 이동하여 옵션을 구성합니다.
   e. **저장 및 게시**를 클릭합니다.

디바이스 종료

Wyse Management Suite를 사용하면 Windows Embedded Standard, ThinLinux 및 ThinOS 씬 클라이언트와 같은 디바이스를 종료할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. **기타 옵션** 드롭다운 목록에서 **지금 종료**를 클릭합니다.
   디바이스를 종료하는 원격 명령이 선택한 디바이스로 전송됩니다. 디바이스가 서버에 응답하고 명령이 성공적으로 적용됩니다.
   노트: 지금 종료 옵션은 Linux 운영 체제에서 실행 중인 씬 클라이언트에 대해 활성화되지 않습니다.

디바이스 태그 지정

Wyse Management Suite에서 **디바이스 태그 지정** 옵션을 사용하여 디바이스 또는 디바이스 그룹을 식별할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
   기본 설정 디바이스 목록이 표시됩니다.
3. 하나 이상의 디바이스를 선택합니다. **기타 옵션** 드롭다운 목록에서 **디바이스 태그 지정**을 클릭합니다.
   디바이스 태그 지정 설정 창이 표시됩니다.
4. 기본 설정 태그 이름을 입력합니다.
5. **태그 설정**을 클릭합니다.

디바이스 규정 준수 상태

기본적으로 다음 색상이 디바이스 상태로 표시됩니다.

- 빨간색 - 등록된 디바이스가 7일 이상 체크인되지 않은 경우.
- 회색 - 디바이스에 구성 정책을 적용하는 경우.
- 녹색 - 디바이스에 모든 구성 정책을 적용하는 경우.

기본값의 범위는 1일~99일입니다.

온라인 상태 옵션은 디바이스 이름 옆에 있습니다. 다음과 같은 색상이 온라인 상태로 표시됩니다.

- 빨간색 - 디바이스에서 3회 이상 하트비트를 전송하지 않은 경우.
- 회색 - 디바이스에서 2회 이상, 3회 이하 동안 하트비트를 전송하지 않은 경우.
- 녹색 - 디바이스에서 하트비트를 정기적으로 전송하는 경우.

Windows Embedded Standard 또는 ThinLinux 이미지 가져오기

전제조건

- Wyse Management Suite 1.3 원격 리포지토리를 사용하는 경우 복구/복구 + OS 가져오기 템플릿을 리포지토리에서 사용할 수 없습니다. 템플릿에 액세스하려면 Wyse Management Suite를 1.4 이상으로 업그레이드해야 합니다.
- ThinLinux 이미지 가져오기 작업을 수행하려면 ThinLinux 디바이스에서 **설정** 창을 닫아야 합니다. ThinLinux 디바이스에서 OS/OS+복구 이미지를 가져오기 전에 이 작업을 수행해야 합니다.
- ThinLinux 1.x에서 2.x로 업그레이드하려면 관리자가 디바이스를 최신 WDA 및 Merlin으로 업데이트한 다음 이미지를 가져와야 합니다. 이 가져온 이미지는 ThinLinux 1.x에서 2.x로 업그레이드하는 데 사용되어야 합니다.
- 로컬 리포지토리를 사용하는 경우 서버가 실행 중인 가상 시스템에 Wyse Management Suite의 가져오기를 수행하고 필요한 서비스를 실행할 수 있는 충분한 메모리가 있는지 확인합니다.

단계

1. **Windows Embedded Standard** 또는**ThinLinux** 디바이스 페이지로 이동합니다.
2. **기타 작업** 드롭다운 목록에서 **OS 이미지 가져오기** 옵션을 선택합니다.
3. 다음 세부 정보를 입력하거나 선택합니다.
   - **이미지 이름**—이미지 이름을 입력합니다. 이미지를 유사한 이름을 가진 성공적으로 완료되지 않은 이미지 파일로 대치하려면 **이름 재정의**를 클릭합니다.
   - **파일 리포지토리**—드롭다운 목록에서 이미지가 업로드되는 파일 리포지토리를 선택합니다. 파일 리포지토리는 두 가지 유형이 있습니다.
     - 로컬 리포지토리
     - 원격 Wyse Management Suite 리포지토리
   - **가져오기 유형**—가져오기 유형 요구 사항에 따라 **기본** 또는 **고급** 중 하나를 선택합니다.
     - **기본** 가져오기 유형을 선택하면 다음 옵션이 표시됩니다.
       - 압축
       - OS
       - BIOS
       - 복구––ThinLinux 2.x용
     - **고급** 가져오기 유형을 선택하면 템플릿 선택을 위한 드롭다운 목록이 표시됩니다. 기본적으로 사용할 수 있는 템플릿을 선택합니다.

       노트: 기존 템플릿 또는 기본 템플릿을 편집하여 수동으로 만든 맞춤형 템플릿을 사용할 수 있습니다.
4. **이미지 가져오기 준비**를 클릭합니다.

결과

OS 이미지 가져오기 명령을 전송하면 클라이언트 디바이스가 서버에서 이미지 가져오기 요청을 받습니다. 이미지 가져오기 요청 메시지가 클라이언트 측에 표시됩니다. 다음 옵션 중 하나를 클릭합니다.

- **Sysprep 이후 가져오기** - 디바이스가 재시작되고 비활성화된 상태의 운영 체제에 로그인합니다. 맞춤형 Sysprep을 실행합니다. 사용자 지정 sysprep이 완료되면 디바이스가 Merlin 운영 체제로 부팅되고 이미지 가져오기 작업이 수행됩니다.

  노트: 이 옵션은 Windows Embedded Standard 디바이스에 적용됩니다.
- **지금 가져오기**—디바이스가 Merlin 운영 체제로 부팅되고 이미지 가져오기 작업이 수행됩니다.

로그 파일 요청

Windows Embedded Standard, ThinOS 및 ThinLinux 디바이스에서 디바이스 로그를 요청할 수 있습니다. ThinOS 디바이스에서는 시스템 로그를 업로드합니다. Windows Embedded Standard에서는 Wyse Device Agent 로그 및 Windows 이벤트 뷰어 로그를 업로드합니다. Linux 또는 ThinLinux에서는 Wyse Device Agent 로그 및 시스템 로그를 업로드합니다.

전제조건

로그 파일을 가져오려면 디바이스를 활성화해야 합니다.

단계

1. **디바이스** 페이지로 이동하여 특정 디바이스를 클릭합니다.
   디바이스 세부 정보가 표시됩니다.
2. **디바이스 로그** 탭을 클릭합니다.
3. **로그 파일 요청**을 클릭합니다.
4. 로그 파일을 Wyse Management Suite 서버에 업로드한 후에 **여기를 클릭** 링크를 클릭하고 로그를 다운로드합니다.

   노트: 디바이스 로그는 `Hostname-timestamp` 형식입니다. Dell Hybrid Client, Linux 또는 ThinLinux는 로그 파일을 `.tar` 형식으로 업로드하고, Windows 또는 ThinOS 9.x 시스템은 로그 파일을 `.zip` 형식으로 업로드합니다.

디바이스 문제 해결

디바이스 페이지를 사용하여 문제 해결 정보를 보고 관리할 수 있습니다.

단계

1. **디바이스 세부 정보** 페이지에서 **문제 해결** 탭을 클릭합니다.
2. **스크린샷 요청**을 클릭합니다.
   클라이언트 권한 유무와 상관없이 씬 클라이언트의 스크린샷을 캡처할 수 있습니다. **사용자 동의 필요** 확인란을 선택할 경우 클라이언트에 메시지가 표시됩니다. 이 옵션은 Windows Embedded Standard, Linux 및 ThinLinux 디바이스에만 적용할 수 있습니다.
3. **프로세스 목록 요청**을 클릭하여 씬 클라이언트에서 실행 중인 프로세스 목록을 확인합니다.
4. **서비스 목록 요청**을 클릭하여 씬 클라이언트에서 실행 중인 서비스 목록을 확인합니다.
5. **모니터링 시작**을 클릭하여 성능 메트릭 콘솔에 액세스합니다.
   성능 메트릭 콘솔에 다음과 같은 세부 정보가 표시됩니다.
   - 최근 1분 평균 CPU
   - 최근 1분 평균 메모리 사용량

Dell Hybrid Client를 이미지로 다시 설치

명령을 전송하여 Dell Hybrid Client를 이미지로 다시 설치할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **이미지로 다시 설치**를 클릭합니다.
   알림 창이 표시됩니다.
5. **명령 전송**을 클릭합니다.
   이 작업은 디바이스에 대한 복구 이미지 기능을 수행합니다.

Dell Generic Client를 하이브리드 클라이언트로 변환

명령을 전송하여 Dell Generic Client를 Dell Hybrid Client로 변환할 수 있습니다.

전제조건

Dell Ubuntu 디바이스(일반 클라이언트)는 복구 파티션에 Dell Hybrid Bundle과 함께 사전 로드되어야 합니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 일반 클라이언트 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **Convert to Hybrid**를 클릭합니다.
   알림 창이 표시됩니다.
5. **명령 전송**을 클릭합니다.

   노트: **Convert to Hybrid** 명령은 **작업**, **디바이스** 및 **디바이스 세부 정보** 페이지에서도 사용할 수 있습니다.

Dell Hybrid Client용 구성 사용자 인터페이스 패키지 가져오기

Dell Hybrid Client가 Wyse Management Suite 서버에 있는 버전보다 더 높은 버전의 구성 스키마를 가지고 있는 경우 최신 구성 사용자 인터페이스 패키지를 가져올 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 구성하려는 디바이스를 클릭합니다.
   디바이스 세부 정보 페이지가 표시됩니다.
4. **기타 작업** 드롭다운 메뉴에서 **구성 UI 패키지 가져오기**를 클릭합니다.
   알림 창이 표시됩니다.
5. **명령 전송**을 클릭합니다.

Dell Hybrid Client를 출고 시 설정으로 재설정

명령을 보내서 Dell Hybrid Client를 출고 시 설정으로 재설정할 수 있습니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. 필터를 적용하여 기본 설정 디바이스를 찾습니다.
3. 해당 디바이스의 확인란을 선택합니다.
4. **기타 작업** 드롭다운 메뉴에서 **출고 시 설정으로 재설정**을 클릭합니다.
   알림 창이 표시됩니다.
5. Dell Hybrid Client 재설정 이유를 입력합니다.
6. **명령 전송**을 클릭합니다.

디바이스의 대량 그룹 변경

Wyse Management Suite 3.2에서 일련번호, MAC 주소 또는 호스트 이름을 사용하여 여러 디바이스 그룹을 변경할 수 있습니다. 이 옵션은 Pro 라이선스가 있는 Wyse Management Suite에만 적용할 수 있습니다.

전제조건

디바이스의 일련번호, MAC 주소 또는 호스트 이름을 사용하여 CSV 파일을 생성합니다.

단계

1. **디바이스**를 클릭합니다.
   디바이스 페이지가 표시됩니다.
2. **기타 작업** 드롭다운 목록에서 **그룹 대량 변경**을 선택합니다.
   그룹 할당 대량 변경 창이 표시됩니다.
3. **디바이스를 필터링할 속성 선택** 드롭다운 목록에서 선택한 속성을 기반으로 새 그룹으로 변경할 디바이스를 필터링할 속성을 선택합니다.
4. CSV 파일을 선택하려면 **찾기**를 클릭하고 CSV 파일이 있는 위치로 이동합니다.
5. **이 디바이스에 대한 새 그룹 선택** 드롭다운 목록에서 디바이스에 대한 새 그룹을 선택합니다.
6. **저장**을 클릭합니다.

   노트: 한 번에 최대 100개의 다비이스 그룹을 변경할 수 있습니다.

9

앱 및 데이터

이 섹션에서는 Wyse 관리 콘솔을 사용하여 일상적인 디바이스 애플리케이션 작업, 운영 체제 이미징, 인벤토리 관리 및 정책 설정을 실시하는 방법을 설명합니다. 리포지토리 이름은 색상으로 구분되어 상태를 나타냅니다.

앱 및 데이터 페이지를 사용하여 다음과 같은 유형의 정책을 구성할 수 있습니다.

- 표준 애플리케이션 정책 - 이 정책을 사용하면 단일 애플리케이션 패키지를 설치할 수 있습니다.
- 고급 애플리케이션 정책 - 이 정책을 사용하면 여러 애플리케이션 패키지를 설치할 수 있습니다.
- 이미지 정책 - 이 정책을 사용하면 운영 체제를 설치할 수 있습니다.

애플리케이션 정책 및 운영 체제 이미지를 씬 클라이언트에 배포하는 작업은 특정 시간대나 디바이스에 구성한 시간대에 따라 즉시 또는 나중으로 예약할 수 있습니다.

노트: Wyse Management Suite 3.3에서 클라이언트로 구성을 5,000회 동시 다운로드할 수 있습니다. 추가적인 동시 다운로드는 슬롯이 사용 가능한 상태가 될 때까지 대기 상태로 전환됩니다. 60초 후 요청 시간이 초과됩니다.

주제:

- 애플리케이션 정책
- 이미지 정책
- 파일 리포지토리 관리

애플리케이션 정책

Wyse Management Suite는 다음과 같은 유형의 애플리케이션 인벤토리 및 애플리케이션 배포 정책을 지원합니다.

- 씬 클라이언트 애플리케이션 인벤토리 구성
- Wyse 소프트웨어 씬 클라이언트 애플리케이션 인벤토리 구성
- 표준 애플리케이션 정책을 생성하여 씬 클라이언트에 배포
- 고급 애플리케이션 정책을 생성하여 씬 클라이언트에 배포
- 표준 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포
- 고급 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포

Windows 기반 디바이스에 대한 중요 참고 사항:

- 확장자가 .msi, .exe, .msu, .msp인 Windows 기반 애플리케이션에 대한 설치를 지원합니다.

  다른 확장자를 가진 애플리케이션은 `%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA`로 다운로드됩니다.

- Wyse Management Suite를 사용하여 .exe 애플리케이션을 배포하는 경우 자동 설치 방법을 따릅니다. 필요한 경우 적절한 자동 매개변수를 입력해야 합니다. 예: **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.
- 파일 확장자가 .bat, .cmd, .ps1, .vbs인 스크립트 배포를 지원합니다.

  다른 확장자를 가진 스크립트는 `%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA`로 다운로드됩니다.

- Wyse Management Suite를 사용하여 푸시된 모든 스크립트는 비대화식이어야 합니다. 즉, 설치하는 동안 사용자 개입이 필요하지 않습니다.
- 고급 애플리케이션 정책에서 0 이외의 값을 반환하는 스크립트/exe가 있는 경우 오류로 간주됩니다.
- 고급 애플리케이션 정책에서 사전 설치에 실패하면 애플리케이션 설치가 계속되지 않습니다.
- 표준 애플리케이션을 사용하여 푸시된 모든 exe/스크립트는 작업 상태에서 업데이트되는 오류 코드와 함께 성공한 것으로 보고됩니다.
- 확장자가 msi/msu/msp인 애플리케이션의 경우 표준 오류 코드가 보고됩니다. 애플리케이션이 REBOOT_REQUIRED를 반환하면 디바이스가 한 번 더 재부팅됩니다.

Linux 디바이스에 대한 중요 참고 사항:

- ThinLinux 2.0의 경우 확장자가 .bin, .deb 그리고 Thin Linux 1.0의 경우 확장자가 .RPM인 Linux 기반 애플리케이션에 대한 설치를 지원합니다.
- 확장자가 .sh인 ThinLinux 디바이스의 경우 스크립트 배포를 지원합니다.
- 표준 또는 고급 애플리케이션 정책에서 0 이외의 값을 반환하는 스크립트/deb/rpm이 있는 경우 오류로 간주됩니다.
- 고급 애플리케이션 정책에서 사전 설치에 실패하면 앱 설치가 계속되지 않습니다.

씬 클라이언트 애플리케이션 인벤토리 구성

단계

1. **Apps and Data** 탭을 클릭합니다.
2. 왼쪽 창에서 **App Inventory** > **Thin Client**로 이동합니다.
   Thin Client Inventory 창에 애플리케이션 세부 정보가 표시됩니다.
3. 인벤토리에 애플리케이션을 추가하려면 씬 클라이언트 애플리케이션 파일을 `<repo-dir>\repository\thinClientApps` 폴더에 놓습니다.
   Wyse Management Suite 리포지토리는 모든 파일에 대한 메타데이터를 정기적으로 Wyse Management Suite 서버로 전송합니다.
4. 애플리케이션을 편집하려면 다음을 수행합니다.
   a. 목록에서 업로드된 애플리케이션을 선택합니다.
   b. **앱 편집**을 클릭합니다.
      애플리케이션 편집 창이 표시됩니다.
   c. 메모를 입력합니다.
   d. **저장**을 클릭합니다.

   노트: 운영자가 업로드한 애플리케이션에 전역 접미사가 추가됩니다.

   서로 다른 리포지토리에 있는 애플리케이션이 한 번만 나열됩니다. **리포지토리 이름** 열에는 애플리케이션이 있는 리포지토리의 수가 표시됩니다. 열 위로 마우스를 이동하면 리포지토리의 이름을 볼 수 있습니다. 또한 리포지토리 이름은 사용 가능 여부를 지정할 수 있도록 색상으로 구분됩니다.

Wyse 소프트웨어 씬 클라이언트 애플리케이션 인벤토리 구성

단계

1. **앱 및 데이터** 탭을 클릭합니다.
2. 왼쪽 창에서 **앱 인벤토리** > **Wyse 소프트웨어 씬 클라이언트**로 이동합니다.
3. 애플리케이션을 인벤토리에 추가하려면 `<repo-dir>\repository\softwareTcApps` 폴더에 씬 클라이언트 애플리케이션 파일을 배치합니다.
   Wyse Management Suite 리포지토리는 모든 파일에 대한 메타데이터를 정기적으로 Wyse Management Suite 서버로 전송합니다.

표준 애플리케이션 정책을 생성하여 씬 클라이언트에 배포

단계

1. 로컬 리포지토리에서 **thinClientApps**로 이동하고 애플리케이션을 폴더에 복사합니다.
2. **앱 및 데이터** > **앱 인벤토리** > **씬 클라이언트**로 이동하여 애플리케이션이 Wyse Management Suite에 등록되어 있는지 확인합니다.

   노트: 앱 인벤토리 인터페이스에 최근에 추가한 프로그램이 표시되기까지 약 2분 정도 소요됩니다.

3. **앱 및 데이터** > **앱 정책** > **씬 클라이언트**로 이동합니다.
4. **정책 추가**를 클릭합니다.
   표준 앱 정책 추가 창이 표시됩니다.
5. **정책 이름**을 입력합니다.
6. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
7. **작업** 드롭다운 목록에서 작업을 선택합니다.
8. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
9. 애플리케이션을 필터링하려면 **확장자를 기준으로 파일 필터링** 확인란을 선택합니다.
10. **애플리케이션** 드롭다운 목록에서 애플리케이션을 선택합니다.
    애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.

    노트: Wyse Management Suite 3.1에서 스크립트를 추가하여 ThinLinux 디바이스에 애플리케이션을 설치할 수 있습니다. ThinLinux용 스크립트에 유효한 shebang이 있는지 확인해야 합니다.
11. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
12. **자동으로 정책 적용** 드롭다운 목록의 다음 옵션 중에서 선택합니다.

- **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
- **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
- **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

노트: Windows 기반 디바이스의 경우 .exe 파일에 대해 자동 설치 매개변수를 지정하여 애플리케이션을 자동 모드로 실행합니다. 예: **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.

13. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.

    노트: 애플리케이션 설치 시간 초과 옵션은 Windows Embedded Standard, Wyse 소프트웨어 씬 클라이언트, Linux 및 Thin Linux 디바이스에만 적용됩니다.

14. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
15. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
16. 다음 옵션 중에서 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
17. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
18. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

    노트: 표준 애플리케이션 정책을 사용하여 BIOS를 업데이트할 수 있습니다. BIOS를 업데이트하려면 **`/s/r/f/p=fireport`**를 설치 매개변수로 사용해야 합니다.

표준 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포

단계

1. 로컬 리포지토리에서**softwareTcApps**로 이동하고 애플리케이션을 폴더에 복사합니다.
2. **앱 및 데이터** > **앱 인벤토리** > **Wyse 소프트웨어 씬 클라이언트**로 이동하여 애플리케이션이 Wyse Management Suite에 등록되어 있는지 확인합니다.

   노트: 앱 인벤토리 인터페이스에 최근에 추가한 프로그램이 표시되기까지 약 2분 정도 소요됩니다.

3. **정책 추가**를 클릭합니다.
   표준 앱 정책 추가 창이 표시됩니다.
4. **정책 이름**을 입력합니다.
5. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
6. **작업** 드롭다운 목록에서 작업을 선택합니다.
7. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
8. 애플리케이션을 필터링하려면 **확장자를 기준으로 파일 필터링** 확인란을 선택합니다.
9. **애플리케이션** 드롭다운 목록에서 애플리케이션을 선택합니다.
   애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
10. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
11. **자동으로 정책 적용** 드롭다운 목록의 다음 옵션 중에서 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.

- **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
- **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

노트: Windows 기반 디바이스의 경우 .exe 파일에 대해 자동 설치 매개변수를 지정하여 애플리케이션을 자동 모드로 실행합니다. 예: **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.

12. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.

    노트: 애플리케이션 설치 시간 초과 옵션은 Windows Embedded Standard 디바이스 및 Wyse 소프트웨어 씬 클라이언트에만 적용됩니다.

13. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
14. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
15. 다음 옵션 중에서 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
16. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
17. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

표준 애플리케이션 정책을 사용하여 Citrix StoreFront에 대해 SSO(Single Sign-on) 활성화

Citrix StoreFront에 대해 SSO(Single Sign-On)를 활성화하려면 다음을 수행합니다.

- **시나리오 1**—최신 버전의 Citrix Receiver에서 Citrix StoreFront에 대해 SSO(Single Sign-On)를 활성화하려면 다음을 수행합니다.
  1. 표준 애플리케이션 정책을 생성하여 배포한 후 **/silent** 매개변수를 사용하여 Citrix Receiver를 제거합니다.
  2. 표준 애플리케이션 정책을 생성하여 배포한 후 **/silent /includeSSON /AutoUpdateCheck = Disabled** 매개변수를 사용하여 Citrix Receiver를 다시 설치합니다.
- **시나리오 2**—Citrix Receiver를 업그레이드하고 StoreFront에 대해 SSO(Single Sign-On)를 활성화하려면 다음을 수행합니다.
  1. 표준 애플리케이션 정책을 생성하여 배포한 후 **/silent /includeSSON /AutoUpdateCheck = Disabled** 매개변수를 사용하여 Citrix Receiver를 업그레이드합니다.
- **시나리오 3**—Citrix Receiver를 다운그레이드하고 StoreFront에 대해 SSO(Single Sign-On)를 활성화하려면 다음을 수행합니다.
  1. 표준 애플리케이션 정책을 생성하여 배포한 후 **/silent /includeSSON /AutoUpdateCheck = Disabled** 매개변수를 사용하여 Citrix Receiver를 다운그레이드합니다.

고급 애플리케이션 정책을 생성하여 씬 클라이언트에 배포

단계

1. 애플리케이션 및 설치 전/후 스크립트를 복사하여(필요한 경우) 씬 클라이언트에 배포합니다.
2. 애플리케이션 및 사전/사후 설치 스크립트를 로컬 리포지토리 또는 Wyse Management Suite 리포지토리의 `thinClientApps` 폴더에 저장합니다.
3. **앱 및 데이터** > **앱 인벤토리** > **씬 클라이언트**로 이동하여 애플리케이션이 등록되어 있는지 확인합니다.
4. **앱 및 데이터** > **앱 정책** > **씬 클라이언트**로 이동합니다.
5. **고급 정책 추가**를 클릭합니다.
   고급 앱 정책 추가 페이지가 표시됩니다.
6. **정책 이름**을 입력합니다.

7. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
8. 하위 그룹에 정책을 적용하려면 **하위 그룹** 확인란을 선택합니다.
9. **작업** 드롭다운 목록에서 작업을 선택합니다.
10. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
11. 애플리케이션을 필터링하려면 **확장자를 기준으로 파일 필터링** 확인란을 선택합니다.
12. **앱 추가**를 클릭하고 **앱**에서 하나 이상의 애플리케이션을 선택합니다. 각 애플리케이션에 대해 **사전 설치**, **사후 설치** 및 **설치 매개변수**에서 사전 및 사후 설치 스크립트를 선택할 수 있습니다.

    노트: Wyse Management Suite 3.1에서 스크립트를 추가하여 ThinLinux 디바이스에 애플리케이션을 설치할 수 있습니다. ThinLinux용 스크립트에 유효한 shebang이 있는지 확인해야 합니다.

13. 애플리케이션을 설치한 후 시스템을 재부팅하려면 **재부팅**을 선택합니다.
14. **앱 추가**를 클릭하고 단계를 반복하여 여러 애플리케이션을 추가합니다.

    노트: 처음 장애 발생 시 애플리케이션 정책을 중지하려면 **앱 종속성 활성화**를 선택합니다. 이 옵션을 선택하지 않으면 애플리케이션 장애가 정책 실행에 영향을 미칩니다.

    애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
15. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
16. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
    설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 클라이언트의 메시지입니다.
17. 정책 실행 시 지연을 허용하려면 **정책 실행 지연 허용** 확인란을 선택합니다. 이 옵션을 선택하면 다음 드롭다운 메뉴가 활성화됩니다.
    - **지연할 수 있는 최대 시간** 드롭다운 목록에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
    - **최대 지연** 드롭다운 목록에서 정책 실행을 지연할 수 있는 횟수(1~3회)를 선택합니다.
18. **자동으로 정책 적용** 드롭다운 목록의 다음 옵션 중에서 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
    - **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

    노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

    노트: Windows 기반 디바이스의 경우 .exe 파일에 대해 자동 설치 매개변수를 지정하여 애플리케이션을 자동 모드로 실행합니다. 예: **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.

19. **쓰기 필터 검사 건너뛰기** 확인란을 선택하여 쓰기 필터 주기를 건너뜁니다. 이 옵션은 Windows Embedded Standard 운영 체제 디바이스 및 Wyse Software 씬 클라이언트 디바이스에 적용할 수 있습니다.
20. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.

    노트: 애플리케이션 설치 시간 초과 옵션은 Windows Embedded Standard 디바이스 및 Wyse 소프트웨어 씬 클라이언트에만 적용됩니다.

21. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
22. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
23. 다음 옵션 중에서 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
24. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
25. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

고급 애플리케이션 정책을 생성하여 Wyse 소프트웨어 씬 클라이언트에 배포

단계

1. 애플리케이션 및 설치 전/후 스크립트(필요한 경우)를 복사하여 씬 클라이언트에 배포합니다.
2. 애플리케이션 및 사전/사후 설치 스크립트를 로컬 리포지토리 또는 Wyse Management Suite 리포지토리의 `softwareTcApps` 폴더에 저장합니다.
3. **앱 및 데이터** > **앱 인벤토리** > **Wyse 소프트웨어 씬 클라이언트**로 이동하여 애플리케이션이 등록되어 있는지 확인합니다.
4. **앱 및 데이터** > **앱 정책** > **Wyse 소프트웨어 씬 클라이언트**로 이동합니다.
5. **고급 정책 추가**를 클릭합니다.
   고급 앱 정책 추가 페이지가 표시됩니다.
6. **정책 이름**을 입력합니다.
7. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
8. 하위 그룹에 정책을 적용하려면 **하위 그룹** 확인란을 선택합니다.
9. **작업** 드롭다운 목록에서 작업을 선택합니다.
10. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
11. 애플리케이션을 필터링하려면 **확장자를 기준으로 파일 필터링** 확인란을 선택합니다.
12. **앱 추가**를 클릭하고 **앱**에서 하나 이상의 애플리케이션을 선택합니다. 각 애플리케이션에 대해 **사전 설치**, **사후 설치** 및 **설치 매개변수**에서 사전 및 사후 설치 스크립트를 선택할 수 있습니다.
13. 애플리케이션을 설치한 후 시스템을 재부팅하려면 **재부팅**을 선택합니다.
14. **앱 추가**를 클릭하고 단계를 반복하여 여러 애플리케이션을 추가합니다.

    노트: 처음 장애 발생 시 애플리케이션 정책을 중지하려면 **앱 종속성 활성화**를 선택합니다. 이 옵션을 선택하지 않으면 애플리케이션 장애가 정책 실행에 영향을 미칩니다.

    애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
15. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
16. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
    설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 클라이언트의 메시지입니다.
17. 정책 실행 시 지연을 허용하려면 **정책 실행 지연 허용** 확인란을 선택합니다. 이 옵션을 선택하면 다음 드롭다운 메뉴가 활성화됩니다.
    - **지연할 수 있는 최대 시간** 드롭다운 목록에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
    - **최대 지연** 드롭다운 목록에서 정책 실행을 지연할 수 있는 횟수(1~3회)를 선택합니다.
18. **자동으로 정책 적용** 드롭다운 목록의 다음 옵션 중에서 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
    - **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

    노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

    노트: Windows 기반 디바이스의 경우 .exe 파일에 대해 자동 설치 매개변수를 지정하여 애플리케이션을 자동 모드로 실행합니다. 예: **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.
19. **쓰기 필터 검사 건너뛰기** 확인란을 선택하여 쓰기 필터 주기를 건너뜁니다. 이 옵션은 Windows Embedded Standard 운영 체제 디바이스 및 Wyse Software 씬 클라이언트 디바이스에 적용할 수 있습니다.
20. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.

    노트: **애플리케이션 설치 시간 초과** 옵션은 Windows Embedded Standard 디바이스 및 Wyse 소프트웨어 씬 클라이언트에만 적용됩니다.
21. **저장**을 클릭하여 정책을 생성합니다.

관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.

22. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
23. 다음 옵션 중에서 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
24. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
25. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

표준 애플리케이션 정책 생성 및 Dell Hybrid Client에 배포

단계

1. 로컬 리포지토리에서 **hybridClientApps**로 이동하고 애플리케이션을 폴더에 복사합니다.

   노트: Dell Hybrid Client에서는 Dell에서 서명한 애플리케이션만 배포하고 설치할 수 있습니다.

   노트: 운영자는 Dell Hybrid Client 번들 및 패키지를 운영자 계정에서 업로드할 수 있습니다. 운영자가 패키지 및 파일을 업로드하면 모든 테넌트에서 볼 수 있습니다. 테넌트는 파일을 삭제하거나 수정할 수 없습니다. 운영자는 ISO 파일을 업로드할 수 없습니다.

2. **앱 및 데이터** > **앱 인벤토리** > **하이브리드 클라이언트**로 이동하여 애플리케이션이 Wyse Management Suite에 등록되어 있는지 확인합니다.

   노트: 앱 인벤토리 인터페이스에 최근에 추가한 프로그램이 표시되기까지 약 2분 정도 소요됩니다.

3. **앱 및 데이터** > **앱 정책** > **하이브리드 클라이언트**로 이동합니다.
4. **정책 추가**를 클릭합니다.
   표준 앱 정책 추가 창이 표시됩니다.
5. **정책 이름**을 입력합니다.
6. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
7. **작업** 드롭다운 목록에서 작업을 선택합니다.
8. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
9. **애플리케이션** 드롭다운 목록에서 애플리케이션을 선택합니다.
   애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
10. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
11. **설치 매개변수** 필드에 선택한 애플리케이션의 설치 매개변수를 입력합니다.
12. **자동으로 정책 적용** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
    - **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

    노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

13. **시간 초과(1~999분)** 상자에서 클라이언트에 메시지 대화 상자가 표시되어야 하는 시간(분)을 지정합니다. 시간 초과는 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다.
14. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.
15. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
16. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
17. 다음 옵션 중에서 선택합니다.

- **즉시** - 서버가 작업을 즉시 실행합니다.
- **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
- **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.

18. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
19. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

노트: Dell Hybrid Client 버전 1.1을 1.5로 업그레이드하기 전에 **DHCImageupgardeAddon** 패키지를 푸시해야 합니다.

고급 애플리케이션 정책 생성 및 Dell Hybrid Client에 배포

단계

1. 애플리케이션 및 설치 스크립트를 복사하여(필요한 경우) 씬 클라이언트에 배포합니다.

   노트: Dell Hybrid Client에서는 Dell에서 서명한 애플리케이션 및 스크립트만 배포하고 설치할 수 있습니다.

   노트: 운영자는 Dell Hybrid Client 번들 및 패키지를 운영자 계정에서 업로드할 수 있습니다. 운영자가 패키지 및 파일을 업로드하면 모든 테넌트에서 볼 수 있습니다. 테넌트는 파일을 삭제하거나 수정할 수 없습니다. 운영자는 ISO 파일을 업로드할 수 없습니다.

2. 애플리케이션 및 설치 스크립트를 로컬 리포지토리 또는 Wyse Management Suite 리포지토리의 `hybridClientApps` 폴더에 저장합니다.
3. **앱 및 데이터** > **앱 인벤토리** > **하이브리드 클라이언트**로 이동하여 애플리케이션이 등록되어 있는지 확인합니다.
4. **앱 및 데이터** > **앱 정책** > **하이브리드 클라이언트**로 이동합니다.
5. **고급 정책 추가**를 클릭합니다.
   고급 앱 정책 추가 페이지가 표시됩니다.
6. **정책 이름**을 입력합니다.
7. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
8. 하위 그룹에 정책을 적용하려면 **하위 그룹** 확인란을 선택합니다.
9. **작업** 드롭다운 목록에서 작업을 선택합니다.
10. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
11. 애플리케이션을 필터링하려면 **확장자를 기준으로 파일 필터링** 확인란을 선택합니다.
12. **앱 추가**를 클릭하고 **앱**에서 하나 이상의 애플리케이션을 선택합니다. 각 애플리케이션에 대해 **사전 설치**, **사후 설치** 및 **설치 매개변수**에서 사전 및 사후 설치 스크립트를 선택할 수 있습니다.
13. 애플리케이션을 설치한 후 시스템을 재부팅하려면 **재부팅**을 선택합니다.
14. **앱 추가**를 클릭하고 단계를 반복하여 여러 애플리케이션을 추가합니다.

    노트: 처음 장애 발생 시 애플리케이션 정책을 중지하려면 **앱 종속성 활성화**를 선택합니다. 이 옵션을 선택하지 않으면 애플리케이션 장애가 정책 실행에 영향을 미칩니다.

    애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
15. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
16. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
    설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 클라이언트의 메시지입니다.
17. 정책 실행 시 지연을 허용하려면 **정책 실행 지연 허용** 확인란을 선택합니다. 이 옵션을 선택하면 다음 드롭다운 메뉴가 활성화됩니다.
    - **지연할 수 있는 최대 시간** 드롭다운 목록에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
    - **최대 지연** 드롭다운 목록에서 정책 실행을 지연할 수 있는 횟수(1~3회)를 선택합니다.
18. **자동으로 정책 적용** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.

- **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

19. **시간 초과(1~999분)** 상자에서 클라이언트에 메시지 대화 상자가 표시되어야 하는 시간(분)을 지정합니다. 시간 초과는 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다.
20. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.
21. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
22. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
23. 다음 옵션 중 하나를 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
24. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
25. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

노트: Dell Hybrid Client 버전 1.1을 1.5로 업그레이드하기 전에 **DHCImageupgardeAddon** 패키지를 푸시해야 합니다.

표준 애플리케이션 정책 생성 및 Dell Generic Client에 배포

단계

1. 로컬 리포지토리에서 **genericClientApps**로 이동하고 애플리케이션 패키지를 폴더에 복사합니다.

   노트: Dell Generic Client에서는 Dell에서 서명한(DHC Fish 스크립트, DCA-Enabler 패키지, DHC 번들 또는 DHC ISO 이미지 파일) 애플리케이션만 배포하고 설치할 수 있습니다.

2. **앱 및 데이터** > **앱 인벤토리** > **일반 클라이언트**로 이동하여 애플리케이션이 Wyse Management Suite에 등록되어 있는지 확인합니다.

   노트: 앱 인벤토리 인터페이스에 최근에 추가한 프로그램이 표시되기까지 약 2분 정도 소요됩니다.

3. **앱 및 데이터** > **앱 정책** > **일반 클라이언트**로 이동합니다.
4. **정책 추가**를 클릭합니다.
   표준 앱 정책 추가 창이 표시됩니다.
5. **정책 이름**을 입력합니다.
6. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
7. **작업** 드롭다운 목록에서 작업을 선택합니다.
8. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
9. **애플리케이션** 드롭다운 목록에서 애플리케이션을 선택합니다.
   애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
10. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
11. **자동으로 정책 적용** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.
    - **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

   노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

12. **시간 초과(1~999분)** 상자에서 클라이언트에 메시지 대화 상자가 표시되어야 하는 시간(분)을 지정합니다. 시간 초과는 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다.
13. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.
14. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
15. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
16. 다음 옵션 중에서 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
17. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
18. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

고급 애플리케이션 정책 생성 및 Dell Generic Client에 배포

단계

1. 애플리케이션 및 설치 스크립트(필요한 경우)를 로컬 리포지토리 또는 Wyse Management Suite 원격 리포지토리의 `genericClientApps` 폴더에 복사합니다.

   노트: Dell Generic Client에는 Dell 서명 애플리케이션 및 스크립트(DHC Fish 스크립트, DCA-Enabler 패키지, DHC 번들 또는 DHC ISO 이미지 파일)만 배포하고 설치할 수 있습니다.

2. **앱 및 데이터** > **앱 인벤토리** > **일반 클라이언트**로 이동하여 애플리케이션이 등록되어 있는지 확인합니다.
3. **앱 및 데이터** > **앱 정책** > **일반 클라이언트**로 이동합니다.
4. **고급 정책 추가**를 클릭합니다.
   고급 앱 정책 추가 페이지가 표시됩니다.
5. **정책 이름**을 입력합니다.
6. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
7. 하위 그룹에 정책을 적용하려면 **하위 그룹** 확인란을 선택합니다.
8. **작업** 드롭다운 목록에서 작업을 선택합니다.
9. **OS 유형** 드롭다운 목록에서 운영 체제를 선택합니다.
10. **확장자를 기준으로 파일 필터링** 확인란을 선택하여 애플리케이션을 필터링합니다.
11. **앱 추가**를 클릭하고 **앱**에서 하나 이상의 애플리케이션을 선택합니다.
12. 애플리케이션을 설치한 후 시스템을 재부팅하려면 **재부팅**을 선택합니다.
13. **앱 추가**를 클릭하고 단계를 반복하여 여러 애플리케이션을 추가합니다.

    노트: 처음 장애 발생 시 애플리케이션 정책을 중지하려면 **앱 종속성 활성화**를 선택합니다. 이 옵션을 선택하지 않으면 애플리케이션 장애가 정책 실행에 영향을 미칩니다.

    애플리케이션 파일을 여러 리포지토리에서 사용할 수 있는 경우 리포지토리 수가 파일 이름 옆에 표시됩니다.
14. 이 정책을 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
15. 메시지 대화 상자를 클라이언트에 표시할 시간(분)을 지정합니다.
    설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 클라이언트의 메시지입니다.
16. 정책 실행 시 지연을 허용하려면 **정책 실행 지연 허용** 확인란을 선택합니다. 이 옵션을 선택하면 다음 드롭다운 메뉴가 활성화됩니다.
    - **지연할 수 있는 최대 시간** 드롭다운 목록에서 정책 실행을 지연할 수 있는 최대 시간(1~24시간)을 선택합니다.
    - **최대 지연** 드롭다운 목록에서 정책 실행을 지연할 수 있는 횟수(1~3회)를 선택합니다.
17. **자동으로 정책 적용** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
    - **자동으로 정책을 적용하지 않음** - 이 옵션은 디바이스에 자동으로 정책을 적용하지 않습니다.
    - **새 디바이스에 정책 적용** - 이 옵션은 선택한 그룹에 속하는 등록된 디바이스 또는 선택한 그룹으로 이동하는 디바이스에 정책을 자동으로 적용합니다. 이 옵션을 선택하면 그룹에 등록된 모든 새 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다. 등록되어 새로 추가된 디바이스 개수의 작업 상태는 표시되지 않습니다.

- **체크인 시 디바이스에 정책 적용** - 이 옵션은 체크인 시 디바이스에 자동으로 적용됩니다. 이 옵션을 선택하면 그룹에 있는 모든 디바이스에 정책이 적용됩니다. 그룹에 있는 기존 디바이스에서 작업을 즉시 또는 디바이스 체크인 전 예약된 시간에 실행하려면 정책을 예약해야 합니다. 정책을 예약하면 작업 상태에 그룹에 이미 있는 디바이스 수가 표시됩니다.

  노트: Wyse Management Suite에 체크인되고 새로 추가된 디바이스의 작업 상태는 표시되지 않습니다.

18. **시간 초과(1~999분)** 상자에서 클라이언트에 메시지 대화 상자가 표시되어야 하는 시간(분)을 지정합니다. 시간 초과는 설치를 시작하기 전에 작업을 저장할 시간을 알려 주는 메시지를 클라이언트에 표시합니다.
19. 정의된 값 이후에 설치 프로세스를 중지하려면 **애플리케이션 설치 시간 초과** 필드에 시간(분)을 지정합니다. 기본값은 60분입니다.
20. **저장**을 클릭하여 정책을 생성합니다.
    관리자가 그룹을 기준으로 이 정책을 디바이스에 예약할 수 있는 메시지가 표시됩니다.
21. 동일한 페이지에서 작업을 예약하려면 **예**를 선택합니다.
22. 다음 옵션 중 하나를 선택합니다.
    - **즉시** - 서버가 작업을 즉시 실행합니다.
    - **디바이스 시간대에서** - 서버가 각 디바이스 시간대에 대해 하나의 작업을 생성하고 디바이스 시간대의 선택한 날짜 또는 시간으로 작업을 예약합니다.
    - **선택한 시간대에서** - 서버가 지정된 시간대의 날짜 또는 시간에 실행할 하나의 작업을 생성합니다.
23. 작업을 생성하려면 **미리 보기**를 클릭하면 다음 페이지에 일정이 표시됩니다.
24. **작업** 페이지로 이동하여 작업의 상태를 확인할 수 있습니다.

이미지 정책

Wyse Management Suite는 다음과 같은 유형의 운영 체제 이미지 배포 정책을 지원합니다.

- 리포지토리에 Windows Embedded Standard 운영 체제 및 ThinLinux 이미지 추가
- 리포지토리에 ThinOS 펌웨어 추가
- 리포지토리에 ThinOS 패키지 파일 추가
- 리포지토리에 ThinOS BIOS 파일 추가
- 리포지토리에 Terdici 펌웨어 추가
- Windows Embedded Standard 및 ThinLinux 이미지 정책 생성
- Dell Hybrid Client 이미지 정책 생성

리포지토리에 Windows Embedded Standard 운영 체제 및 ThinLinux 이미지 추가

전제조건

- Wyse Management Suite를 클라우드 배포와 함께 사용하는 경우**포털 관리** > **콘솔 설정** > **파일 리포지토리**로 이동합니다. **다운로드 버전 3.2.0**을 클릭하여 `WMS_Repo.exe` 파일을 다운로드하고 Wyse Management Suite 리포지토리 설치 프로그램을 설치합니다.
- Wyse Management Suite를 온프레미스 배포와 함께 사용하는 경우, Wyse Management Suite 설치 프로세스 중에 로컬 리포지토리가 설치됩니다.

단계

1. Windows Embedded Standard 운영 체제 이미지 또는 ThinLinux 이미지를 `<Repository Location>\repository\osImages\zipped` 폴더에 복사합니다.

   Wyse Management Suite는 압축된 폴더에서 파일을 추출하고 `<Repository Location>\repository\osImages\valid` 위치에 있는 파일을 업로드합니다. 이미지 추출은 이미지 크기에 따라 몇 분이 걸릴 수 있습니다.

   노트: ThinLinux 운영 체제의 경우 merlin 이미지(예: `1.0.7_3030LT_merlin.exe`)를 다운로드하고 `<Repository Location>\Repository\osImages\zipped` 폴더에 복사합니다.

   이미지가 리포지토리에 추가됩니다.
2. 등록된 이미지를 보려면 **앱 및 데이터** > **OS 이미지 리포지토리** > **WES/ThinLinux**로 이동합니다.

리포지토리에 ThinOS 펌웨어 추가

단계

1. **앱 및 데이터** 탭의 **OS 이미지 리포지토리** 아래에서 **ThinOS**를 클릭합니다.
2. **펌웨어 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
3. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
4. 파일에 대한 설명을 입력합니다.
5. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
6. **업로드**를 클릭합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 디바이스 또는 디바이스 그룹에 펌웨어를 배포하려면 해당 디바이스 또는 그룹 구성 페이지로 이동합니다.

ThinOS BIOS 파일을 리포지토리에 추가

단계

1. **앱 및 데이터** 탭의 **OS 이미지 리포지토리** 아래에서 **ThinOS**를 클릭합니다.
2. **BIOS 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
3. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
4. 파일에 대한 설명을 입력합니다.
5. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
6. BIOS 플랫폼 유형 드롭다운 목록에서 플랫폼을 선택합니다.
7. **업로드**를 클릭합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 디바이스 또는 디바이스 그룹에 BIOS 파일을 배포하려면 해당 디바이스 또는 그룹 구성 페이지로 이동합니다.

ThinOS 패키지 파일을 리포지토리에 추가

단계

1. **앱 및 데이터** 탭의 **OS 이미지 리포지토리** 아래에서 **ThinOS**를 클릭합니다.
2. **패키지 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
3. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
4. 파일에 대한 설명을 입력합니다.
5. **업로드**를 클릭합니다.

   노트: 애플리케이션이 공용 리포지토리에 있는 경우 애플리케이션 참조가 인벤토리에 추가됩니다. 그렇지 않으면 애플리케이션이 공용 리포지토리에 업로드되고 참조가 인벤토리에 추가됩니다. 또한 운영자가 업로드한 ThinOS 펌웨어 및 BIOS 패키지는 테넌트 관리자가 삭제할 수 없습니다.

Windows Embedded Standard 및 ThinLinux 이미지 정책 생성

단계

1. **앱 및 데이터** 탭의 **OS 이미지 정책** 아래에서 **WES / ThinLinux**를 클릭합니다.
2. **정책 추가**를 클릭합니다.
   WES/ ThinLinux 정책 추가 화면이 표시됩니다.
3. **WES/ ThinLinux 정책 추가** 페이지에서 다음을 수행합니다.

a. **정책 이름**을 입력합니다.
b. **그룹** 드롭다운 메뉴에서 그룹을 선택합니다.
c. **OS 유형** 드롭다운 메뉴에서 OS 유형을 선택합니다.
d. **OS 하위 유형 필터** 드롭다운 메뉴에서 OS 하위 유형 필터를 선택합니다.
e. 이미지를 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
f. **OS 이미지** 드롭다운 메뉴에서 이미지 파일을 선택합니다.
g. **규칙** 드롭다운 메뉴에서 이미지 정책에 대해 설정하려는 다음 규칙 중 하나를 선택합니다.
   - 업그레이드만
   - 다운그레이드 허용
   - 이 버전 강제 적용
h. **자동으로 정책 적용** 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - 자동으로 적용하지 마십시오 – 이미지 정책이 Wyse Management Suite에 등록된 디바이스에 자동으로 적용되지 않습니다.
   - 정책을 새 디바이스에 적용합니다 – 이미지 정책이 Wyse Management Suite에 등록된 새 디바이스에 적용됩니다.
   - 체크인 시 정책을 디바이스에 적용합니다 – 이미지 정책이 Wyse Management Suite에 등록된 체크인 시 새 디바이스에 적용됩니다.

4. **저장**을 클릭합니다.

리포지토리에 ThinOS 9.x 펌웨어 추가

단계

1. Wyse Management Suite로 로그인합니다.
2. **앱 및 데이터** 탭의 **OS 이미지 리포지토리**에서 **ThinOS 9.x**를 클릭합니다.
3. **펌웨어 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
4. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
5. 파일에 대한 설명을 입력합니다.
6. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
7. **업로드**를 클릭합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 디바이스 또는 디바이스 그룹에 펌웨어를 배포하려면 해당 디바이스 또는 그룹 구성 페이지로 이동합니다.

   노트: 운영자는 운영자 계정에서 펌웨어를 업로드할 수 있으며 모든 테넌트에 표시됩니다. 테넌트는 파일을 삭제하거나 수정할 수 없습니다.

ThinOS 9.x BIOS 파일을 리포지토리에 추가

단계

1. **앱 및 데이터** 탭의 **OS 이미지 리포지토리**에서 **ThinOS 9.x**를 클릭합니다.
2. **BIOS 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
3. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
4. 파일에 대한 설명을 입력합니다.
5. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
6. BIOS 플랫폼 유형 드롭다운 목록에서 플랫폼을 선택합니다.
7. **업로드**를 클릭합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 디바이스 또는 디바이스 그룹에 BIOS 파일을 배포하려면 해당 디바이스 또는 그룹 구성 페이지로 이동합니다.

   노트: 운영자는 운영자 계정에서 펌웨어를 업로드할 수 있으며 모든 테넌트에 표시됩니다. 테넌트는 파일을 삭제하거나 수정할 수 없습니다.

리포지토리에 ThinOS 애플리케이션 패키지 추가

단계

1. 테넌트 자격 증명을 사용하여 Wyse Management Suite에 로그인합니다.
2. **앱 및 데이터** 탭의 **OS 이미지 리포지토리**에서 **ThinOS 9.x**를 클릭합니다.
3. **패키지 파일 추가**를 클릭합니다.
   패키지 추가 화면이 표시됩니다.
4. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
   - EULA가 패키지에 포함된 경우 패키지의 EULA 세부 정보와 공급업체 이름이 표시됩니다. 공급업체 이름을 클릭하여 각 공급업체의 라이선스 계약을 읽을 수 있습니다. **수락**을 클릭하여 패키지를 업로드합니다. 동일한 공급업체의 EULA 세부 정보를 다시 보지 않으려면 **이 정보를 다시 표시하지 않음**을 선택할 수 있습니다. 패키지의 라이선스 계약에 개별적으로 동의해야 합니다. **거부**를 클릭하면 패키지가 업로드되지 않습니다.
   - EULA가 패키지에 포함되어 있지 않은 경우 5단계로 이동합니다.
5. **업로드**를 클릭합니다.

   노트: 운영자는 운영자 계정에서 패키지를 업로드할 수 있으며 모든 테넌트에 표시됩니다. 테넌트는 이러한 파일을 삭제하거나 수정할 수 없습니다.

Dell Hybrid Client 이미지 정책 생성

Dell Hybrid Client 이미지 정책을 생성하여 Windows 10 IoT Enterprise, ThinLinux 2.x 및 ThinOS 8.x 운영 체제를 실행하는 Wyse 5070 씬 클라이언트를 Dell Hybrid Client 디바이스로 변환할 수 있습니다.

단계

1. **앱 및 데이터** 탭의 **OS 이미지 정책**에서 **하이브리드 클라이언트**를 클릭합니다.
2. **정책 추가**를 클릭합니다.
3. **하이브리드 클라이언트 정책 추가** 페이지에서 다음을 수행합니다.
   a. **정책 이름**을 입력합니다.
   b. **그룹** 드롭다운 메뉴에서 그룹을 선택합니다.
   c. **OS 유형** 드롭다운 메뉴에서 OS 유형을 선택합니다.
   d. **OS 하위 유형 필터** 드롭다운 메뉴에서 OS 하위 유형 필터를 선택합니다.
   e. 이미지를 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
   f. **OS 이미지** 드롭다운 메뉴에서 이미지 파일을 선택합니다.
   g. **규칙** 드롭다운 메뉴에서 **이 버전 강제 적용**을 선택합니다.
   h. **자동으로 정책 적용** 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
      - 자동으로 정책을 적용하지 않음 – 이미지 정책이 Wyse Management Suite에 등록된 디바이스에 자동으로 적용되지 않습니다.
      - 새 디바이스에 정책 적용 – 이미지 정책이 Wyse Management Suite에 등록된 새 디바이스에 적용됩니다.
4. **저장**을 클릭합니다.

   노트: DHC 라이선스 수는 Dell Hybrid Client로 변환된 Wyse 5070 씬 클라이언트 수보다 크거나 같아야 합니다.

   노트: zip 또는 exe 형식으로 제공된 DHC 변환 OS 이미지를 `\repository\osImages\zipped` 폴더에 복사해야 합니다. 리포지토리 동기화 후 DHC OS 이미지가 **앱 및 데이터** > **OS 이미지 리포지토리** > **하이브리드 클라이언트**에 표시됩니다.

   노트: Windows Embedded, ThinLinux, ThinOS 및 PCoIP 운영 체제가 설치된 ThinOS를 실행하는 Wyse 5070 씬 클라이언트에 DHC 변환 이미지를 배포하려면 OS 이미지 정책을 생성해야 합니다.

   노트: Windows 10 IoT Enterprise 및 ThinLinux 2.x 운영 체제를 실행하는 씬 클라이언트의 경우 Merlin 패키지를 408 이상으로 업데이트해야 합니다.

파일 리포지토리 관리

이 섹션에서는 배경 화면, 로고, EULA 텍스트 파일, Windows 무선 프로필 및 인증서 파일과 같은 파일 리포지토리 인벤토리를 보고 관리할 수 있습니다.

단계

1. **앱 및 데이터** 탭에서 **파일 리포지토리** 아래의 **인벤토리**를 클릭합니다.
2. **파일 추가**를 클릭합니다.

   파일 추가 화면이 표시됩니다.
3. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
4. **유형** 드롭다운 메뉴에서 파일 형식에 맞는 다음 옵션 중 하나를 선택합니다.
   - 인증서
   - 배경 화면
   - 로고
   - EULA 텍스트 파일
   - Windows 무선 프로파일
   - INI 파일
   - 로캘
   - 프린터 매핑
   - 글꼴
   - 호스트
   - 규칙

   노트: 업로드할 수 있는 파일의 최대 크기 및 지원되는 형식을 보려면 정보 **정보 (i)** 아이콘을 클릭합니다.
5. 기존 파일을 덮어쓰려면 확인란을 선택합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 파일을 할당하려면 해당 디바이스 구성 페이지로 이동합니다.
6. **업로드**를 클릭합니다.

마케팅 그룹에 속한 모든 디바이스의 배경 화면을 변경하는 방법

단계

1. **앱 및 데이터** 탭으로 이동합니다.
2. 왼쪽 창의 탐색 표시줄에서 **인벤토리**를 선택합니다.
3. **파일 추가** 버튼을 클릭합니다.
4. 배경 화면으로 사용할 이미지를 찾아서 선택합니다.
5. 유형으로 **배경 화면**을 선택합니다.
6. 설명을 입력하고 **업로드**를 클릭합니다.

새 배경 화면을 할당하여 그룹의 구성 정책을 변경하려면 다음을 수행합니다.

1. **그룹 및 구성** 페이지로 이동합니다.
2. 정책 그룹을 선택합니다.
3. **정책 편집**을 클릭하고 **WES**를 선택합니다.
4. **데스크탑 환경**을 선택하고 **이 항목 구성**을 클릭합니다.
5. **데스크탑 배경 화면**를 선택합니다.
6. 드롭다운 목록에서 배경 화면 파일을 선택합니다.
7. **저장 및 게시**를 클릭합니다.

구성 정책의 상태를 확인하려면 **작업**을 클릭합니다. 디바이스의 상태를 확인하려면 **세부 내용** 열에서 상태 플래그 옆에 있는 번호를 클릭합니다.

10

규칙 관리

이 섹션에서는 Wyse Management Suite 콘솔에서 규칙을 추가 및 관리하는 방법을 설명합니다. 다음과 같은 필터링 옵션이 제공됩니다.

- **등록**
- **관리되지 않는 디바이스 자동 할당**
- **경고 알림**

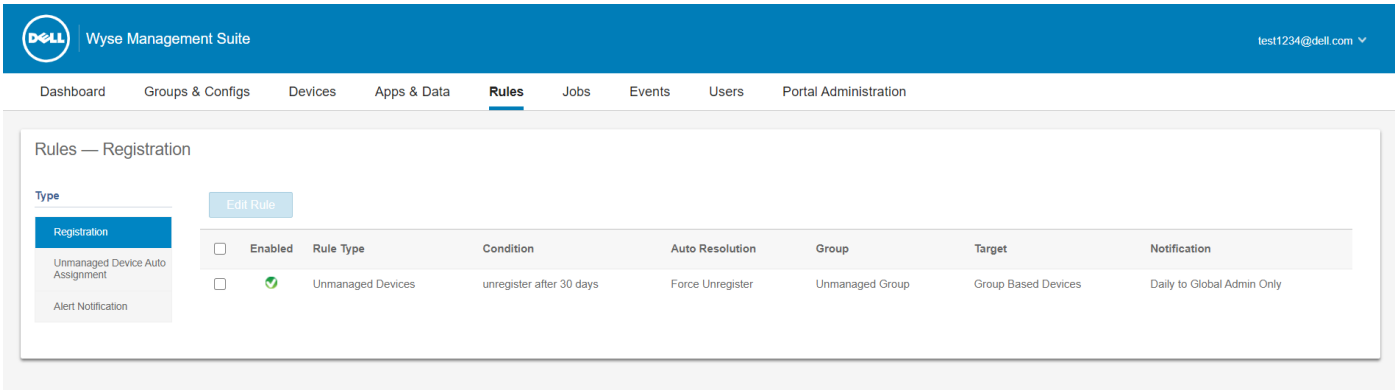


그림 9 . 규칙 페이지

주제:

- 등록 규칙 편집
- 관리되지 않는 디바이스에 대한 자동 할당 규칙 생성
- 관리되지 않는 디바이스 자동 할당 규칙 편집
- 관리되지 않는 디바이스 자동 할당에 대한 규칙 비활성화 및 삭제
- 규칙 순서 저장
- 경고 알림에 대한 규칙 추가
- 경고 알림 규칙 편집
- 디바이스 자동 등록 취소를 위한 규칙 생성

등록 규칙 편집

등록 옵션을 사용하여 관리되지 않는 디바이스에 대한 규칙을 구성합니다.

단계

1. **규칙**을 클릭합니다.
   규칙 페이지가 표시됩니다.
2. **등록**을 클릭하고 관리되지 않는 디바이스 옵션을 선택합니다.
3. **규칙 편집**을 클릭합니다.
   규칙 편집 창이 표시됩니다.

   다음과 같은 세부 정보를 볼 수 있습니다.
   - 규칙
   - 설명
   - 디바이스 대상
   - 그룹
4. 드롭다운 메뉴에서 대상 클라이언트를 선택하여 **알림 대상** 옵션과 **알림 빈도** 적용 기간 옵션을 적용합니다.

노트: 알림 주기는 대상 디바이스에 대해 매 4시간, 매 12시간, 매일 또는 매주 단위로 구성할 수 있습니다.

5. **(1–30일) 후 규칙 적용** 상자에 규칙을 적용할 때까지의 일 수를 입력합니다.

   노트: 기본적으로 관리되지 않는 디바이스의 등록은 30일 후에 등록되지 않습니다.

6. **저장**을 클릭합니다.

관리되지 않는 디바이스에 대한 자동 할당 규칙 생성

단계

1. **규칙** 탭을 클릭합니다.
2. **관리되지 않는 디바이스 자동 할당** 옵션을 선택합니다.
3. **규칙 추가** 탭을 클릭합니다.
4. **이름**을 입력하고 **대상 그룹**을 선택합니다.
5. **조건 추가** 옵션을 클릭하고 할당된 규칙의 조건을 선택합니다.
6. **저장**을 클릭합니다.
   이 규칙은 관리되지 않는 그룹 목록에 표시됩니다. 이 규칙은 자동으로 적용되고 해당 디바이스는 대상 그룹에 나열됩니다.

   노트: **등록 보류 중** 상태의 디바이스에는 규칙이 적용되지 않습니다.

관리되지 않는 디바이스 자동 할당 규칙 편집

단계

1. **규칙** 탭을 클릭합니다.
2. **관리되지 않는 디바이스 자동 할당** 옵션을 선택합니다.
3. 규칙을 선택하고 **편집** 옵션을 선택합니다.
4. **이름**을 입력하고 **대상 그룹**을 선택합니다.
5. **조건 추가** 옵션을 클릭하고 할당된 규칙의 조건을 선택합니다.
6. **저장**을 클릭합니다.

관리되지 않는 디바이스 자동 할당에 대한 규칙 비활성화 및 삭제

단계

1. **규칙** 탭을 클릭합니다.
2. **관리되지 않는 디바이스 자동 할당** 옵션을 선택합니다.
3. 규칙을 선택하고 **규칙 비활성화** 옵션을 클릭합니다.
   선택한 규칙이 비활성화됩니다.
4. 비활성화된 규칙을 선택하고 **비활성화된 규칙 삭제** 옵션을 클릭합니다.
   규칙이 삭제됩니다.

규칙 순서 저장

전제조건

여러 규칙이 있는 경우 디바이스에 적용할 규칙 순서를 변경할 수 있습니다.

단계

1. **규칙** 탭을 클릭합니다.
2. **관리되지 않는 디바이스 자동 할당** 옵션을 선택합니다.
3. 이동할 규칙을 선택한 다음 최상위 순서로 이동합니다.
4. **규칙 순서 저장**을 클릭합니다.

   노트: IPV6 접두사 규칙 순서는 변경할 수 없습니다.

경고 알림에 대한 규칙 추가

단계

1. **규칙** 탭을 클릭합니다.
2. **경고 알림** 옵션을 선택합니다.
3. **규칙 추가**를 클릭합니다.
   규칙 추가 창이 표시됩니다.
4. **규칙** 드롭다운 목록에서 규칙을 선택합니다.
5. **설명**을 입력합니다.
6. **그룹** 드롭다운 목록에서 기본 설정 옵션을 선택합니다.
7. 드롭다운 메뉴에서 **알림 대상**을 적용할 대상 디바이스와 **알림 빈도**를 적용할 지속 시간을 선택합니다.
8. **저장**을 클릭합니다.

경고 알림 규칙 편집

단계

1. **규칙** 탭을 클릭합니다.
2. **경고 알림** 옵션을 선택합니다.
3. **규칙 편집**을 클릭합니다.
   규칙 편집 창이 표시됩니다.
4. **규칙** 드롭다운 목록에서 규칙을 선택합니다.
5. **설명**을 입력합니다.
6. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
7. 드롭다운 목록에서 **알림 대상**을 적용할 대상 디바이스와 **알림 빈도**를 적용할 지속 시간을 선택합니다.
8. **저장**을 클릭합니다.

디바이스 자동 등록 취소를 위한 규칙 생성

Wyse Management Suite 3.2에서 일정 기간 동안 Wyse Management Suite에 체크인하지 않는 경우 디바이스를 자동으로 등록 취소하는 규칙을 생성할 수 있습니다.

단계

1. **규칙** 탭을 클릭합니다.
2. **체크인 실패** 옵션을 클릭합니다.

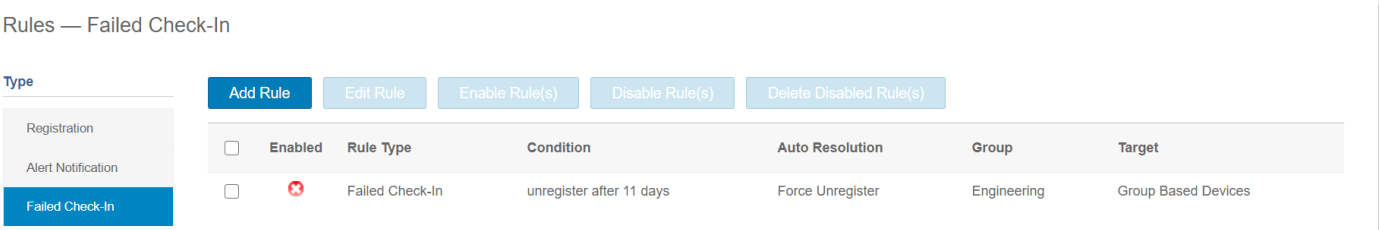


그림 10 . 체크인 실패 탭

3. **규칙 추가**를 클릭합니다.
   규칙 추가 창이 표시됩니다.

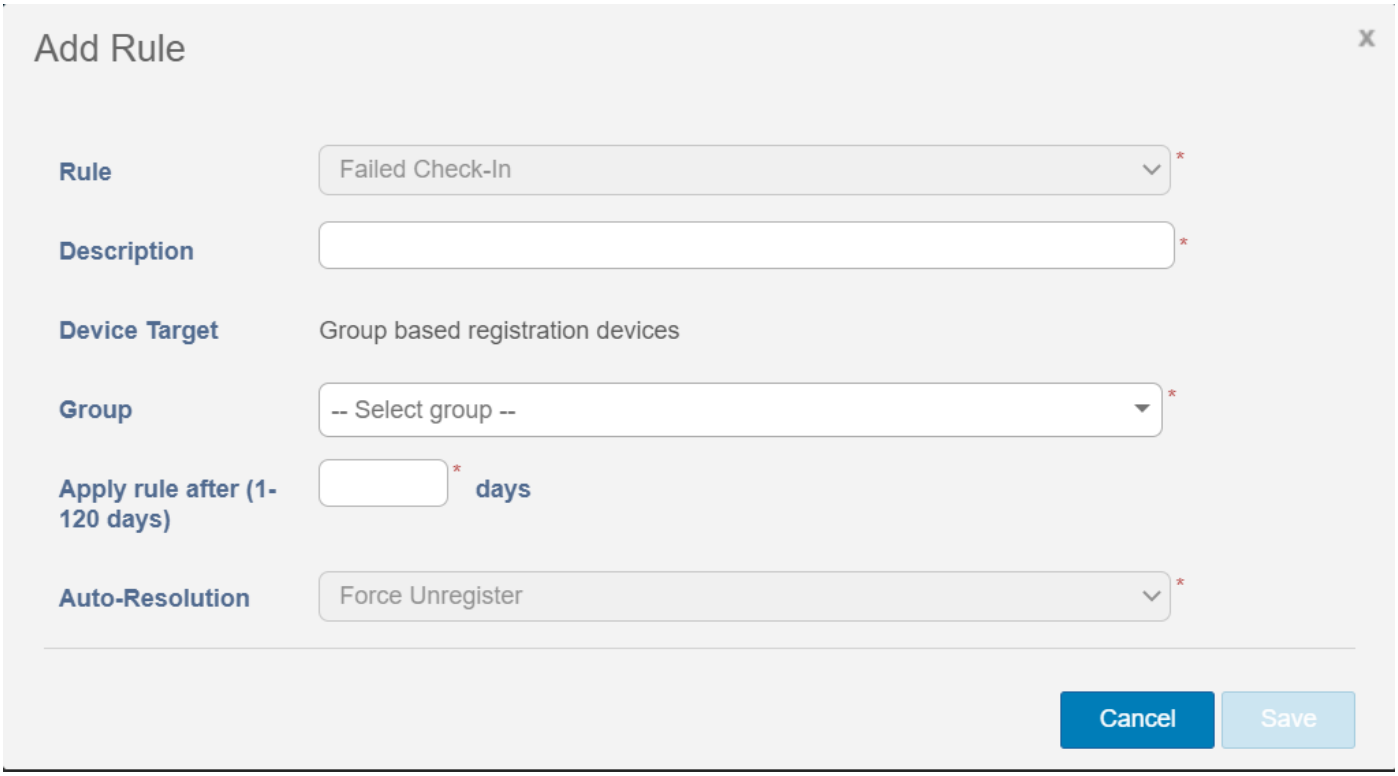


그림 11 . 규칙 추가

4. 규칙에 대한 설명을 입력합니다.
5. 디바이스를 등록 취소해야 하는 그룹을 선택합니다.
6. **1~120일 이후 규칙 적용** 필드에 Wyse Management Suite에서 디바이스가 등록 취소되기 전까지 유지되는 기간을 일 단위로 입력합니다.

   노트: 디바이스가 지정된 기간 동안 체크인하지 않는 경우에만 디바이스가 Wyse Management Suite에서 등록 취소됩니다.
7. **저장**을 클릭합니다.
   규칙을 편집, 활성화, 비활성화 또는 삭제할 수도 있습니다.

11

작업 관리

이 섹션에서는 관리 콘솔에서 작업을 예약하고 관리하는 방법에 대해 설명합니다.

이 페이지에서는 다음 필터링 옵션을 기반으로 작업을 볼 수 있습니다.

- **구성 그룹**—드롭다운 메뉴에서 구성 그룹 유형을 선택합니다.
- **예약자**—드롭다운 메뉴에서 예약 작업을 수행한 예약자를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
  - 관리자
    - 앱 정책
    - 이미지 정책
    - 디바이스 명령
  - 시스템
    - 그룹 구성 게시
    - 기타
- **OS 유형**—드롭다운 메뉴에서 운영 체제를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse 소프트웨어 씬 클라이언트
  - 하이브리드 클라이언트
  - 일반 클라이언트
- **상태**—드롭다운 메뉴에서 작업 상태를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
  - 예약됨
  - 실행 중/진행 중
  - 완료됨
  - 취소됨
  - 실패함
- **세부 상태**—드롭다운 메뉴에서 세부 상태를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
  - 하나 이상 실패함
  - 하나 이상 보류 중
  - 하나 이상 진행 중
  - 하나 이상 취소됨
  - 하나 이상 완료됨
- **기타 작업**—드롭다운 메뉴에서 **BIOS 관리자 암호 동기화** 옵션을 선택합니다. BIOS 관리자 암호 동기화 작업 창이 표시됩니다.

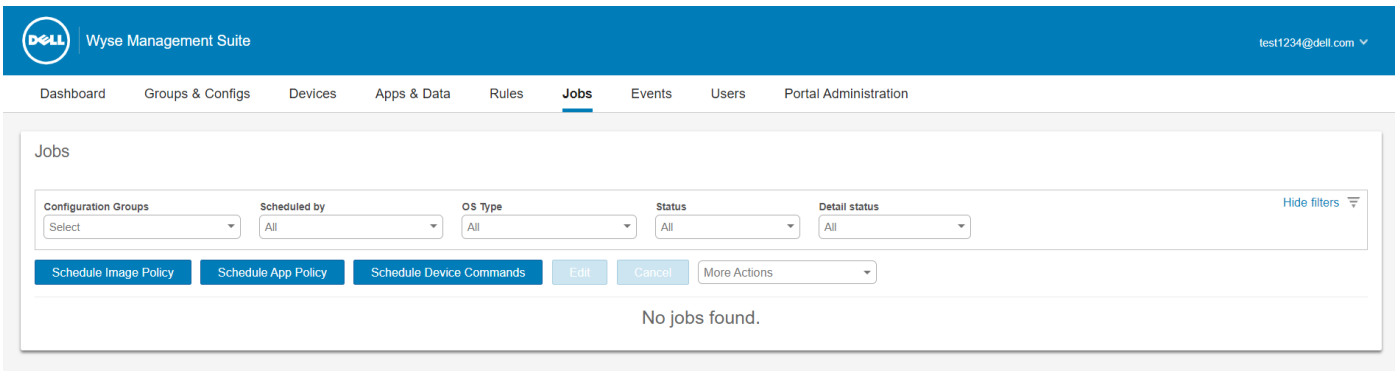


그림 12 . 작업 페이지

주제:

- BIOS 관리자 암호 동기화
- 필터를 사용하여 예약된 작업 검색
- 디바이스 명령 작업 예약
- 이미지 정책 예약
- 애플리케이션 정책 예약
- 실패한 작업 재시작

BIOS 관리자 암호 동기화

단계

1. **작업**을 클릭합니다.
   작업 페이지가 표시됩니다.
2. **기타 작업** 드롭다운 메뉴에서 **BIOS 관리자 암호 동기화** 옵션을 선택합니다.
   BIOS 관리자 암호 동기화 작업 창이 표시됩니다.
3. 암호를 입력합니다. 암호는 최소 4자, 최대 32자여야 합니다.
4. 암호를 보려면 **암호 보기** 확인란을 선택합니다.
5. **OS 유형** 드롭다운 메뉴에서 기본 설정 옵션을 선택합니다.
6. **플랫폼** 드롭다운 메뉴에서 기본 설정 옵션을 선택합니다.
7. 작업 이름을 입력합니다.
8. **그룹** 드롭다운 메뉴에서 기본 설정 옵션을 선택합니다.
9. 하위 그룹을 포함하려면 **모든 하위 그룹 포함** 확인란을 선택합니다.
10. **설명** 상자에 설명을 입력합니다.
11. **미리 보기**를 클릭합니다.

필터를 사용하여 예약된 작업 검색

이 섹션에서는 관리 콘솔에서 예약된 작업을 검색하고 작업을 관리하는 방법을 설명합니다.

단계

1. **작업**을 클릭합니다.
   작업 페이지가 표시됩니다.
2. **구성 그룹** 드롭다운 메뉴에서 기본 정책 그룹 또는 관리자가 추가한 그룹을 선택합니다.
3. **예약자** 드롭다운 메뉴에서 예약 작업을 수행한 예약자를 선택합니다.
   사용 가능한 옵션은 다음과 같습니다.
   - 관리자
     - 앱 정책
     - 이미지 정책
     - 디바이스 명령
   - 시스템
     - 그룹 구성 게시
     - 기타
4. **OS 유형** 드롭다운 메뉴에서 운영 체제를 선택합니다.
   사용 가능한 옵션은 다음과 같습니다.
   - ThinOS
   - WES
   - Linux
   - Thin Linux
   - Wyse 소프트웨어 씬 클라이언트
   - Teradici-프라이빗 클라우드

- Dell Hybrid Client

5. **상태** 드롭다운 메뉴에서 작업의 상태를 선택합니다.
   사용 가능한 옵션은 다음과 같습니다.
   - 예약됨
   - 실행 중/진행 중
   - 완료됨
   - 취소됨
   - 실패함
6. **세부 상태** 드롭다운 메뉴에서 세부 상태를 선택합니다.
   사용 가능한 옵션은 다음과 같습니다.
   - 하나 이상 실패함
   - 하나 이상 보류 중
   - 하나 이상 진행 중
   - 하나 이상 취소됨
   - 하나 이상 완료됨
7. **기타 작업** 드롭다운 메뉴에서 **BIOS 관리자 암호 동기화** 옵션을 선택합니다.
   BIOS 관리자 암호 동기화 작업 창이 표시됩니다. 자세한 내용은 BIOS 관리자 암호 동기화를 참조하십시오.

디바이스 명령 작업 예약

단계

1. **작업** 페이지에서 **디바이스 명령 작업 예약**을 클릭합니다.
   디바이스 명령 작업 화면이 표시됩니다.
2. 다음 옵션을 구성합니다.
   a. **명령** 드롭다운 목록에서 명령을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.
      - Restart
      - Wake On LAN
      - Shutdown
      - Query
      - Reimage
      - Lock - ThinOS 8.x 및 ThinOS 9.x 디바이스에 적용
      - Send message - Windows Embedded, ThinLinux, ThinOS 8.x, ThinOS 9.x 및 Dell Hybrid Client 기반 디바이스에 적용
      - Factory Reset - ThinOS 8.x, ThinOS 9.x 및 Dell Hybrid Client 기반 디바이스에 적용

      디바이스 명령은 반복되는 작업입니다. 선택한 요일 및 특정 시간에 명령이 선택한 디바이스로 전송됩니다.
   b. **OS 유형** 드롭다운 목록에서 운영 체제 유형을 선택합니다.
   c. **이름** 필드에 작업 이름을 입력합니다.
   d. **그룹** 드롭다운 목록에서 그룹 이름을 선택합니다.
   e. 작업 설명을 입력합니다.
   f. **실행** 드롭다운 목록에서 날짜 또는 시간을 선택합니다.
   g. 다음 세부 정보를 입력하거나 선택합니다.
      - **유효** - 시작 및 종료 날짜를 입력합니다.
      - **시작 및 종료 시간** - 시작 시간과 종료 시간을 입력합니다.
      - **요일** - 요일을 선택합니다.
3. 예약된 작업의 세부 정보를 보려면 **미리 보기** 옵션을 클릭합니다.
4. 다음 페이지에서 **예약** 옵션을 클릭하여 작업을 시작합니다.

이미지 정책 예약

이미지 정책은 반복 작업이 아닙니다. 각 명령은 디바이스에 따라 다릅니다.

단계

1. **작업** 페이지에서 **이미지 정책 예약** 옵션을 클릭합니다.
   이미지 업데이트 작업 화면이 표시됩니다.
2. 드롭다운 목록에서 정책을 선택합니다.
3. 작업 설명을 입력합니다.
4. 드롭다운 목록에서 날짜 또는 시간을 선택합니다.
5. 다음 세부 정보를 입력하거나 선택합니다.
   - **유효** - 시작 및 종료 날짜를 입력합니다.
   - **시작 및 종료 시간** - 시작 시간과 종료 시간을 입력합니다.
   - **요일** - 요일을 선택합니다.
6. 예약된 작업의 세부 정보를 보려면 **미리 보기** 옵션을 클릭합니다.
7. 작업을 시작하려면 **예약** 옵션을 클릭합니다.

애플리케이션 정책 예약

애플리케이션 정책은 반복 작업이 아닙니다. 각 명령은 디바이스에 따라 다릅니다.

단계

1. **작업** 페이지에서 **애플리케이션 정책 예약** 옵션을 클릭합니다.
   앱 정책 작업 화면이 표시됩니다.
2. 드롭다운 목록에서 정책을 선택합니다.
3. 작업 설명을 입력합니다.
4. 드롭다운 목록에서 날짜 또는 시간을 선택합니다.
5. 다음 세부 정보를 입력하거나 선택합니다.
   - **유효** - 시작 및 종료 날짜를 입력합니다.
   - **시작 및 종료 시간** - 시작 시간과 종료 시간을 입력합니다.
   - **요일** - 요일을 선택합니다.
6. 예약된 작업의 세부 정보를 보려면 **미리 보기** 옵션을 클릭합니다.
7. 다음 페이지에서 **예약** 옵션을 클릭하여 작업을 시작합니다.

실패한 작업 재시작

Wyse Management Suite 3.2에서 디바이스 명령, 애플리케이션 정책 및 이미지 정책의 실패한 작업을 재시작할 수 있습니다. 실패한 작업에 대한 일정을 생성할 수도 있습니다. 이 옵션은 Pro 라이선스가 있는 Wyse Management Suite에만 적용할 수 있습니다.

전제조건

- 작업은 예약되어 실패한 작업이어야 합니다.
- 예약된 작업은 디바이스 명령, 애플리케이션 정책 또는 이미지 정책이어야 합니다.

단계

1. **작업** 탭을 클릭합니다.
2. 실패한 작업을 선택하고 **실패한 작업 재시작**을 클릭합니다.
   작업 상태가 **재시작됨**으로 변경됩니다.
3. **실행** 드롭다운 목록에서 작업을 예약합니다.
4. 예약된 작업의 세부 정보를 보려면 **미리 보기** 옵션을 클릭합니다.
5. 다음 페이지에서 **예약** 옵션을 클릭하여 작업을 시작합니다.

   노트: 전역 관리자, 맞춤 구성 역할을 보유한 사용자(작업 권한이 할당된 경우) 또는 특정 그룹의 그룹 관리자는 실패한 작업을 재시작할 수 있습니다.

   노트: 실패한 작업에 대해 새 하위 작업이 생성되므로 실패한 작업은 한 번만 재시작할 수 있습니다.

12

이벤트 관리

이벤트 페이지에서는 관리 시스템에서 관리 콘솔을 사용하여 모든 이벤트 및 경고를 확인할 수 있습니다. 또한 시스템 감사 목적으로 이벤트 및 경고 감사를 보는 지침을 제공합니다.

이벤트 및 경고 요약은 시스템에서 발생한 일에 대한 읽기 쉬운 일일 요약을 얻는 데 사용됩니다. **감사** 창은 정보를 일반적인 감사 로그 보기로 정렬합니다. 각 이벤트의 타임스탬프, 이벤트 유형, 소스 및 설명을 시간 순서대로 볼 수 있습니다.

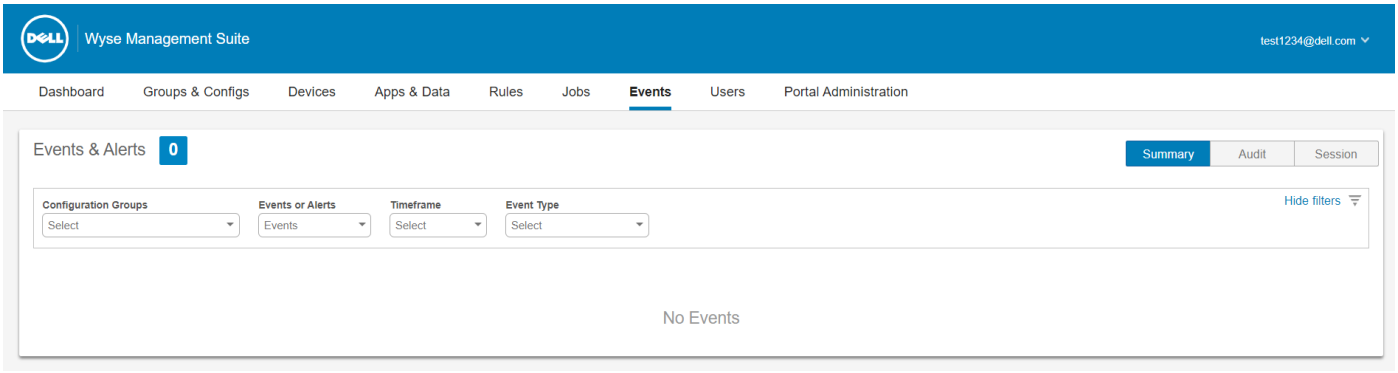


그림 13 . 이벤트 페이지

주제:

- 필터를 사용하여 이벤트 또는 경고 검색
- 이벤트 요약 보기
- 감사 로그 보기
- 최종 사용자 세션 보고

필터를 사용하여 이벤트 또는 경고 검색

단계

1. **이벤트**를 클릭합니다.
   이벤트 페이지가 표시됩니다.
2. **구성 그룹** 드롭다운 메뉴에서 기본 정책 그룹 또는 관리자가 추가한 그룹을 선택합니다.
3. **이벤트 또는 경고** 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - 이벤트
   - 현재 경고
   - 경고 내역
4. **기간 범위** 드롭다운 메뉴에서 다음 운영 체제 중 하나를 선택합니다.
   이 옵션을 사용하면 특정 시간대에 발생한 이벤트를 볼 수 있습니다. 드롭다운 메뉴에서 사용할 수 있는 옵션은 다음과 같습니다.
   - 오늘
   - 어제
   - 이번 주
   - 맞춤 지정
5. **이벤트 유형** 드롭다운 메뉴에서 운영 체제를 선택합니다.
   모든 이벤트는 특정 그룹으로 분류됩니다. 드롭다운 메뉴에서 사용할 수 있는 옵션은 다음과 같습니다.
   - 액세스
   - 등록
   - 구성

- 원격 명령
- 관리
- 준수

이벤트 요약 보기

이벤트 및 경고 창에는 시스템에서 발생한 모든 이벤트와 경고가 표시됩니다. **이벤트** > **요약**로 이동합니다.

감사 로그 보기

감사 창은 정보를 일반적인 감사 로그 보기로 정렬합니다. 각 이벤트의 타임스탬프, 이벤트 유형, 소스 및 설명을 시간 순서대로 볼 수 있습니다.

단계

1. **이벤트** > **감사**로 이동합니다.
2. **구성 그룹** 드롭다운 목록에서 감사 로그를 볼 그룹을 선택합니다.
3. **기간 범위** 드롭다운 목록에서 해당 기간 동안 발생한 이벤트를 볼 기간을 선택합니다.

   노트: 감사 파일은 번역되지 않으며 영어로만 제공됩니다.

최종 사용자 세션 보고

최종 사용자 세션 보고 옵션을 사용하여 서로 다른 시간 간격 동안 사용자 세션을 보고할 수 있습니다.

전제조건

세션 보고 활성화 옵션을 활성화해야 합니다. 자세한 내용은 Dell Hybrid Client에 대한 Wyse Management Suite 클라이언트 설정 구성을 참조하십시오.

단계

1. **이벤트**를 클릭합니다.
   이벤트 페이지가 표시됩니다.
2. **세션**을 클릭합니다.
   최종 사용자 세션 페이지가 표시됩니다.
3. **기간** 드롭다운 메뉴에서 옵션을 선택하여 이벤트를 봅니다. 드롭다운 메뉴에서 사용할 수 있는 옵션은 다음과 같습니다.
   - 오늘
   - 어제
   - 이번 주
   - 맞춤형

13

사용자 관리

이 섹션에서는 관리 콘솔에서 일상적인 사용자 관리 작업을 수행하는 방법을 설명합니다. 세 가지 사용자 유형이 있습니다.

- **관리자** – Wyse Management Suite 관리자는 전역 관리자, 그룹 관리자 또는 뷰어 역할을 할당할 수 있습니다.
  - 전역 관리자는 모든 Wyse Management Suite 기능에 액세스할 수 있습니다.
  - 그룹 관리자는 자신에게 할당된 특정 그룹의 모든 자산과 기능에 액세스할 수 있습니다.
  - 뷰어는 모든 데이터에 대한 읽기 전용 액세스 권한을 가지며, 종료 및 재시작과 같은 특정 실시간 명령을 트리거할 수 있습니다.

  관리자를 선택한 경우 다음과 같은 작업을 수행할 수 있습니다.
  - 관리자 추가
  - 관리자 편집
  - 관리자 활성화
  - 관리자 비활성화
  - 관리자 삭제
  - 관리자 잠금 해제

- **할당되지 않은 관리자** – AD 서버에서 가져온 사용자는 **할당되지 않은 관리자** 페이지에 표시됩니다. 나중에 포털에서 이러한 사용자에게 역할을 할당할 수 있습니다.

  사용자를 더 빠르고 효과적으로 관리하려면 사용 가능한 필터 옵션에 따라 원하는 사용자를 선택합니다. **할당되지 않은 사용자**를 선택한 경우 다음 작업을 수행할 수 있습니다.
  - 사용자 추가
  - 사용자 편집
  - 사용자 활성화
  - 사용자 비활성화
  - 사용자 삭제

- **최종 사용자** - **최종 사용자** 탭을 사용하여 Wyse Management Suite에 개별 사용자를 추가할 수 있습니다. 개별 사용자에게 설정을 구성하고 배포할 수 있습니다. 설정은 사용자 계정에 적용되며 사용자가 로그인할 때 씬 클라이언트에 적용됩니다. 이 옵션은 ThinOS 9.x 운영 체제 및 Dell Hybrid Client를 실행하는 씬 클라이언트에만 적용됩니다.

노트: .CSV 파일에서만 사용자를 대량으로 가져올 수 있습니다. Active Directory에서 최종 사용자를 대량으로 가져올 수 없습니다.

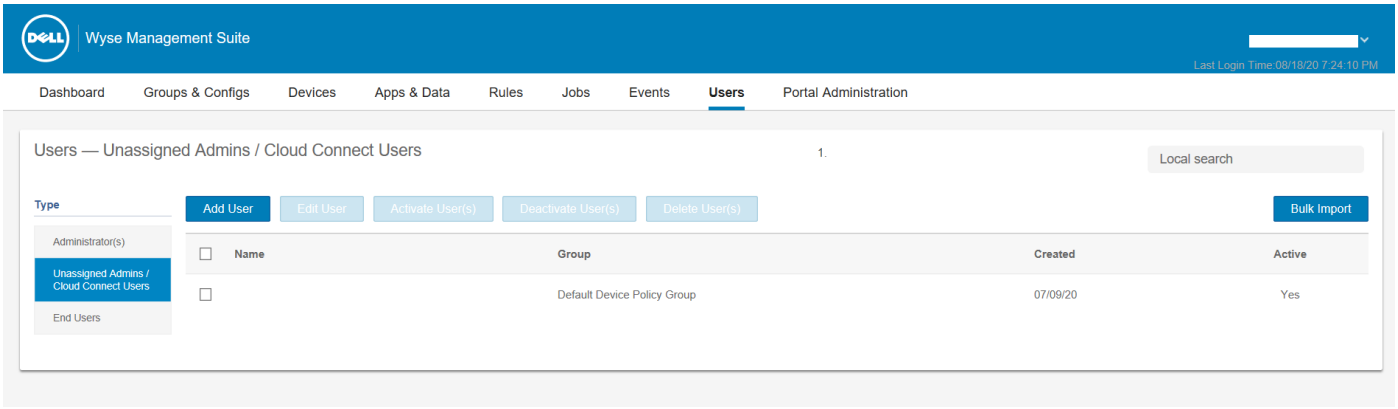


그림 14 . 사용자 페이지

주제:

- 새 관리자 프로필 추가
- Wyse Management Suite에서 WMS 맞춤 구성 역할 생성
- 가져온 AD 그룹에 WMS 맞춤 구성 역할 할당

- 할당되지 않은 관리자 또는 클라우드 연결 사용자 대량 가져오기
- 관리자 프로필 편집
- 관리자 프로필 활성화
- 관리자 프로필 비활성화
- 관리자 프로필 삭제
- 관리자 프로필 잠금 해제
- 관리자 프로필 비활성화
- 관리되지 않는 디바이스에 대한 자동 할당 규칙 생성
- 최종 사용자 추가
- 최종 사용자 편집
- 최종 사용자 정책 구성
- 최종 사용자 대량 가져오기
- 최종 사용자 삭제
- 사용자 프로파일 편집

새 관리자 프로필 추가

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. **관리자 추가**를 클릭합니다.
   새 관리자 사용자 창이 표시됩니다.
4. 해당 필드에 이메일 ID와 사용자 이름을 입력합니다.
5. 이메일에 표시된 것과 동일한 사용자 이름을 사용하려면 확인란을 선택합니다.
6. 다음 중 하나를 수행합니다.
   - **개인 정보** 탭을 클릭한 경우 다음 세부 사항을 입력합니다.
     - 이름
     - 성
     - 제목
     - 휴대폰 번호
   - **역할** 탭을 클릭한 경우 다음 세부 사항을 입력합니다.
     a. **역할** 섹션의 **역할** 드롭다운 목록에서 **관리자 역할**을 선택합니다.
        - 전역 관리자
        - 그룹 관리자
        - 뷰어

        노트: **관리자 역할**을 **뷰어**로 선택하면 다음과 같은 관리 작업이 표시됩니다.
        - 디바이스 쿼리
        - 디바이스 등록 해제
        - 재시작/종료 디바이스
        - 그룹 할당 변경
        - 원격 그림자
        - 디바이스 잠금
        - 디바이스 지우기
        - 메시지 전송
        - WOL 디바이스

     b. **암호** 섹션에 맞춤형 암호를 입력합니다. 임의의 암호를 생성하려면 **임의의 암호 생성** 라디오 버튼을 선택합니다.
7. **저장**을 클릭합니다.

Wyse Management Suite에서 WMS 맞춤 구성 역할 생성

전역 관리자는 Wyse Management Suite 3.1 이상 버전을 사용하여 새 관리자 역할을 생성하고 Wyse Management Suite의 다양한 기능에 대한 세부 사용 권한을 제공할 수 있습니다. 맞춤 구성 전역 관리자 역할을 사용하여 여러 사용자를 생성할 수 있습니다.

단계

1. **사용자** 탭으로 이동합니다.
2. **관리자**를 클릭합니다.
3. **관리자 추가**를 클릭합니다.
   새 관리자 사용자 창이 표시됩니다.
4. 해당 필드에 이메일 ID와 사용자 이름을 입력합니다.
5. **역할**을 클릭합니다.
6. **역할** 드롭다운 목록에서 **맞춤 구성 WMS 역할**을 선택합니다.
7. 각 범주에서 사용자가 수행할 수 있는 적절한 기능을 선택합니다.
8. **저장**을 클릭합니다.
   다음 표에서는 맞춤 구성 역할에 할당할 수 있는 지원되는 사용 권한과 지원되지 않는 사용 권한에 대한 세부 정보를 제공합니다.

표 10. 맞춤 구성 역할에 대한 사용 권한

지원됨	지원되지 않음
구성 편집 또는 제거	대량 디바이스 예외
그룹 추가, 편집, 삭제	그룹 관리자 생성
참조 파일 업로드	전역 관리자 생성
디바이스 세부 정보 예외 생성	뷰어 관리자 생성
규칙	할당되지 않은 관리자에게 역할 할당
앱 및 데이터	구독(라이선스 가져오기 및 내보내기)
최종 사용자 대량 가져오기	WMS 서버 URL 변경
원격 리포지토리 관리	MQTT URL 변경
보고서	구성 UI 업로드
기타	맞춤 구성 브랜딩
포털 관리 페이지의 Active Directory	

가져온 AD 그룹에 WMS 맞춤 구성 역할 할당

Wyse Management Suite 3.2의 Active Directory에서 가져온 그룹에 역할을 할당할 수 있습니다. 그룹에 할당된 권한은 그룹의 모든 사용자에게 적용됩니다.

단계

1. 전역 관리자로 로그인합니다.
2. **포털 관리** > **Active Directory** > **한 번 가져오기**로 이동하여 자격 증명을 입력합니다.
   도메인의 모든 그룹이 왼쪽 창에 나열됩니다.
3. 가져오려는 그룹을 선택합니다.
   선택한 그룹이 페이지의 오른쪽 창으로 이동합니다.
4. **역할 할당** 확인란을 선택하여 그룹 역할 할당을 위한 그룹을 가져옵니다.

   노트: **역할 할당** 옵션을 선택하지 않으면 그룹이 기본 사용자 정책 그룹에 추가되고 **그룹** 페이지에서 볼 수 있습니다.

5. **그룹 가져오기**를 클릭합니다.
   그룹을 가져오고 기본 역할을 할당합니다.
6. **사용자** 탭으로 이동하고 **그룹 할당**을 클릭합니다.

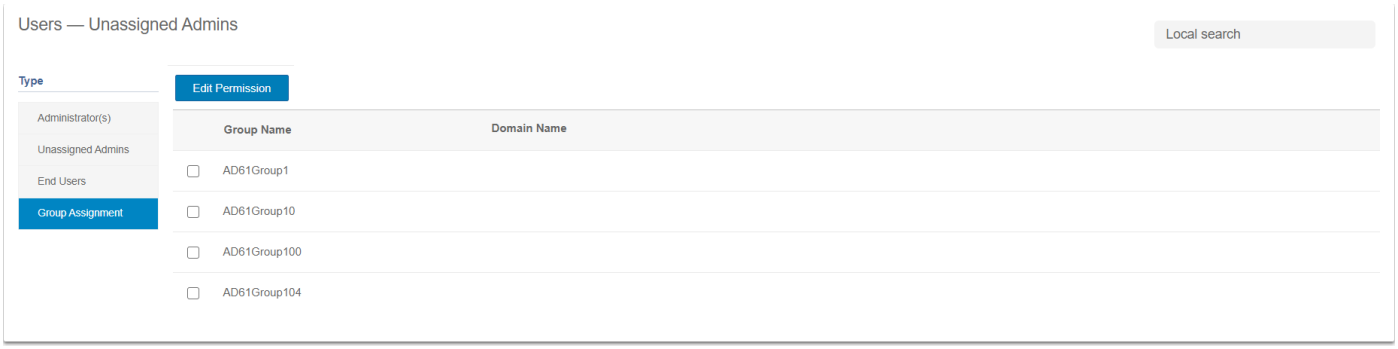


그림 15 . 그룹 할당

가져온 그룹이 **그룹 할당** 탭에 나열됩니다.

7. 역할을 할당하려는 그룹을 선택하고 **권한 편집**을 클릭합니다.
   역할 창이 표시됩니다.
8. 드롭다운 목록에서 할당하려는 역할을 선택하고 **저장**을 클릭합니다.

노트: 사용자가 그룹 역할 할당을 사용하여 이미 역할을 할당한 경우 **사용자** > **관리자**로 이동하여 개별 사용자 또는 하위 그룹의 권한을 편집합니다. 이러한 권한은 그룹 역할 할당보다 우선합니다.

노트: 퍼블릭 클라우드의 경우 Wyse Management Suite 리포지토리 버전 3.2를 사용하여 WMS 맞춤 구성 역할을 할당할 수 있습니다.

노트: 도메인 사용자로 로그인하려면 먼저 그룹을 가져온 다음 사용자를 가져와야 합니다. 그런 다음 그룹 할당 탭을 사용하여 그룹에 역할을 할당할 수 있습니다.

노트: 사용자를 가져오려면 Active Directory에 구성된 이름, 성 및 이메일이 사용자 세부 정보에 있어야 합니다. 이러한 사용자는 **할당되지 않은 관리자** 탭에 나열됩니다.

노트: 도메인 컨트롤러는 하나만 추가할 수 있습니다. 여러 도메인을 가져올 때 사용자는 서버에 로그인할 수 없습니다.

할당되지 않은 관리자 또는 클라우드 연결 사용자 대량 가져오기

단계

1. **사용자**를 클릭합니다.
   사용자 페이지가 표시됩니다.
2. **할당되지 않은 관리자** 옵션을 선택합니다.
3. **대량 가져오기**를 클릭합니다.
   대량 가져오기 창이 표시됩니다.
4. **찾아보기**를 클릭하고 CSV 파일을 선택합니다.
5. 사용자 그룹을 선택하여 가져온 사용자를 할당해야 합니다.
6. **가져오기**를 클릭합니다.

관리자 프로필 편집

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. **관리자 편집**을 클릭합니다.
   관리자 사용자 편집 창이 표시됩니다.
4. 해당 필드에 이메일 ID와 사용자 이름을 입력합니다.

노트: 로그인 이름을 업데이트하면 콘솔에서 강제로 로그아웃됩니다. 업데이트된 계정 로그인 이름을 사용하여 콘솔에 로그인합니다.

5. 다음 중 하나를 수행합니다.
   - **개인 정보** 탭을 클릭한 경우 다음 세부 사항을 입력합니다.
     - 이름
     - 성
     - 제목
     - 휴대폰 번호
   - **역할** 탭을 클릭한 경우 다음 세부 사항을 입력합니다.
     a. **역할** 섹션의 **역할** 드롭다운 목록에서 **관리자 역할**을 선택합니다.
     b. **암호** 섹션에 맞춤형 암호를 입력합니다. 임의의 암호를 생성하려면 **임의의 암호 생성** 라디오 버튼을 선택합니다.
6. **저장**을 클릭합니다.

관리자 프로필 활성화

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. 활성화할 관리자를 선택합니다.
4. **관리자 활성화**를 클릭합니다.

관리자 프로필 비활성화

관리자 프로필을 비활성화하면 콘솔에 로그인할 수 없고 등록된 디바이스 목록에서 계정이 제거됩니다.

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. 목록에서 사용자를 선택하고 **관리자 비활성화**를 클릭합니다.
   경고 창이 표시됩니다.
4. **확인**을 클릭합니다.

관리자 프로필 삭제

이 작업 정보

프로필을 삭제하기 전에 관리자를 비활성화해야 합니다. 관리자 프로필을 삭제하려면 다음을 수행합니다.

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. 삭제할 특정 관리자의 확인란을 선택합니다.
4. **관리자 삭제**를 클릭합니다.
   경고 창이 표시됩니다.
5. **삭제** 링크를 활성화하기 위해 삭제 이유를 입력합니다.
6. **삭제**를 클릭합니다.

관리자 프로필 잠금 해제

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. 잠금 해제하려는 관리자를 선택합니다.
4. **관리자 잠금 해제**를 클릭합니다.

관리자 프로필 비활성화

단계

1. **사용자**를 클릭합니다.
2. **관리자**를 클릭합니다.
3. 비활성화하려는 관리자를 선택합니다.
4. **관리자 비활성화**를 클릭합니다.

관리되지 않는 디바이스에 대한 자동 할당 규칙 생성

단계

1. **규칙** 탭을 클릭합니다.
2. **관리되지 않는 디바이스 자동 할당** 옵션을 선택합니다.
3. **규칙 추가** 탭을 클릭합니다.
4. **이름**을 입력하고 **대상 그룹**을 선택합니다.
5. **조건 추가** 옵션을 클릭하고 할당된 규칙의 조건을 선택합니다.
6. **저장**을 클릭합니다.
   이 규칙은 관리되지 않는 그룹 목록에 표시됩니다. 이 규칙은 자동으로 적용되고 해당 디바이스는 대상 그룹에 나열됩니다.

최종 사용자 추가

단계

1. **사용자** 탭을 클릭합니다.
2. **최종 사용자**를 클릭합니다.
3. **사용자 추가**를 클릭합니다.
4. 사용자 이름, 도메인, 이름, 성, 이메일 주소, 직함 및 전화 번호를 입력합니다.
5. **저장**을 클릭합니다.

최종 사용자 편집

단계

1. **사용자** 탭을 클릭합니다.
2. **최종 사용자**를 클릭합니다.
3. **최종 사용자 편집**을 클릭합니다.
4. 해당 필드에 이메일 ID와 사용자 이름을 입력합니다.
5. **저장**을 클릭합니다.

최종 사용자 정책 구성

개별 사용자에게 설정을 구성하고 배포할 수 있습니다. 설정은 사용자 계정에 적용되며 사용자가 로그인할 때 씬 클라이언트에 적용됩니다. 이 옵션은 ThinOS 9.x 운영 체제 및 Dell Hybrid Client를 실행하는 씬 클라이언트에만 적용됩니다.

단계

1. **사용자** 탭을 클릭합니다.
2. **최종 사용자**를 클릭합니다.
3. 사용자를 선택합니다.
   최종 사용자 세부 정보 페이지가 표시됩니다.
4. **정책 편집** 드롭다운 메뉴를 클릭하고 운영 체제를 선택합니다.
5. 필요한 정책을 구성하고 **저장 및 게시**를 클릭합니다.

   노트: 온프레미스 환경에서는 사용자 수에 제한이 없습니다. 10,000명의 사용자를 퍼블릭 클라우드 환경에 추가할 수 있습니다.

최종 사용자 대량 가져오기

단계

1. **사용자** 탭을 클릭합니다.
2. **최종 사용자**를 클릭합니다.
3. **대량 가져오기**를 클릭합니다.
4. **찾아보기**를 클릭하고 .csv 파일을 선택합니다.
5. .csv 파일에 헤더가 있는 경우 **CSV 파일에 헤더 줄 있음** 옵션을 선택합니다.
6. **사용자 그룹 선택** 드롭다운 목록에서 사용자를 추가할 사용자 그룹을 선택합니다.
7. **가져오기**를 클릭합니다.

   노트: 파일당 최대 100명의 사용자를 Wyse Management Suite에 추가할 수 있으며 .csv 파일의 파일 크기는 150KB를 초과할 수 없습니다.

   노트: 퍼블릭 클라우드에 최대 10,000명의 사용자를 추가할 수 있습니다. 프라이빗 클라우드에 추가할 수 있는 사용자 수는 제한이 없습니다.

최종 사용자 삭제

단계

1. **최종 사용자** 탭을 클릭합니다.
2. **최종 사용자 삭제**를 클릭합니다.
   경고 창이 표시됩니다. 삭제 링크를 활성화하기 위해 삭제 이유를 입력합니다.
3. **삭제**를 클릭합니다.

사용자 프로파일 편집

단계

1. **사용자**를 클릭합니다.
2. **할당되지 않은 관리자**를 클릭합니다.
3. **사용자 편집**을 클릭합니다.
   관리자 사용자 편집 창이 표시됩니다.
4. 해당 필드에 이메일 ID와 사용자 이름을 입력합니다.

노트: 로그인 이름을 업데이트하면 콘솔에서 강제로 로그아웃됩니다. 업데이트된 계정 로그인 이름을 사용하여 콘솔에 로그인합니다.

5. 다음 중 하나를 수행합니다.
   - **개인 정보** 탭을 클릭하고 다음 세부 사항을 입력합니다.
     - 이름
     - 성
     - 제목
     - 휴대폰 번호
   - **역할** 탭을 클릭하고 세부 사항을 입력합니다.
     a. **역할** 섹션의 **역할** 드롭다운 목록에서 **관리자 역할**을 선택합니다.
     b. **암호** 섹션에 맞춤형 암호를 입력합니다. 임의의 암호를 생성하려면 **임의의 암호 생성** 라디오 버튼을 선택합니다.
6. **저장**을 클릭합니다.

14

포털 관리

이 섹션에서는 시스템 설정 및 유지 관리에 필요한 시스템 관리 작업에 대한 간략한 개요를 다룹니다.

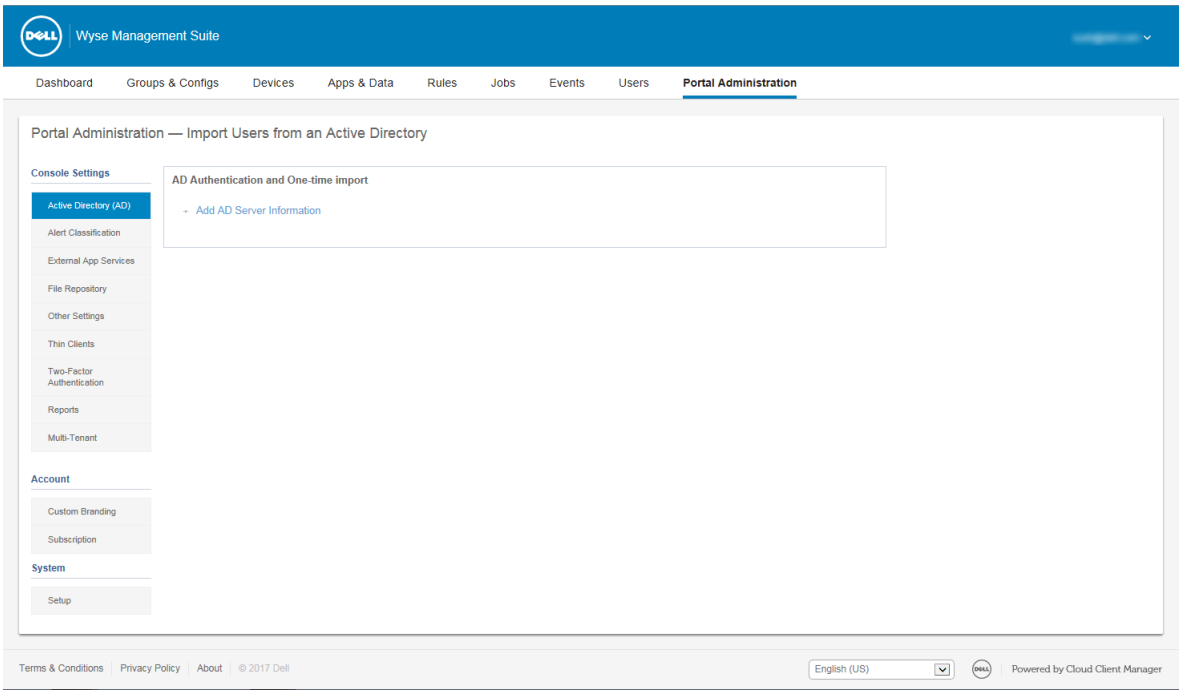


그림 16 . 포털 관리

주제:

- Active Directory를 통해 할당되지 않은 사용자 또는 사용자 그룹을 퍼블릭 클라우드로 가져오기
- Active Directory 서버 정보 추가
- 경고 분류
- API(Application Programming Interface) 계정 생성
- Wyse Management Suite 파일 리포지토리 액세스
- 기타 설정 구성
- Teradici 구성 관리
- 2단계 인증 활성화
- 다중 테넌트 계정 활성화
- 보고서 생성
- 맞춤형 브랜딩 활성화
- 시스템 설정 관리
- 보안 MQTT 구성
- SSL을 통한 보안 LDAP 활성화

Active Directory를 통해 할당되지 않은 사용자 또는 사용자 그룹을 퍼블릭 클라우드로 가져오기

단계

1. 파일 리포지토리를 다운로드하고 설치합니다. 파일 리포지토리 액세스를 참조하십시오. 리포지토리는 회사 네트워크를 사용하여 설치해야 하며 사용자를 끌어오려면 AD 서버에 액세스할 수 있어야 합니다.
2. 퍼블릭 클라우드에 리포지토리를 등록합니다. 등록 후에는 UI에 나와 있는 단계를 따라 Wyse Management Suite 퍼블릭 클라우드로 사용자를 가져옵니다. Wyse Management Suite 퍼블릭 클라우드로 가져온 후에는 AD 사용자의 역할을 편집할 수 있습니다.
3. 퍼블릭 클라우드에서 ADFS를 설정합니다.

Active Directory 서버 정보 추가

Active Directory 사용자 및 사용자 그룹을 Wyse Management Suite 프라이빗 클라우드로 가져올 수 있습니다.

단계

1. Wyse Management Suite 프라이빗 클라우드에 로그인합니다.
2. **포털 관리** > **콘솔 설정** > **AD(Active Directory)**로 이동합니다.
3. **AD 서버 정보 추가** 링크를 클릭합니다.
4. **AD 서버 이름**, **도메인 이름**, **서버 URL** 및 **포트**와 같은 서버 세부 정보를 입력합니다.
   LDAP 포트 389를 사용하여 연결하는 경우 보안 LDAP를 활성화하도록 경고 메시지가 표시됩니다. SSL을 통한 보안 LDAP를 구성하고 활성화하려면 SSL을 통한 보안 LDAP 활성화를 참조하십시오.
5. **저장**을 클릭합니다.
6. **가져오기**를 클릭합니다.
7. 사용자 이름과 암호를 입력합니다.

   노트: 그룹 및 사용자를 검색하려면 **검색 기반**을 기반으로 그룹을 필터링하고 **그룹 이름 포함** 옵션을 이용할 수 있습니다. 다음과 같이 값을 입력할 수 있습니다.

   - `OU=<OU Name>`.

     예: `OU=TestOU`.

   - `DC=<Child Domain>, DC=<Parent Domain>, DC=com,`.

     예: `DC=Skynet, DC=Alpha, DC=Com`.

   쉼표 뒤에 공백을 입력할 수 있지만 작은따옴표 또는 큰따옴표를 사용할 수 없습니다.

8. **로그인**을 클릭합니다.
9. **사용자 그룹** 페이지에서 **그룹 이름**을 클릭하고 그룹 이름을 입력합니다.
10. **검색** 필드에 선택할 그룹 이름을 입력합니다.
11. 그룹을 선택합니다.
    선택한 그룹이 오른쪽 창으로 이동합니다.
12. **사용자 이름 콘텐츠 필드**에서 사용자 이름을 입력합니다.
13. **사용자 가져오기** 또는 **그룹 가져오기**를 클릭합니다.
    이러한 항목은 다음 시나리오에서 사용자 가져오기 프로세스 중에 생략되며 Wyse Management Suite로 가져올 수 없습니다.
    - 유효하지 않은 이름을 제공한 경우
    - 성을 제공하지 않은 경우
    - 이메일 주소를 이름으로 제공하는 경우

    Wyse Management Suite 포털에는 가져온 Active Directory 사용자 수와 함께 확인 메시지가 표시됩니다. 가져온 Active Directory 사용자가**할당되지 않은 관리자** > **사용자 탭**에 나열됩니다. 그룹을 가져오는 위치에도 확인 메시지가 표시됩니다.
14. 다른 역할 또는 권한을 할당하려면 사용자를 선택하고 **사용자 편집**을 클릭합니다.

    Active Directory 사용자에게 역할을 지정하면 해당 역할이 **사용자** 페이지의 **관리자** 탭으로 이동합니다.

노트: 구성 중에 **AD 인증 및 한 번 가져오기** 페이지를 닫으려면 **AD 로그아웃** 옵션을 클릭합니다.

노트: 그룹을 가져온 후 도메인 사용자로 로그인하려면 관리자는 사용자 탭 아래의 할당되지 않은 사용자 탭을 사용하여 그룹 사용자를 가져와야 합니다. 관리자가 그룹만 가져와 그룹에만 역할을 할당하는 경우 그룹 사용자를 가져오지 않고서 도메인 사용자로 로그인할 수 없습니다.

다음 단계

Active Directory 사용자는 도메인 자격 증명을 사용하여 Wyse Management Suite 관리 포털에 로그인할 수 있습니다. Wyse Management Suite 포털에 로그인하려면 다음을 수행합니다.

1. Wyse Management Suite 관리 포털을 시작합니다.
2. 로그인 화면에서 **도메인 자격 증명으로 로그인** 링크를 클릭합니다.
3. 도메인 사용자 자격 증명을 입력하고 **로그인**을 클릭합니다.

하위 도메인 자격 증명을 사용하여 Wyse Management Suite 포털에 로그인하려면 다음을 수행합니다.

1. Wyse Management Suite 관리 포털을 시작합니다.
2. 로그인 화면에서 **도메인 자격 증명으로 로그인** 링크를 클릭합니다.
3. **사용자 도메인 변경**을 클릭합니다.
4. 사용자 자격 증명 및 완전한 도메인 이름을 입력합니다.
5. **로그인**을 클릭합니다.

가져온 Active Directory 사용자는 전역 관리자 로그인을 사용하여 **사용자** 페이지에서 활성화하거나 비활성화할 수 있습니다. 계정이 비활성화된 경우 Wyse Management Suite 관리 포털에 로그인할 수 없습니다.

노트: SSL을 통한 보안 LDAP를 구성하고 활성화하려면 SSL을 통한 보안 LDAP 활성화를 참조하십시오.

퍼블릭 클라우드에서 Active Directory 페더레이션 서비스 기능 구성

퍼블릭 클라우드에서 ADFS(Active Directory Federation Services)를 구성할 수 있습니다.

단계

1. **포털 관리자** 페이지의 **콘솔 설정**에서 **AD(Active Directory)**를 클릭합니다.
2. ADFS에 Wyse Management Suite 세부 정보를 입력합니다. Wyse Management Suite .xml 파일을 업로드해야 하는 ADFS 서버의 위치 세부 정보를 확인하려면 **정보 (i)** 아이콘 위로 마우스를 이동합니다.

   노트: Wyse Management Suite .xml 파일을 다운로드하려면 다운로드 링크를 클릭합니다.

3. ADFS에서 Wyse Management Suite 규칙을 설정합니다. 맞춤형 클레임 규칙 세부 정보를 확인하려면 **정보 (i)** 아이콘 위로 마우스를 이동합니다.

   노트: Wyse 관리 규칙을 보려면 **WMS 규칙 보기** 링크를 클릭합니다. **Wyse Management Suite 규칙** 창에서 제공된 링크를 클릭하여 Wyse Management Suite 규칙을 다운로드할 수도 있습니다.

4. ADFS 세부 정보를 구성하려면 **구성 추가**를 클릭하고 다음을 수행합니다.

   노트: 테넌트가 ADFS 구성을 따르도록 허용하려면 ADFS 메타데이터 파일을 업로드합니다.

   a. 씬 클라이언트에 저장된 .XML 파일을 업로드하려면 **XML 파일 업로드**를 클릭합니다.
   파일은 `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`에서 확인할 수 있습니다.
   b. 해당 상자에 엔터티 ID 및 X.509 서명 인증서의 세부 정보를 입력합니다.
   c. ADFS 로그인 URL 주소와 ADFS 로그아웃 URL 주소를 해당 상자에 입력합니다.
   d. 테넌트가 ADFS를 사용하여 SSO(Single Sign-On)를 구성할 수 있도록 하려면 **ADFS를 사용하여 SSO 활성화** 확인란을 선택합니다. 이 기능은 SAML(Security Assertion and Markup Language) 표준 사양을 따릅니다.
   e. 구성 정보의 유효성을 검사하려면 **ADFS 로그인 테스트**를 클릭합니다. 이를 통해 테넌트는 저장하기 전에 설정을 테스트할 수 있습니다.

   노트: 테넌트는 ADFS를 사용하여 SSO 로그인을 활성화/비활성화할 수 있습니다.

5. **저장**을 클릭합니다.
6. 메타데이터 파일을 저장한 후 **구성 업데이트**를 클릭합니다.

   노트: 테넌트는 ADFS에서 구성된 AD 자격 증명을 사용하여 로그인 및 로그아웃할 수 있습니다. AD 사용자를 Wyse Management Suite 서버로 가져왔는지 확인해야 합니다. 로그인 페이지에서 **로그인**을 클릭하고 도메인 자격 증명을 입력합니다. AD 사용자의 이메일 주소를 입력하고 로그인해야 합니다. 사용자를 퍼블릭 클라우드로 가져오려면 원격 리포지토리가 설치되어 있어야 합니다. ADFS 문서에 대한 자세한 내용은 Technet.microsoft.com을 참조하십시오.

결과

ADFS 테스트 연결에 성공하면 원격 리포지토리에 있는 AD 커넥터를 사용하여 사용자를 가져옵니다.

경고 분류

경고 페이지에는 경고가 **위험**, **경고** 또는 **정보**로 분류되어 표시됩니다.

노트: 이메일을 통해 경고를 수신하려면 오른쪽 상단 모서리에 표시된 사용자 이름 메뉴에서 경고 **경고 기본 설정** 옵션을 선택합니다.

위험, **경고** 또는 **정보**와 같은 알림 유형 중에서, 다음 경고에 대해 원하는 것을 선택합니다.

- 디바이스 상태 경고
- 디바이스가 체크인되지 않음

API(Application Programming Interface) 계정 생성

이 작업 정보

이 섹션에서는 보안 API(Application Programming Interface) 계정을 생성할 수 있습니다. 이 서비스는 특별 계정을 생성할 수 있는 기능을 제공합니다. 외부 애플리케이션 서비스를 구성하려면 다음을 수행합니다.

단계

1. Wyse Management Suite 포털에 로그인하고 **포털 관리** 탭을 클릭합니다.
2. **콘솔 설정**에서 **외부 앱 서비스**를 선택합니다.
3. **추가** 탭을 선택하여 API 서비스를 추가합니다.
   외부 앱 서비스 추가 대화 상자가 표시됩니다.
4. 외부 애플리케이션 서비스를 추가하려면 다음 세부 정보를 입력합니다.
   - 이름
   - 설명
5. **자동 승인** 확인란을 선택합니다.
   확인란을 선택하면 전역 관리자의 승인이 필요하지 않습니다.
6. **저장**을 클릭합니다.

Wyse Management Suite 파일 리포지토리 액세스

파일 리포지토리는 **파일**이 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.

이미지 가져오기 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. **체크인**을 클릭한 다음 **명령 전송**을 클릭하여 디바이스 정보 명령을 디바이스로 전송합니다.
7. **등록 취소** 옵션을 클릭하여 온프레미스 서비스를 등록 취소합니다.
8. **편집**을 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.

    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 못함**이라는 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 저장**을 클릭합니다.

서브넷 매핑

Wyse Management Suite 2.0에서 파일 리포지토리에 서브넷을 할당할 수 있습니다. 파일 리포지토리를 최대 25개의 서브넷 또는 범위에 연결할 수 있습니다. 또한 리포지토리에 연결된 서브넷의 우선 순위를 지정할 수 있습니다.

Wyse Management Suite 2.1에서 서브넷 매핑을 사용하여 BIOS 패키지를 배포할 수 있습니다. 원격 리포지토리, 테넌트 클라우드 리포지토리 또는 운영자 클라우드 리포지토리에서 여러 펌웨어 패키지를 업로드하고 배포할 수 있습니다. 이 기능은 Wyse Management Suite Pro 라이선스에서만 사용할 수 있습니다.

서브넷 매핑 구성

단계

1. **포털 관리** > **파일 리포지토리**로 이동합니다.

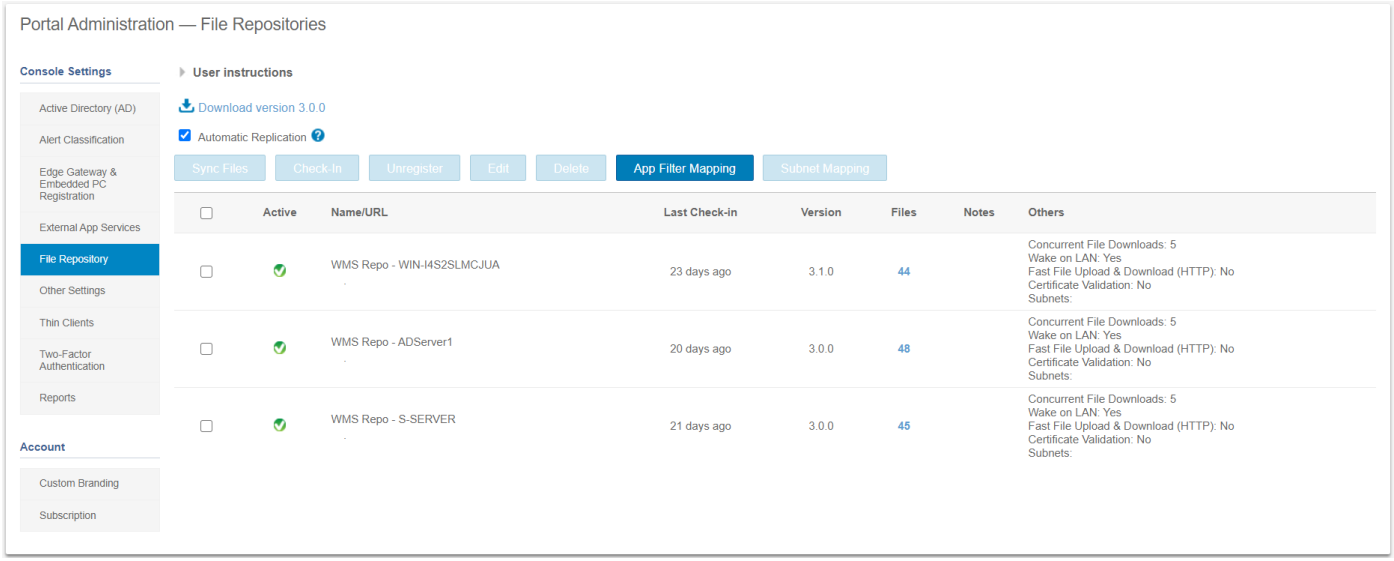


그림 17 . 파일 리포지토리

2. 파일 리포지토리를 선택합니다.
3. **서브넷 매핑** 옵션을 클릭합니다.
4. 서브넷 또는 범위를 한 줄에 하나의 값을 입력합니다. 범위 구분에는 하이픈을 사용해야 합니다.
5. 구성된 서브넷이나 범위를 통해서만 파일 리포지토리에 액세스하려는 경우 필요에 따라 **이 파일 리포지토리에 매핑되지 않은 서브넷의 디바이스에서 서브넷 근접성을 사용하는 폴백 메서드로 이 파일 리포지토리에서 파일을 다운로드하도록 허용** 확인란을 선택 취소합니다.

   노트: 이 파일 리포지토리에 매핑되지 않은 서브넷의 디바이스에서 서브넷 근접성을 사용하는 폴백 메서드로 이 파일 리포지토리에서 파일을 다운로드하도록 허용 옵션은 기본적으로 선택되어 있습니다.

기타 설정 구성

다음 설정을 사용하여 **APNS 경고**, **라이선스 만료 경고** 및 기타 **셀프 서비스 법적 계약**을 적용할 수 있습니다.

- **대시보드 페이지의 라이선스 만료 경고 해제** - 이 확인란을 선택하면 라이선스 만료 경고가 **대시보드** 페이지에 표시되지 않습니다.
- **라이선스 만료 이메일 알림 활성화** - 라이선스 만료 이메일 알림을 활성화하려면 이 확인란을 선택합니다. 라이선스가 만료되기 전에 테넌트에 이메일 알림이 발송됩니다. 이 옵션은 기본적으로 사용됩니다. 라이선스가 다음 기간 후에 만료될 시 이메일 알림이 발송됩니다.
  - 60일
  - 30일
  - 14일
- **Android 설정 정책 구성 페이지에서 고급 Dell Wyse 클라우드 연결 옵션을 활성화합니다(참고: Professional 계층만 해당)** - Android 설정 정책 구성 페이지에서 고급 Dell Wyse 클라우드 연결 옵션을 활성화하려면 이 옵션을 선택합니다.
- **하트비트 간격**- 시간을 입력합니다. 디바이스가 하트비트 신호를 60분~360분 간격으로 전송합니다. 프라이빗 클라우드의 최소 간격은 5분입니다.
- **체크인 간격** - 시간을 입력합니다. 디바이스가 8시간에서 24시간 간격으로 전체 확인 신호를 전송합니다.
- **준수 알림이 체크인되지 않음** - 디바이스가 **규정 준수 미체크인 알림**을 트리거하기 전 일 수를 입력합니다. 1-99 범위 내에 있어야 합니다.
- **WMS 콘솔 시간 초과** - 사용자가 콘솔에서 로그아웃된 후 유휴 시간을 분 단위로 입력합니다. 이 설정은 전역 관리자가 구성할 수 있습니다. 기본값은 30분입니다.
- **등록 유효성 검사** - **등록 유효성 검사 옵션**이 활성화되면 자동 검색된 디바이스가 **디바이스** 페이지에서 **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.
- **EULA 동의 재설정** - **EULA 동의** 페이지를 재설정하여 ThinOS 9.x에 대한 EULA Embedded 펌웨어/패키지 업로드 중에 마법사를 다시 표시하려면 이 확인란을 선택합니다.
- **WMS API**- Wyse Management Suite API를 활성화하려면 이 확인란을 선택합니다.

Wyse Management Suite API 활성화

Wyse Management Suite 서버는 전용 API를 사용하여 사용자 인터페이스 구성 요소에서 생성된 요청을 지원합니다. Java 스크립트로 생성된 사용자 인터페이스는 필요한 데이터를 JSON 형식으로 가져오기 위해 API 호출과 같은 REST를 사용합니다. JSON 형식은 요청에 따라 다릅니다. 디바이스 세부 정보를 검색하거나 Wyse Management Suite 서버에서 작업을 수행하고 현재 서비스와 같은 맞춤 구성 클라이언트와 서버를 통합할 수 있습니다.

전제조건

Wyse Management Suite API를 사용하려면 Pro 라이선스 유형이 필요합니다.

단계

1. 관리자로 로그인합니다.
2. **포털 관리** > **기타 설정**으로 이동합니다.
3. **WMS API 활성화** 확인란을 선택합니다.
4. **설정 저장**을 클릭합니다.
   지원되는 API 및 관련 문서에 대한 자세한 내용은 https://api-marketplace.dell.com에서 Wyse Management Suite API를 참조하십시오.

Teradici 구성 관리

Teradici 서버를 추가하려면 다음을 수행합니다.

단계

1. **포털 관리** 탭의 **콘솔 설정**에서 **Teradici**를 클릭합니다.
2. **서버 추가**를 클릭합니다.
   서버 추가 화면이 표시됩니다.
3. **서버 이름**을 입력합니다. 포트 번호가 자동으로 채워집니다.
4. CA 유효성 검사를 활성화하려면 **CA 유효성 검사** 확인란을 선택합니다.
5. **테스트**를 클릭합니다.

2단계 인증 활성화

시스템에 활성화된 전역 관리자 사용자가 2명 이상 있어야 합니다.

전제조건

작업을 진행하기 전에 둘 이상의 전역 관리자를 생성합니다.

이 작업 정보

1. Wyse Management Suite 포털에 로그인하고 **포털 관리자** 탭을 클릭합니다.
2. **콘솔 설정**에서 **2단계 인증**을 클릭합니다.
3. 2단계 인증을 활성화하려면 확인란을 선택해야 합니다.
   노트: 관리자는 관리 포털에 로그인할 때 OTP(One-Time Passcode)를 사용하여 두 번째 인증 계수를 확인해야 합니다.
4. 이메일 주소로 OTP를 받게 됩니다. 일회용 암호를 입력합니다.

기본적으로 OTP 확인은 8회 시도할 수 있습니다. 암호 확인에 실패하면 계정이 잠깁니다. 잠긴 계정은 전역 관리자만 잠금 해제할 수 있습니다.

다중 테넌트 계정 활성화

이 섹션에서는 서로 독립적으로 관리할 수 있는 테넌트 계정을 생성할 수 있습니다. 조직을 독립적으로 관리할 수 있습니다. 각 계정에는 고유한 라이선스 키가 있어야 하며, 고유한 관리자 계정, 정책, 운영 체제 이미지, 애플리케이션, 규칙, 경고 등을 설정할 수 있습니다. 이러한 조직은 상급 운영자가 생성합니다.

다중 테넌트 계정을 활성화하려면 다음을 수행합니다.

1. Wyse Management Suite 포털에 로그인하고 **포털 관리자** 탭을 클릭합니다.
2. **콘솔 설정** 아래의 **멀티-테넌트**를 선택합니다.
3. 확인란을 선택하여 다중 테넌트 옵션을 활성화합니다.
4. 다음 세부 사항을 입력합니다.
   - 사용자 이름
   - 암호
   - 암호 확인
   - 이메일
5. **설정 저장**을 클릭합니다.

보고서 생성

작업, 디바이스, 그룹, 이벤트, 경고 및 정책에 대한 보고서를 다운로드할 수 있습니다. 최종 지점의 문제를 해결하려는 경우 관리자와 보고서를 공유할 수 있습니다.

단계

1. **포털 관리** > **보고서**로 이동합니다.
2. **보고서 생성** 옵션을 클릭합니다.
   보고서 생성 창이 표시됩니다.
3. **유형** 드롭다운 목록에서 보고서 유형을 선택합니다.
4. **그룹** 드롭다운 목록에서 그룹을 선택합니다.
5. 구분 기호를 선택합니다.
6. **저장**을 클릭합니다.

맞춤형 브랜딩 활성화

이 작업 정보

이 옵션을 사용하면 회사 이름과 로고 또는 브랜드를 추가할 수 있습니다. 자체 헤더 로고, 파비콘을 업로드하고, 헤더 제목을 추가하고, 헤더 색상을 변경하여 Wyse Management Suite 포털을 사용자 정의할 수 있습니다. 맞춤형 브랜딩을 액세스하고 지정하려면 다음을 수행합니다.

단계

1. **포털 관리자** > **계정** > **맞춤형 브랜딩**으로 이동합니다.
2. **맞춤형 브랜딩 활성화**를 클릭합니다.
3. **헤더 로고**에서 **찾아보기**를 클릭하고 폴더 위치에서 헤더 로고 이미지를 선택합니다.
   헤더 로고의 최대 크기는 500*50 픽셀이어야 합니다.
4. **제목** 옵션에 제목을 입력합니다.
5. 브라우저에서 제목을 보려면 **window/tab 브라우저에서 제목 표시** 확인란을 선택합니다.
6. **헤더 배경색** 및 **헤더 텍스트 색**에 대한 색상 코드를 입력합니다.
7. **찾아보기**를 클릭하고 **파비콘**을 선택합니다.
   브라우저 주소 표시줄의 웹 사이트 URL 옆에 파비콘이 나타납니다.
   노트: 이미지를 **.ico** 파일로 저장해야 합니다.
8. **설정 저장**을 클릭합니다.

시스템 설정 관리

설치 중에 구성된 SMTP 세부 정보, 인증서, MQTT 세부 정보 및 외부 Wyse Management Suite URL 세부 정보를 변경할 수 있습니다.

Wyse Management Suite 2.1에서는 서버 측의 변경 없이 최신 구성 설정을 업데이트할 수 있는 ThinOS 9.x 디바이스에 대한 **동적 스키마 구성**이 지원됩니다. 퍼블릭 클라우드에서 Wyse Management Suite 운영자는 9.x 구성 사용자 인터페이스를 업그레이드할 수 있습니다. 프라이빗 클라우드의 경우(Pro 기능만 해당) 전역 사용자는 9.x 구성 사용자 인터페이스를 업그레이드할 수 있습니다. **다중 테넌트** 기능이 활성화되어 있는 경우 Wyse Management Suite 운영자가 **관리** 섹션에서 최신 스키마를 업로드할 수 있습니다.

단계

1. Wyse Management Suite 포털에 로그인하고 **포털 관리자** 탭을 클릭합니다.
2. **시스템**에서 **설정**을 클릭합니다.
3. 모든 디바이스-서버 통신에 대해 서버 인증서 유효성 검사를 수행하려면 이 확인란을 선택합니다.
4. **이메일 경고를 위한 SMTP 업데이트** 영역에 다음 세부 정보를 입력합니다.
   - SMTP 서버
   - 주소에서 전송
   - 사용자 이름
   - 암호
   - 테스트 주소

   현재 인증서 - 프라이빗 클라우드에 대한 CA 유효성 검사를 활성화하려면 **인증서 유효성 검사** 확인란을 선택합니다. 파일 다운로드, 로컬 리포지토리에서 운영 체제 이미지 다운로드를 포함하여 서버 및 클라이언트의 모든 통신에서 인증서를 사용합니다.

   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 못함**이라는 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.
5. 다음 옵션을 선택하고 세부 정보를 입력합니다.
   - **키/인증서** - HTTPS 키/인증서 파일 쌍을 업로드합니다(PEM 형식만 지원됨).
   - **PKCS-12** - HTTPS PKCS-12(.pfx, .p12)를 업로드합니다. IIS pfx에는 Apache 중간급 인증서가 필요합니다.
6. 외부 MQTT 세부 정보를 업데이트하려면 **외부 MQTT 변경** 옵션을 클릭하고 세부 정보를 구성합니다.
7. 외부 Wyse Management Suite URL을 업데이트하려면 **외부 WMS URL 변경** 옵션을 클릭하고 세부 정보를 구성합니다.

   노트: 이전 구성으로 되돌리려면 **마지막 URL로 되돌리기** 옵션을 클릭하고 **저장**을 클릭합니다.
8. 9.x 구성 사용자 인터페이스를 업그레이드하려면 **구성 UI 패키지** 필드에서 **파일 선택**을 클릭하고 .zip 파일로 이동합니다.

   노트: **다중 테넌트** 기능이 활성화되어 있는 경우 이 옵션을 사용할 수 없습니다.
9. **저장**을 클릭합니다.

보안 MQTT 구성

Wyse Management Suite 3.2에서 Windows 10 IoT Enterprise, Dell Hybrid Client, ThinOS 9.1 MR1, 원격 리포지토리에 대한 보안 MQTT 연결을 구성할 수 있습니다.

단계

1. **포털 관리** > **시스템** > **설정**으로 이동합니다.
2. 보안 MQTT를 구성하려면 **WMS URL** 필드의 **기본 MQTT** 드롭다운 목록에서 **외부 보안 MQTT**를 선택합니다.

중요 정보

이전 에이전트가 있는 디바이스는 비보안 포트와 계속 통신하며 Windows Embedded 디바이스 및 Dell Hybrid Client 지원 디바이스와 같이 새 에이전트가 있는 디바이스는 보안 포트와 통신할 수 있습니다.

기본 MQTT에 대한 기본 선택은 외부 MQTT(`tcp://<WMS URL>:1883`)입니다.

퍼블릭 클라우드의 경우 기본 MQTT에 대한 기본 선택은 외부 MQTT(`tcp://<WMS URL>:443`)입니다.

Wyse Management Suite 공용 서버에 등록된 모든 디바이스가 외부 MQTT에 연결됩니다. 원격 포트 1883이 차단된 경우 에이전트는 보안 MQTT 서버에 다시 연결합니다.

외부 MQTT와 외부 보안 MQTT 간에 선택된 기본 MQTT는 Wyse Management Suite 온프레미스 서버에서만 사용할 수 있습니다. 요구 사항에 따라 기본 MQTT를 외부 보안 MQTT(`tls://<WMS URL>:8443`)로 업데이트할 수 있습니다.

보안 MQTT를 지원하는 최신 에이전트가 있는 모든 디바이스는 외부 보안 MQTT에 연결됩니다. 보안 MQTT를 지원하지 않는 이전 에이전트는 계속해서 외부 MQTT(`tcp://<WMS URL>:1883`)를 사용합니다.

SSL을 통한 보안 LDAP 활성화

단계

1. 요구 사항에 따라 SSL 인증서를 다운로드, 내보내기 또는 생성합니다.

   노트: SSL 인증서를 생성하는 자세한 방법은 https://docs.microsoft.com/의 *타사 인증 기관으로 SSL을 통한 LDAP 활성화*를 참조하십시오.

2. Wyse Management Suite로 로그인합니다.
3. **포털 관리** > **설정** > **신뢰 저장소 인증서**로 이동하여 인증서를 가져옵니다.

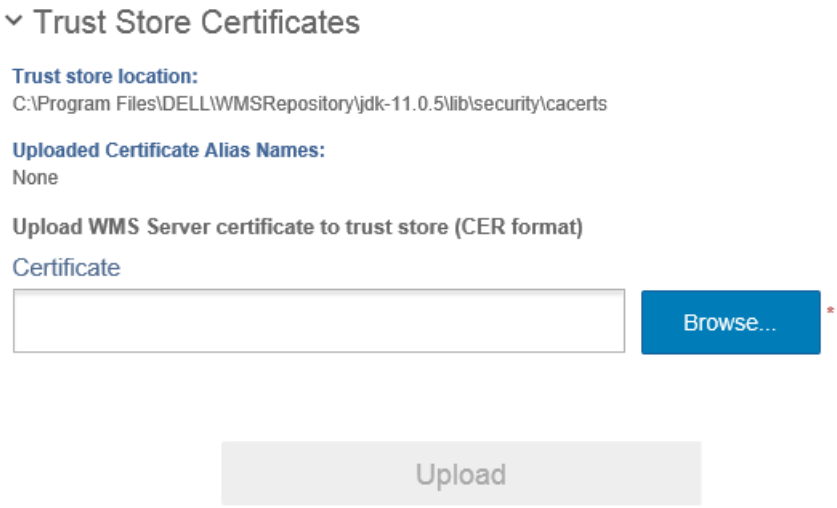


그림 18 . 신뢰 저장소 인증서

4. LDAP 인증서가 업로드되면 **저장** 또는 **저장 및 재시작**을 클릭할 수 있습니다.

   노트: **취소**를 클릭하여 업로드 프로세스를 중지할 수도 있습니다.

5. 씬 클라이언트에서 **시작** > **서비스**로 이동하여 **Dell WMS: Tomcat Service**를 재시작합니다.
6. Wyse Management Suite에 다시 로그인합니다.
7. **포털 관리** > **Actve Directory** > **AD 인증 및 한 번 가져오기**로 이동합니다.
8. **서버 URL** 필드에 LDAPS 주소를 입력합니다.
9. **포트** 필드에 구성된 보안 포트를 입력합니다. 예: 636 또는 3269
10. **저장**을 클릭합니다.
11. AD 자격 증명을 입력하고 Active Directory에 연결합니다.

    노트: 온프레미스 설치 후 OOBE 화면에서 인증서를 업데이트하여 서버 인증서를 가져오고 보안 LDAP를 구성할 수 있습니다.

다음 단계

- 단일 테넌트로 온프레미스 설치를 마친 후 **포털 관리** > **설정**으로 이동하여 인증서의 공개 키를 신뢰 저장소로 가져옵니다. 다중 테넌트 설정의 경우 **WMS 운영자 관리** > **시스템 설정** > **LDAPS**로 이동합니다. 공개 키를 가져온 후 **저장 및 재시작**을 클릭하면 Tomcat 서비스가 재시작됩니다.
- OOBE 화면에서 인증서를 가져온 후 **지금 재시작**을 클릭하면 Tomcat이 자동으로 재시작됩니다.

15

Dell Wyse 5070 디바이스 및 Dell Ubuntu Generic Client를 Dell Hybrid Client로 변환

Wyse Management Suite Pro 3.1 이상 버전을 사용하여 Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x 및 ThinOS 8.6을 실행하는 Dell Wyse 5070 디바이스를 Dell Hybrid Client로 변환할 수 있습니다. 또한 Wyse Management Suite Pro 3.1 이상 버전을 사용하여 Ubuntu 18.04 및 Windows 10을 실행하는 Dell OptiPlex 7070 Ultra 시스템을 Dell Hybrid Client로 변환할 수 있습니다.

주제:

- Dell Wyse 5070 변환
- Dell Generic Client를 Dell Hybrid Client로 변환

Dell Wyse 5070 변환

전제조건

- Windows 10 또는 ThinLinux 2.x(을)를 실행하는 Wyse 5070 디바이스에 4.0.8 이상의 최신 부트 에이전트가 없는 경우 Dell 지원 사이트에서 다운로드합니다.
- ThinOS 8.6_511을 실행하는 Wyse 5070 디바이스에 4.0.8 이상의 최신 부트 에이전트가 없는 경우 Dell 지원 사이트에서 다운로드합니다.
- Windows 10 IoT Enterprise 디바이스를 변환하는 경우 Dell 지원 사이트에서 Dell Hybrid Client 이미지 DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_32GB.exe를 다운로드합니다.
- ThinLinux 2.x 또는 ThinOS 8.6 디바이스를 변환하는 경우 Dell 지원 사이트에서 Dell Hybrid Client 이미지 DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_16GB.exe를 다운로드합니다.
- Wyse Management Suite Pro 3.1 이상 버전을 사용하는지 확인합니다.
- Hybrid Client 라이선스 수가 Dell Hybrid Client로 변환해야 하는 디바이스 수보다 크거나 같은지 확인합니다. Dell Hybrid Client 라이선스를 Wyse Management Suite로 가져올 수 있습니다.
- Wyse Management Suite가 퍼블릭 클라우드에 설정되어 있고 변환 이미지를 퍼블릭 클라우드에 등록하려는 경우 온프레미스 리포지토리를 로컬로 설정하고 구성해야 합니다. 자세한 내용은 원격 리포지토리를 참조하십시오.

이 작업 정보

Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x 및 ThinOS 8.6을 Dell Hybrid Client로 변환하는 프로세스는 기존 드라이브의 내용과 파티션 구조를 제거합니다. 변환 프로세스는 Wyse Management Suite에 디바이스를 등록하는 데 관련된 인증서 및 설정만 보존합니다. 다른 모든 데이터, 인증서 및 구성 설정은 보존되지 않습니다. Dell Hybrid Client로 변환한 후에는 디바이스를 원래 상태로 다시 변환할 수 없습니다. 그러나 Dell 지원 사이트에서 Dell Wyse USB Imaging Tool을 사용하여 원래 운영 체제를 복원할 수 있습니다. 기존 데이터 및 설정은 복원되지 않습니다.

단계

1. Wyse Management Suite에 Dell Hybrid Client 이미지를 등록합니다. 등록 방법에 대한 자세한 내용은 리포지토리에 Hybrid Client 이미지 추가를 참조하십시오.
   - 디바이스의 스토리지 크기가 16GB 이상인 경우 DHC_CONVERSION_5070.exe를 사용합니다.
   - 디바이스의 스토리지 크기가 16GB인 경우 DHC_CONVERSION_5070_16GB.exe를 사용합니다.
2. Dell Hybrid Client 이미지 정책을 생성합니다. Hybrid Client 이미지 정책을 생성하는 방법에 대한 자세한 내용은 Hybrid Client 이미지 정책 생성을 참조하십시오.
3. 디바이스를 Dell Hybrid Client로 변환합니다. 이미지 예약 방법에 대한 자세한 내용은 이미지 예약 정책을 참조하십시오.
   - 디바이스에서 이미지 업데이트 알림을 수신합니다. 부트 에이전트가 Wyse Management Suite 리포지토리에서 이미지를 다운로드하고 내부적으로 Dell Recovery Tool을 트리거하여 Dell Hybrid Client 이미지를 설치합니다. 이미징이 완료되면 디바이스가 Dell Hybrid Client로 부팅됩니다.
   - Dell Client Agent가 디바이스를 Wyse Management Suite에 Dell Hybrid Client로 등록합니다.
   - Wyse Management Suite는 디바이스를 Dell Hybrid Client 디바이스로 관리합니다.

리포지토리에 Dell Hybrid Client 이미지 추가

단계

1. Wyse Management Suite를 사용하여 Dell Hybrid Client 변환 이미지를 리포지토리 위치 또는 운영 체제 이미지 폴더에 복사합니다.

   노트: Dell Technologies는 이미지 파일을 로컬 시스템에 복사한 다음 Wyse Management Suite 리포지토리 위치에 복사할 것을 권장합니다. Wyse Management Suite는 압축된 폴더에서 파일을 추출하고 리포지토리 위치 또는 운영 체제 이미지 폴더로 파일을 업로드합니다.

   이미지가 리포지토리에 추가됩니다.
2. 저장된 이미지를 보려면 **앱 및 데이터** > **OS 이미지 리포지토리** > **하이브리드 클라이언트**로 이동합니다.

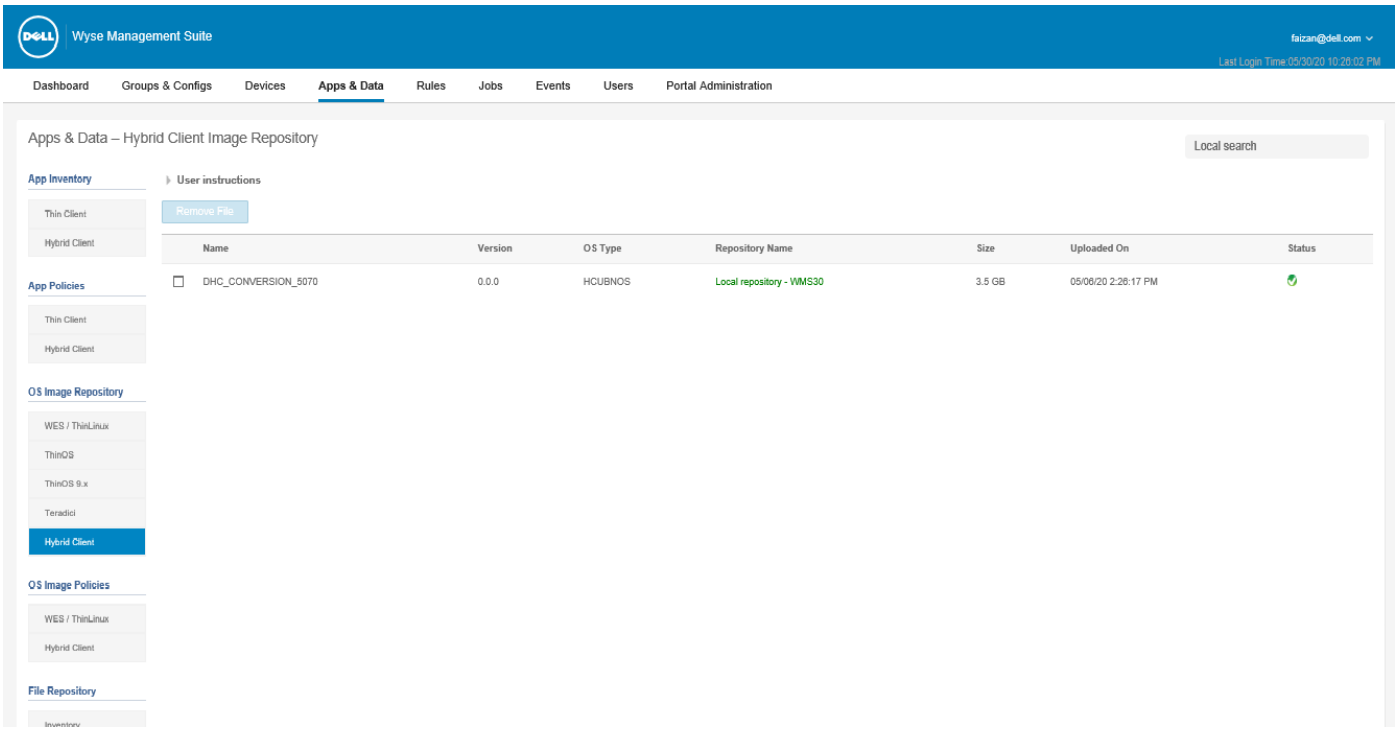


그림 19 . 리포지토리에 Dell Hybrid Client 이미지 추가

하이브리드 클라이언트 이미지 정책 생성

단계

1. **앱 및 데이터**로 이동하여 **OS 이미지 정책**에서 **하이브리드 클라이언트**를 클릭합니다.
2. **정책 추가**를 클릭하고 **하이브리드 클라이언트 정책 편집** 탭으로 이동합니다.
3. **정책 이름**을 입력하고 **그룹** 탭의 드롭다운 메뉴에서 그룹을 선택합니다.
4. **OS 유형** 탭의 드롭다운 메뉴에서 운영 체제 유형을 선택합니다.
5. **OS 하위 유형 필터** 탭의 드롭다운 메뉴에서 운영 체제 하위 유형 필터를 선택합니다.

   노트: 이미지를 특정 운영 체제 또는 플랫폼에 배포하려면 **OS 하위 유형 필터** 또는 **플랫폼 필터**를 선택합니다.
6. **OS 이미지** 탭의 드롭다운 메뉴에서 이미지 파일을 선택합니다.
7. **규칙** 탭의 드롭다운 목록에서 **이 버전 강제 적용**을 클릭합니다.
8. **자동으로 정책 적용** 탭의 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - **자동으로 정책을 적용하지 않음** – 이미지 정책이 Wyse Management Suite에 등록된 디바이스에 자동으로 적용되지 않습니다.
   - **새 디바이스에 정책 적용** – 이미지 정책이 Wyse Management Suite에 등록된 새 디바이스에 적용됩니다.
9. **저장**을 클릭합니다.

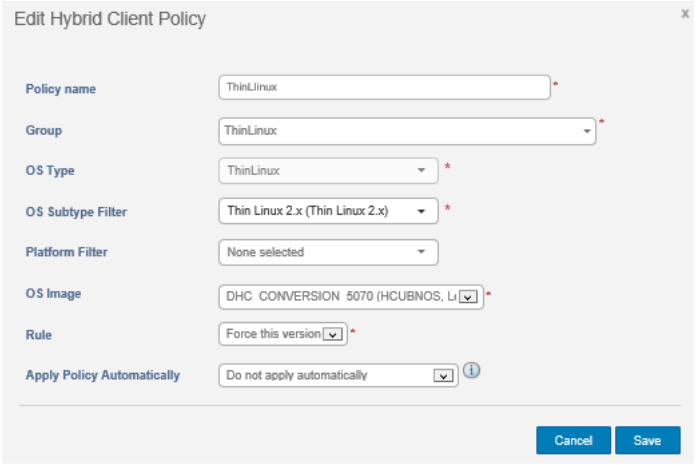


그림 20 . 하이브리드 클라이언트 이미지 정책 생성

이미지 정책 예약

단계

1. **작업**으로 이동하여 **이미지 정책 예약** 탭을 클릭합니다.
   이미지 업데이트 작업 탭이 표시됩니다.
2. **정책** 탭의 드롭다운 메뉴에서 정책을 선택합니다.
3. **설명** 탭에 작업 설명을 입력합니다.
4. 다음과 같이 **실행** 탭의 드롭다운 목록에서 날짜 또는 시간을 선택합니다.
   - **유효** – 시작 날짜와 종료 날짜 입력
   - **시작 및 종료 시간** - 시작 시간과 종료 시간 입력
   - **요일** - 요일 선택
5. 예약된 작업의 세부 정보를 보려면 **미리 보기**를 클릭합니다.
6. 작업을 시작하려면 **예약**을 클릭합니다.

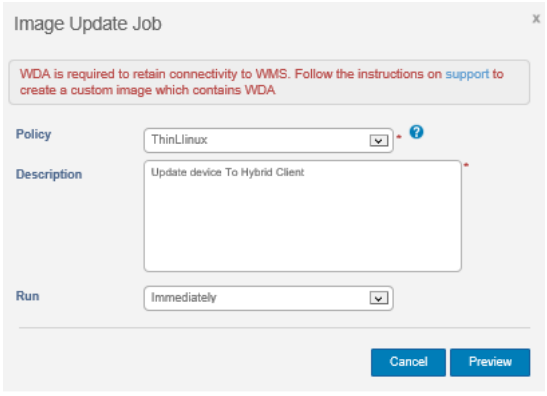


그림 21 . 작업 예약

Dell Generic Client를 Dell Hybrid Client로 변환

전제조건

- Dell Ubuntu 일반 디바이스의 Ubuntu 18.04 또는 20.04를 Dell Hybrid Client로 변환하려면 DCA-Enabler 버전 1.2가 필요합니다. www.dell.com/support의 **드라이버 및 다운로드** 페이지에서 패키지를 다운로드할 수 있습니다.

- DCA Enabler 버전 1.0 또는 1.1이 디바이스에 설치되어 있으면 1.2로 업그레이드해야 합니다. DCA Enabler를 업그레이드하려면 디바이스를 Wyse Management Suite 3.2에 등록하고 Wyse Management Suite를 사용하여 `DCA_Enabler_ Package 1.2.0-xx`를 디바이스로 푸시한 다음 `DCA-Enabler 1.2.0-xx`를 배포해야 합니다.
- 디바이스가 복구 파티션에 Dell Hybrid Client 번들과 함께 사전 로드되지 않은 경우 먼저 DHC-Fish-Scripts 패키지를 배포하고 설치해야 합니다.

노트: DCA-Enabler 버전이 1.1.0-17 이하일 경우 Dell Ubuntu 디바이스는 Wyse Management Suite에 Dell Hybrid Client로 등록됩니다. DCA-Enabler 버전이 1.2.0-xx 이상인 경우 디바이스는 Dell Generic Client로 등록됩니다.

단계

1. DCA Enabler 버전 1.2를 사용하여 디바이스를 Wyse Management Suite에 등록합니다.
2. 다음 방법 중 하나를 사용하여 일반 클라이언트를 하이브리드 클라이언트로 변환합니다.
   - Convert to Hybrid Client 명령 사용 - Dell Generic Client를 하이브리드 클라이언트로 변환을 참조하십시오.
   - 애플리케이션 정책을 사용하여 Dell Hybrid Client 1.1/1.5 번들 또는 ISO 이미지 파일 배포 - 표준 애플리케이션 정책 생성 및 Dell Generic Client에 배포 및 고급 애플리케이션 정책 생성 및 Dell Generic Client에 배포를 참조하십시오.

     노트: 디바이스 변환이 시작되기 전에 DCA-Enabler는 Wyse Management Suite 연결 데이터를 백업한 다음 Dell Hybrid Client ISO 또는 설치 프로그램 번들을 트리거합니다.

     설치 프로그램이 변환을 완료하면 디바이스가 자동으로 재시작됩니다. 변환 후 디바이스가 변환된 Dell Hybrid Client 운영 체제로 부팅됩니다. Dell Client Agent는 백업된 Wyse Management Suite 연결 데이터를 읽고 Wyse Management Suite 서버에 Dell Hybrid Client 디바이스로 등록합니다.

예

Ubuntu 18.04 LTS를 실행하는 Dell Generic Client를 변환하려면 다음을 수행합니다.

- Dell Hybrid Client 1.0 또는 1.1에 대해서는 애플리케이션 정책을 사용하여 Dell Hybrid Client 1.0 또는 1.1 번들 패키지 파일을 푸시해야 합니다.
- Dell Hybrid Client 1.5의 경우 애플리케이션 정책을 사용하여 Dell Hybrid Client ISO 패키지를 푸시해야 합니다. OS 이미지 업그레이드 툴 `os-upgrade_1.1-10_amd64.deb` 패키지를 푸시하고 Dell Hybrid Client 1.5 ISO 패키지 파일을 푸시해야 합니다.

Ubuntu 20.04 LTS를 실행하는 Dell Generic Client를 Dell Hybrid Client 1.5로 변환하려면 애플리케이션 정책을 사용하여 Dell Hybrid Client 1.5 번들 패키지 파일을 푸시해야 합니다.

16

보안 구성

이 섹션에서는 Wyse Management Suite의 주요 보안 기능에 대해 설명하고 데이터 보호 및 적절한 액세스 제어를 보장하는 데 필요한 절차를 제공합니다.

주제:

- Wyse Management Suite 설치 프로그램에서 TLS 버전 구성 지원
- 퍼블릭 클라우드에서 Active Directory Federation Services 기능 구성
- 보안 LDAP 또는 LDAPS 설정 구성
- 더 이상 사용되지 않는 프로토콜

Wyse Management Suite 설치 프로그램에서 TLS 버전 구성 지원

Wyse Management Suite 3.0에서 Wyse Management Suite의 설치 또는 업그레이드 중에 TLS(Transport Layer Security) 버전을 선택할 수 있도록 온프레미스 설치 프로그램이 개선되었습니다. 권장되는 TLS(Transport Layer Security) 버전은 1.2입니다. 디바이스 에이전트 및 Merlin 이미지를 기반으로 적절한 모든 TLS 버전을 선택해야 합니다. 이전 버전의 Windows Embedded 시스템, Wyse Device Agent(WDA_14.4.0.135_Unified 이하 버전) 및 32비트 Merlin 이미지 버전은 TLSv1.0과만 호환됩니다. 또한 가져오기 툴은 TLSv1.0과만 호환됩니다.

노트: Dell Hybrid Client 1.5를 구성하려면 TLS 1.2를 선택해야 합니다.

퍼블릭 클라우드에서 Active Directory Federation Services 기능 구성

전제조건

- Notepad++ 또는 이와 동등한 애플리케이션이 서버에 설치되어 있어야 합니다.
- 서버에 ADFS가 설치되어 있어야 합니다.

단계

1. **포털 관리자** 페이지의 **콘솔 설정**에서 **AD(Active Directory)**를 클릭합니다.
2. **ADFS에 WMS 세부 정보 제공** 섹션에서 **WMS xml 파일 다운로드**를 클릭합니다.
   `CCM_SP_Metadata.xml` 파일이 다운로드됩니다.
3. 다운로드한 파일을 마우스 오른쪽 버튼으로 클릭하고 **Notepad++로 편집**을 선택합니다.
4. 파일에서 ID 값을 복사합니다. 예를 들어, ccm-sq3을 복사합니다.
5. ADFS 설정 콘솔로 이동합니다.
6. **릴레이 당사자 트러스트**를 마우스 오른쪽 버튼으로 클릭하고 **릴레이 당사자 트러스트 추가**를 선택합니다.
   릴레이 당사자 트러스트 추가 창이 표시됩니다.
7. **시작**을 클릭합니다.
   데이터 소스 선택 창이 표시됩니다.
8. **파일에서 릴레이 당사자에 대한 데이터 가져오기** 옵션을 선택하고 다운로드한 `CCM_SP_Metadata.xml` 파일을 찾습니다.
9. **다음**을 클릭합니다.
10. **표시 이름** 필드에 ID 값(ccm-sq3)을 입력하고 **다음**을 클릭합니다.
11. **액세스 제어 정책 선택** 페이지에서 **다음**을 클릭합니다.
12. **트러스트 추가 준비 완료** 페이지에서 **다음**을 클릭합니다.
13. **닫기**를 클릭합니다.

생성된 릴레이 트러스트가 **릴레이 당사자 트러스트** 콘솔에 나열됩니다.

14. Wyse Management Suite 퍼블릭 클라우드 서버에 로그인합니다.
15. **포털 관리** > **Active Directory**로 이동하고 **WMS 규칙 표시**를 클릭합니다.
16. **WMS 규칙** 창에 표시된 내용을 복사합니다.
17. ADFS 콘솔로 이동하여 릴레이 트러스트를 마우스 오른쪽 버튼으로 클릭하고 **클레임 발급 정책 편집**을 선택합니다.
18. **발급 변환 규칙** 탭에서 **규칙 추가**를 클릭합니다.
19. **확인**을 클릭합니다.
    규칙 템플릿 선택 창이 표시됩니다.
20. **클레임 규칙 템플릿** 드롭다운 목록에서 **사용자 지정 규칙을 사용하여 클레임 보내기** 옵션을 선택하고 **다음**을 클릭합니다.
21. **규칙 추가**를 클릭합니다.
22. **클레임 규칙 이름**을 입력하고 16단계에서 복사한 내용을 **사용자 지정 규칙** 필드에 붙여넣습니다.
23. **마침**을 클릭합니다.
24. **적용**을 클릭한 후 **확인**을 클릭합니다.
25. **포털 관리** > **Active Directory**로 이동하고 **구성 추가**를 클릭합니다.
26. 씬 클라이언트에 저장된 .xml 파일을 업로드하려면 **XML 파일 로드**를 클릭합니다.
    파일은 `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`에서 확인할 수 있습니다.
27. **구성 업데이트**를 클릭합니다.
28. 테넌트가 ADFS를 사용하여 SSO(Single Sign-On)를 구성할 수 있도록 하려면 **ADFS를 사용하여 SSO 활성화** 확인란을 선택합니다. 이 기능은 SAML(Security Assertion and Markup Language) 표준 사양을 따릅니다.
29. 구성 정보의 유효성을 검사하려면 **ADFS 로그인 테스트**를 클릭합니다. 이를 통해 테넌트는 저장하기 전에 설정을 테스트할 수 있습니다.
30. ADFS 자격 증명을 입력하고 **로그인**을 클릭합니다.
    ADFS가 구성되면 **테스트 성공** 메시지가 표시됩니다.
31. 원격 리포지토리에서 Wyse Management Suite 퍼블릭 클라우드로 AD 도메인 사용자를 가져옵니다.
32. **사용자** 페이지로 이동하여 가져온 AD 도메인 사용자에게 역할을 할당합니다.
33. Wyse Management Suite 퍼블릭 클라우드 포털로 이동하여 **도메인 자격 증명으로 로그인** 링크를 클릭합니다.
34. 가져온 AD 도메인 사용자의 이메일 주소를 입력하고 **로그인**을 클릭합니다.
    ADFS에 로그인하면 Wyse Management Suite 서버로 리디렉션됩니다.

보안 LDAP 또는 LDAPS 설정 구성

Active Directory 인증서 서비스에서 루트 인증서를 요청하고 보안 LDAP 또는 LDAPS 설정을 구성하려면 다음을 수행합니다.

단계

1. Active Directory 도메인 서버로 이동합니다.
2. **시작** > **실행**으로 이동합니다.
3. `mmc`를 입력하고 **확인**을 클릭합니다.
   Console1 창이 표시됩니다.
4. **파일** > **스냅인 추가 또는 제거**로 이동합니다.
5. 로컬 시스템에 인증서를 추가하고 **확인**을 클릭합니다.
6. 왼쪽 창에서 `Personal` 폴더를 확장합니다.
7. 인증서를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업** > **새 인증서 요청**으로 이동합니다.
   인증서 등록 창이 표시됩니다.
8. **다음**을 클릭합니다.
9. **인증서 등록 정책 선택** 탭에서 **다음**을 클릭합니다.
10. **도메인 컨트롤러**를 선택하고 **등록**을 클릭합니다.
    도메인 인증서가 도메인 컨트롤러에 설치됩니다.
11. **마침**을 클릭합니다.
    도메인 컨트롤러에 발급된 인증서가 인증서 페이지에 표시됩니다.
12. 인증서를 마우스 오른쪽 버튼으로 클릭하여 데스크탑으로 내보냅니다.

13. Wyse Management Suite 서버에 설정된 AD 도메인 서버 인증서를 Wyse Management Suite Java 키 저장소로 수동으로 가져옵니다. 인증서를 가져오려면 다음을 수행합니다.
    a. Wyse Management Suite가 설치된 서버로 이동합니다.
    b. **명령 프롬프트**를 열고 `<C:\Program Files\DELL\WMS\jdk-11.0.7\bin>keytool.exe> -importcert -alias <certificate name> -keystore "<C:\Program Files\Dell\WMS\jdk-11.0.7\lib\security\cacerts>" -storepass changeit -file "C:\<certificate name>` 명령을 실행합니다.
14. 인증서를 설치하면 Wyse Management Suite Tomcat Service가 재시작됩니다.
15. Wyse Management Suite 서버에 로그인합니다.
16. **포털 관리** > **AD(Active Directory)**로 이동합니다.
17. **AD 서버 정보 추가** 링크를 클릭합니다.
18. AD 도메인 이름을 입력합니다.
19. 서버 URL을 **ldaps://hostname.domain.com**으로 입력합니다. 예를 들어, **ldaps://WMS-DC97.WMSAD97.com**으로 입력합니다.
20. 포트 이름을 **636**으로 입력합니다.
21. **저장**을 클릭합니다.
22. **가져오기**를 클릭합니다.
23. 사용자 이름과 암호를 입력합니다.
24. **로그인**을 클릭합니다.
25. **사용자 그룹** 페이지에서 **그룹 이름**을 클릭하고 그룹 이름을 입력합니다.
26. **검색** 필드에 선택할 그룹 이름을 입력합니다.
27. 그룹을 선택합니다.
    선택한 그룹이 페이지의 오른쪽 창으로 이동됩니다.
28. **사용자 이름 콘텐츠 필드**에서 사용자 이름을 입력합니다.
29. **사용자 가져오기** 또는 **그룹 가져오기**를 클릭합니다.
    Wyse Management Suite 포털에는 가져온 Active Directory 사용자 수와 함께 확인 메시지가 표시됩니다. 가져온 Active Directory 사용자가 **사용자 탭** > **할당되지 않은 관리자**에 나열됩니다.

더 이상 사용되지 않는 프로토콜

SMB(Server Message Block) 프로토콜 버전 2.0은 더 이상 사용되지 않습니다.

17

Teradici 디바이스 관리

Teradici 디바이스 관리 섹션에서는 Teradici 디바이스의 관리 및 검색에 대한 정보를 제공합니다. Teradici 관리 콘솔은 SDK를 사용하여 Tera 디바이스에 대한 관리 및 구성을 지원합니다. Teradici 관리 콘솔은 Pro 라이선스 유형이 있는 Wyse Management Suite 프라이빗 클라우드에만 적용됩니다.

주제:

- Teradici 디바이스 검색
- CIFS 사용 사례 시나리오

Teradici 디바이스 검색

사전 요구 사항

- Microsoft Windows 2012 Server 이상 버전에 최신 버전의 Wyse Management Suite를 설치합니다. Threadx 5.x 및 6.x 디바이스는 최신 버전의 운영 체제에서 작동합니다.
- **EMSDK** 구성 요소를 설치하고 활성화합니다.
- Wyse Management Suite 서버의 FQDN을 **DHCP** 또는 **DNS** 구성으로 사용할 수 있어야 합니다.
- `Cert.pem`이 기본 경로인 `C:\Program Files\Dell\WMS\Teradici\EMSDK`에 있어야 합니다. Threadx 디바이스를 검색하는 데 사용됩니다.

보안 수준

엔드포인트에 구성된 보안 수준에 따라 EBM/EM 인증서를 사용하여 엔드포인트를 프로비저닝해야 할 수도 있습니다.

중간 또는 높은 보안을 위해 구성된 엔드포인트는 EBM 또는 EM에 연결하기 전에 인증서 저장소에 신뢰할 수 있는 인증서가 있어야 합니다. 일부 엔드포인트의 경우 공급업체가 인증서를 출하 시 기본값으로 사전 로드했을 수 있습니다. 그렇지 않으면 엔드포인트의 AWI를 사용하여 인증서를 수동으로 업로드할 수 있습니다.

다음 중 하나가 참인 경우 낮은 보안으로 구성된 엔드포인트는 신뢰할 수 있는 인증서 저장소에 MC 인증서가 필요하지 않습니다.

- DHCP 검색 또는 DNS 검색을 사용하고 있으며 DHCP 또는 DNS 서버가 EBM 인증서의 지문으로 이를 프로비저닝했습니다.
- 수동 검색 방법을 사용하여 검색됩니다.

표 11. 엔드포인트에 대한 인증서 요구 사항

검색 방법	낮은 보안	중간 보안	높은 보안
EBM 지문을 프로비저닝하지 않고 DHCP/DNS 검색	인증서 필요	인증서 필요	적용되지 않음
EBM 지문으로 프로비저닝하여 DHCP/DNS 검색	인증서가 필요하지 않음	인증서 필요	적용되지 않음
높은 보안 환경을 위해 구성된 엔드포인트에 의해 검색이 시작됨	적용되지 않음	적용되지 않음	인증서 필요
MC에서 시작된 수동 검색	인증서가 필요하지 않음	적용되지 않음	적용되지 않음

클라이언트에서 수동 검색

1. `https://<clientIP>`로 이동합니다.
2. 인증서 경고 메시지를 수락합니다.
3. 관리자 암호(기본 암호는 Administrator)를 입력하고 로그인합니다.

4. **업로드** > **인증서**로 이동합니다. 기본 경로에서 `Cert.pem` 파일을 선택하고 **업로드**를 클릭합니다.
5. **구성** > **관리**로 이동합니다. **관리 상태 지우기** 버튼을 클릭하여 디바이스를 새 관리 서버에 등록합니다.
6. **관리자 검색 모드**를 수동으로 설정합니다.
7. **엔드포인트 부트스트랩 관리자 URL**을 **wss://<WMS 서버의 IP 주소>** 형식으로 입력

   노트: EMSDK가 사용자 지정 포트와 함께 설치된 경우 **엔드포인트 부트스트랩 관리자 URL**을 **wss://<IP 주소:맞춤형 포트** 형식으로 입력합니다.
8. **적용**을 클릭한 다음 **계속**을 클릭합니다.
9. **관리 상태**가 엔드포인트 서버에 연결된 것으로 표시됩니다.

DHCP 서버에 PCoIP 엔드포인트 공급업체 클래스 추가

1. DHCP 서버에 로그인합니다.
2. **서버** 창에서 DHCP 서버를 마우스 오른쪽 버튼으로 클릭하고 **DHCP 관리자**를 선택합니다.
3. **IPv4** 옵션을 마우스 오른쪽 버튼으로 클릭한 다음 **공급업체 클래스 정의**를 선택합니다.
4. **추가**를 클릭하여 새 DHCP 공급업체 클래스를 추가합니다.
5. **디스플레이 이름** 필드에 **PCoIP 엔드포인트**를 입력합니다.
6. **ASCII** 열에 공급업체 ID로 **PCoIP 엔드포인트**를 입력합니다.
7. **확인**을 클릭하여 설정을 저장합니다.

DHCP 옵션 구성

1. **IPv4** 옵션을 마우스 오른쪽 단추로 클릭한 다음 **미리 정의된 옵션 설정**을 선택합니다.
2. **옵션** 클래스로 **PCoIP 엔드포인트**를 선택한 다음 **추가**를 클릭합니다.
3. **옵션 유형** 대화 상자에서 이름을 **EBM URI**로, 데이터 유형을 **스트링**으로, 코드를 **10**으로, 설명을 **엔드포인트 부트스트랩 관리자 URI**로 입력한 다음 **확인**을 클릭합니다.
4. **확인**을 클릭하여 설정을 저장합니다.
5. 옵션을 적용할 DHCP 범위를 확장합니다.
6. **범위 옵션**을 마우스 오른쪽 버튼으로 클릭한 다음 **구성 옵션**을 선택합니다.
7. **고급** 탭을 클릭한 다음 **PCoIP 엔드포인트** 공급업체 클래스를 선택합니다.
8. **010 EBM URI** 확인란을 선택한 다음 **스트링** 필드에 유효한 관리 콘솔 URI를 입력합니다. **적용**을 클릭합니다. 이 URL에는 보안 WebSocket 접두사가 필요합니다(예: `wss://<MC IP address>:[port number]`). 5172는 MC의 수신 포트입니다. 이 포트 번호를 입력하는 것은 선택 사항 단계입니다.
9. **확인**을 클릭하여 설정을 저장합니다.
10. **옵션** 클래스로 **PCoIP 엔드포인트**를 선택한 다음 **추가**를 클릭합니다.
11. **옵션 유형** 대화 상자에서 이름을 **EBM X.509 SHA-256 fingerprint**로, 데이터 유형을 **스트링**으로, 코드를 **11**로, 설명을 **EBM X.509 SHA-256 fingerprint**로 입력한 다음 **확인**을 클릭합니다.
12. 옵션을 적용할 DHCP 범위를 확장합니다.
13. **범위 옵션**을 마우스 오른쪽 버튼으로 클릭한 다음 **구성 옵션**을 선택합니다.
14. **고급** 탭을 클릭한 다음 **PCoIP 엔드포인트** 공급업체 클래스를 선택합니다.
15. **011 EBM X.509 SHA-256 fingerprint** 확인란을 선택하고 SHA-256 지문을 붙여넣습니다.
16. **확인**을 클릭하여 설정을 저장합니다.
17. 클라이언트 웹 브라우저로 이동합니다.
18. **구성** > **관리**로 이동하여 **관리자 검색 모드**를 **자동**으로 설정합니다.

19. 클라이언트가 DHCP 서버에 표시된 서버에 연결되어 있습니다.

DNS SRV 레코드 생성

1. **DNS 서버**에 로그인합니다.
2. **서버** 창에서 DNS 서버를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **DNS 관리자**를 선택합니다.
3. **정방향 조회 영역**에서 도메인을 마우스 오른쪽 버튼으로 클릭한 다음 컨텍스트 메뉴에서 **다른 새 레코드**를 선택합니다.
4. **리소스 레코드 유형** 대화 상자의 목록에서 **서비스 위치(SRV)**을 선택하고 **레코드 생성**을 클릭합니다.
5. **서비스**를 **_pcoip-bootstrap**으로, 프로토콜을 **_tcp**로, **포트 번호**를 **5172**(MC의 기본 수신 포트)로 설정합니다. **이 서비스를 제공하는 호스트**에는 MC의 FQDN을 입력합니다.

   노트: DNS 사양이 SRV 레코드의 IP 주소를 허용하지 않으므로 MC의 FQDN을 입력해야 합니다.
6. **확인**을 클릭합니다.

DNS TXT 레코드 추가

1. **정방향 조회 영역**에서 도메인을 마우스 오른쪽 버튼으로 클릭한 다음 컨텍스트 메뉴에서 **다른 새 레코드**를 선택합니다.
2. **리소스 레코드 유형** 대화 상자의 목록에서 **텍스트(TXT)**를 선택한 다음 **레코드 생성**을 클릭합니다.
3. 다음 세부 사항을 입력합니다.
   a. **레코드 이름** 필드에 서비스를 제공하는 Wyse Management Suite 서버의 호스트 이름을 입력합니다. FQDN 필드는 자동으로 채워집니다. 이 필드는 Wyse Management Suite 서버의 FQDN과 일치해야 합니다.
   b. **텍스트** 필드에 **pcoip-bootstrap-cert=**를 입력한 다음 Wyse Management Suite 서버 인증서 SHA-256 지문을 붙여넣습니다.
4. **확인**을 클릭합니다.
5. 클라이언트 웹 브라우저로 이동합니다.
6. 클라이언트가 DNS 서버에 표시된 Wyse Management Suite 서버에 연결되어 있습니다.

SHA-256 지문 생성

1. Mozilla Firefox를 시작합니다.
2. **고급 옵션** 탭으로 이동합니다.
3. **인증서**를 클릭하여 인증서를 봅니다.
4. **인증서 관리자**에서 **인증 기관**을 클릭하고 **가져오기**를 클릭합니다.
5. 인증서를 찾아서 **보기**를 클릭합니다.
6. **SHA-256** 지문을 복사합니다.

CIFS 사용 사례 시나리오

Wyse Management Suite에서는 다음과 같은 사용 사례가 지원됩니다.

- Wyse Management Suite 프라이빗 클라우드를 설치하는 동안 **Wyse Management Suite**를 **유형 설정**으로 선택하는 경우.
  - CIFS 구성 페이지가 표시됩니다. 이 페이지는 공유 폴더 구성에 필요합니다.

    노트: 기본적으로 **CIFS 사용자 자격 증명 구성** 옵션이 비활성화됩니다.
- Wyse Management Suite 프라이빗 클라우드를 설치하는 동안 **Teradici EMSDK**를 **유형 설정**으로 선택하는 경우.
  - CIFS 자격 증명에 기존 계정을 사용하거나 새 계정을 생성할 수 있습니다.

- Wyse Management Suite 프라이빗 클라우드를 설치하는 동안 **Wyse Management Suite** 및 **Teradici EMSDK**를 모두 **유형 설정**으로 선택하는 경우.
  - CIFS 구성 페이지가 표시됩니다. 이 페이지는 공유 폴더 구성에 필요합니다.

    노트: 기본적으로 **CIFS 사용자 자격 증명 구성** 옵션이 비활성화됩니다.
  - CIFS 자격 증명에 기존 계정을 사용하거나 새 계정을 생성할 수 있습니다.
- EMSDK 서비스가 이미 설치되어 있는 시스템에 EMSDK만 설치하는 경우.
  - Teradici EMSDK를 선택하면 **유형 설정** 페이지에서 **다음**을 클릭할 때 경고 메시지가 표시됩니다. 메시지는 다음과 같습니다. **설치 프로그램이 Teradici EMSDK가 이미 설치되어 있음을 감지했습니다. 필요한 경우 EMSDK가 업데이트됩니다**. 포트 번호가 필요하지 않습니다.
    - **CIFS 사용자 자격 증명 구성** 옵션을 선택하는 경우(기본값)
      1. 서비스를 중지합니다.
      2. EMSDK 서비스를 업데이트합니다.
      3. 서비스를 재시작합니다. 미리 구성된 동일한 사용자로 작동합니다.
    - **기존 사용자 사용** 옵션과 함께 **CIFS 사용자 자격 증명 구성** 옵션을 선택하는 경우
      1. 서비스를 중지합니다.
      2. EMSDK 서비스를 업데이트합니다.
      3. 서비스 로그온 사용자를 선택한 사용자로 업데이트합니다.
      4. 서비스를 재시작합니다. 미리 구성된 동일한 사용자로 작동합니다.
    - **새로운 사용자 생성** 옵션과 함께 **CIFS 사용자 자격 증명 구성** 옵션을 선택하는 경우.
      1. 서비스를 중지합니다.
      2. EMSDK 서비스를 업데이트합니다.
      3. 서비스 로그온 사용자를 새로 생성한 사용자로 업데이트합니다.
      4. 서비스를 재시작합니다. 미리 구성된 동일한 사용자로 작동합니다.
- EMSDK 서비스가 이미 설치되어 있는 시스템에 **Wyse Management Suite** 및 **Teradici EMSDK**를 모두 설치하는 경우.
  - **CIFS 사용자 자격 증명 구성** 옵션이 기본적으로 선택되고 회색으로 표시된다는 점을 제외하면 **EMSDK 서비스가 이미 설치되어 있는 시스템에 EMSDK만 설치하는 경우**와 같습니다. CIFS 자격 증명을 입력해야 합니다.

18

라이선스 구독 관리

이 섹션에서는 관리 콘솔 라이선스 구독 및 해당 사용량을 보고 관리할 수 있습니다.

포털 어드민 페이지에서 **구독** 옵션을 볼 수 있습니다. 이 페이지에서는 다음과 같은 정보를 제공합니다.

- 라이선스 구독
- 라이선스 주문
- 라이선스 사용 - 등록된 씬 클라이언트 디바이스
- 서버 정보
- 라이선스 가져오기 - 프라이빗 클라우드
- 프라이빗 클라우드용 라이선스 내보내기 - 퍼블릭 클라우드

주제:

- Wyse Management Suite 퍼블릭 클라우드에서 라이선스 가져오기
- Wyse Management Suite 프라이빗 클라우드로 라이선스 내보내기
- 씬 클라이언트 라이선스 할당
- 라이선스 주문
- 라이선스 만료 이메일 알림 구성

Wyse Management Suite 퍼블릭 클라우드에서 라이선스 가져오기

Wyse Management Suite 퍼블릭 클라우드에서 Wyse Management Suite 프라이빗 클라우드로 라이선스를 가져올 수 있습니다.

단계

1. Wyse Management Suite 프라이빗 클라우드 콘솔에 로그인합니다.
2. **포털 관리** > **계정** > **구독**으로 이동합니다.
3. 다음과 같은 Wyse Management Suite 퍼블릭 클라우드 세부 정보를 입력합니다.
   - 사용자 이름
   - 암호
   - 데이터 센터
   - TC 시트 수
   - Edge Gateway 및 내장형 PC 시트 수
   - Wyse 소프트웨어 씬 클라이언트 시트 수
   - 하이브리드 클라이언트 시트 수
   - 일반 클라이언트 시트/디바이스 수
4. **가져오기**를 클릭합니다.

   노트: Wyse Management Suite 프라이빗 클라우드를 Wyse Management Suite 퍼블릭 클라우드에 연결해야 합니다.

   노트: 관리할 수 있는 일반 디바이스의 총 개수는 하이브리드 클라이언트 및 씬 클라이언트 라이선스에 사용할 수 있는 총 시트 수에 따라 달라집니다.

Wyse Management Suite 프라이빗 클라우드로 라이선스 내보내기

Wyse Management Suite 퍼블릭 클라우드에서 Wyse Management Suite 프라이빗 클라우드로 라이선스를 내보낼 수 있습니다.

단계

1. Wyse Management Suite 퍼블릭 클라우드 콘솔에 로그인합니다.
2. **포털 관리** > **계정** > **구독**으로 이동합니다.
3. Wyse Management Suite 프라이빗 클라우드로 내보내야 하는 씬 클라이언트 시트 수를 입력합니다.
4. **내보내기**를 클릭합니다.
5. 생성된 라이선스 키를 복사합니다.
6. Wyse Management Suite 프라이빗 클라우드 콘솔에 로그인합니다.
7. **포털 관리** > **계정** > **구독**으로 이동합니다.
8. 상자에 생성된 라이선스 키를 입력합니다.
9. **가져오기**를 클릭합니다.

씬 클라이언트 라이선스 할당

Wyse Management Suite 프라이빗 클라우드와 Wyse Management Suite 퍼블릭 클라우드 계정 간에 씬 클라이언트 라이선스를 할당할 수 있습니다.

단계

1. Wyse Management Suite 퍼블릭 클라우드 콘솔에 로그인합니다.
2. **포털 관리** > **계정** > **구독**으로 이동합니다.
3. 씬 클라이언트 시트의 수를 입력합니다.

   노트: 씬 클라이언트 시트는 퍼블릭 클라우드에서 관리할 수 있습니다. 입력한 씬 클라이언트 시트의 수는 **관리 가능** 옵션에 표시된 수를 초과해서는 안 됩니다.

4. **내보내기**를 클릭합니다.

   노트: 퍼블릭 클라우드 라이선스 수는 프라이빗 클라우드로 내보낸 씬 클라이언트 시트 수에 따라 조정됩니다.

5. 생성된 라이선스 키를 복사합니다.
6. Wyse Management Suite 프라이빗 클라우드 콘솔에 로그인합니다.
7. **포털 관리** > **계정** > **구독**으로 이동합니다.
8. 내보낸 라이선스 키를 프라이빗 클라우드로 가져옵니다.

   노트: 현재 프라이빗 클라우드에서 관리 중인 디바이스의 수를 관리하기 위한 씬 클라이언트 시트가 충분하지 않으면 라이선스를 가져올 수 없습니다. 이 경우에는 3~8 단계를 반복하여 씬 클라이언트 시트를 할당합니다.

   노트: Wyse Management Suite 3.2에서 이전 Wyse Management Suite 서버는 퍼블릭 클라우드에서 온라인으로 활성화할 수 없습니다.

라이선스 주문

퍼블릭 클라우드의 **라이선스 주문** 섹션에는 만료된 라이선스를 포함하여 접수된 주문의 목록이 표시됩니다. 기본적으로 만료된 주문은 표시되지 않습니다. 만료된 주문을 보려면 **만료된 주문 포함** 확인란을 선택합니다. 만료된 주문은 빨간색으로 표시되고 30일 이내에 만료되는 주문은 주황색으로 표시됩니다.

노트: 이 기능은 주문 기록을 표시하지 않으므로 온프레미스 배포에는 적용되지 않습니다. 그러나 테넌트 관리자로 퍼블릭 클라우드 포털에 로그인하면 온프레미스 라이선스 주문 기록을 사용할 수 있습니다.

라이선스 만료 이메일 알림 구성

라이선스 만료 이메일 알림을 활성화할 수 있습니다. 라이선스가 만료되기 전에 테넌트에 이메일 알림이 발송됩니다.

단계

1. Wyse Management Suite 프라이빗 클라우드에 로그인합니다.

2. **포털 관리** > **기타 설정**으로 이동합니다.
3. **라이선스 만료 이메일 알림 활성화** 확인란을 선택합니다.
   라이선스가 다음 기간 후에 만료될 시 이메일 알림이 발송됩니다.
   - 60일
   - 30일
   - 14일

   노트: 라이선스 만료 이메일 알림 활성화 옵션은 기본적으로 활성화되어 있습니다.

   또한 라이선스가 만료된 후 24시간 후에 알림이 전송됩니다.

19

Firmware upgrade

Wyse Management Suite를 사용하여 펌웨어를 업그레이드할 수 있습니다.

주제:

- ThinLinux 1.x를 2.1 이상 버전으로 업그레이드
- ThinOS 8.x를 9.0으로 업그레이드

ThinLinux 1.x를 2.1 이상 버전으로 업그레이드

업그레이드하기 전에 TL 2.x에서 사용자 지정 이미지를 가져오려면, ThinLinux 2.x를 준비한 다음 ThinLinux 1.x 이미지를 업그레이드해야 합니다.

ThinLinux 2.x 이미지 준비

전제조건

Wyse Management Suite 버전 1.4 이상을 사용하여 ThinLinux 빌드 버전 2.0.19 또는 2.1을 2.2로 업그레이드합니다.

단계

1. www.dell.com/support로 이동합니다.
2. **제품 지원**을 클릭하여 씬 클라이언트의 **서비스 태그**를 입력한 후 **Enter**를 누릅니다.

   노트: **서비스 태그**가 없는 경우 씬 클라이언트 모델을 수동으로 찾습니다.

3. **드라이버 및 다운로드**를 클릭합니다.
4. **운영 체제** 드롭다운 목록에서 **ThinLinux**를 선택합니다.
5. `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` 및 `wda_3.4.6-05_amd64.tar` 애드온을 다운로드합니다.
6. 다운로드한 애드온을 `<drive C>/wms/localrepo/repository/thinClientsApps/`에 복사합니다.
7. ThinLinux 2.x를 실행하는 씬 클라이언트에서 **설정** > **관리** > **Wyse Device Agent** 로 이동합니다.
8. Wyse Management Suite 서버에 디바이스를 등록합니다.
9. **설정** 창을 닫습니다.

   노트: 설정창이 닫히지 않은 경우 이미지가 배포되면 **프로필 잠김** 오류가 표시됩니다.

10. Wyse Management Suite 콘솔에 로그인합니다.
11. `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` 및 `wda_3.4.6-05_amd64.tar` 애드온에 대한 앱 정책을 생성하고 배포합니다.
12. 씬 클라이언트를 재부팅합니다.
13. Wyse Management Suite 서버에 로그인합니다.
14. 디바이스 페이지로 이동하여 Merlin 및 WDA 버전이 업데이트되었는지 확인합니다.
15. 등록된 디바이스를 클릭하고 **기타 작업** > **OS 이미지 가져오기**로 이동합니다.
    OS 이미지 가져오기 창이 표시됩니다.
16. 이미지의 이름을 입력합니다.
17. 파일 리포지토리 드롭다운 목록에서 파일 리포지토리를 선택합니다.
18. 수행할 끌어오기 작업의 유형을 선택합니다.
    - **기본**—**OS+복구** 확인란을 선택하고 이미지(압축/압축 해제)를 끌어옵니다.
    - **고급**—`Compress_OS_Recovery_Commandsxml/uncompress_OS_Recovery_CommandsXml` 템플릿을 선택하고 이미지를 끌어옵니다.

결과

노트:

- Wyse Management Suite 1.3 원격 리포지토리를 사용하는 경우 XML 파일을 리포지토리에서 사용할 수 없습니다. 파일에 액세스하려면 Wyse Management Suite를 1.4 이상으로 업그레이드해야 합니다.
- 복구 끌어오기 작업으로 사용자 설정이 유지되지 않습니다.

ThinLinux 1.x를 2.x로 업그레이드

단계

1. www.dell.com/support로 이동합니다.
2. **제품 지원**을 클릭하여 씬 클라이언트의 **서비스 태그**를 입력한 후 **Enter**를 누릅니다.

   노트: 서비스 태그가 없는 경우 씬 클라이언트 모델을 수동으로 찾습니다.

3. **드라이버 및 다운로드**를 클릭합니다.
4. **운영 체제** 드롭다운 목록에서 **ThinLinux**를 선택합니다.
5. 페이지를 아래로 스크롤하여 다음을 수행합니다.
   - `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` 및 `merlin-nonpxe_3.7.7-00.05_amd64.deb` 애드온을 다운로드합니다.
   - 최신 ThinLinux 버전 2.x 이미지 파일(`2.1.0.01_3040_16GB_merlin.exe or 2.2.0.00_3040_merlin_16GB.exe`)을 다운로드합니다.
6. 씬 클라이언트에서 **설정** > **관리** > **Wyse Device Agent**로 이동합니다.
7. Wyse Management Suite 서버에 디바이스를 등록합니다.
8. Wyse Management Suite 콘솔에 로그인합니다.
9. `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` 및 `merlin-nonpxe_3.7.7-00.05_amd64.deb` 애드온에 대한 앱 정책을 생성하고 배포합니다.
10. 씬 클라이언트를 재부팅합니다.
11. Wyse Management Suite 서버에 로그인합니다.
12. 다운로드한 이미지(`2.2.0.00_3040_merlin_16GB.exe` 파일)를 `<drive C>/wms/localrepo/repository/osimages/zipped/` 에 복사합니다.

    노트: 압축된 폴더의 이미지가 유효한 폴더에 압축이 풀립니다. 추출 과정은 10-15분 정도 걸릴 수 있습니다.

13. Wyse Management Suite 콘솔에 로그인합니다.
14. **앱 및 데이터** > **OS 이미지 리포지토리** > **WES/ThinLinux**로 이동하여 ThinLinux 이미지를 사용할 수 있는지 확인합니다.
15. **앱 및 데이터** > **OS 이미지 정책(WES/ThinLinux)**으로 이동하고 **앱 정책**을 클릭합니다.
16. 정책 추가 창에서 다음 옵션을 구성합니다.
    - **OS 유형** - ThinLinux
    - **OS 하위 필터** - ThinLinux(ThinLinux)
    - **규칙** - 업그레이드 전용/이 버전 강제 적용

    노트: 정책을 생성하는 동안 리포지토리에 복사된 가져온 이미지/새 이미지를 선택합니다.

17. 필요에 따라 다른 필수 필드를 업데이트하고 **저장**을 클릭합니다.
18. 작업을 예약합니다.
19. 이미지를 업데이트하려면 클라이언트에서 **지금 업데이트**를 클릭합니다.

ThinOS 8.x를 9.0으로 업그레이드

ThinOS 펌웨어를 9.0으로 업그레이드하려면 Wyse Management Suite 버전 2.0 이상을 사용해야 합니다.

다음 표에는 ThinOS 펌웨어 이미지가 나와 있습니다.

표 12. 펌웨어 이미지

플랫폼	ThinOS 펌웨어 이미지
Wyse 3040 씬 클라이언트	A10Q_wnos
Wyse 5070 씬 클라이언트 - 셀러론 프로세서	X10_wnos
Wyse 5070 씬 클라이언트 - 펜티엄 프로세서	X10_wnos
Wyse 5070 Extended 씬 클라이언트 - 펜티엄 프로세서	X10_wnos
Wyse 5470 씬 클라이언트	X10_wnos
Wyse 5470 All-in-One 씬 클라이언트	X10_wnos

리포지토리에 ThinOS 9.x 펌웨어 추가

단계

1. Wyse Management Suite로 로그인합니다.
2. **앱 및 데이터** 탭의 **OS 이미지 리포지토리**에서 **ThinOS 9.x**를 클릭합니다.
3. **펌웨어 파일 추가**를 클릭합니다.
   파일 추가 화면이 표시됩니다.
4. 파일을 선택하려면 **찾아보기**를 클릭하고 파일이 있는 위치로 이동합니다.
5. 파일에 대한 설명을 입력합니다.
6. 기존 파일을 덮어쓰려면 확인란을 선택합니다.
7. **업로드**를 클릭합니다.

   노트: 확인란을 선택했지만 그룹 또는 디바이스에 할당되지 않은 경우 해당 파일이 리포지토리에 추가됩니다. 디바이스 또는 디바이스 그룹에 펌웨어를 배포하려면 해당 디바이스 또는 그룹 구성 페이지로 이동합니다.

   노트: 운영자는 운영자 계정에서 펌웨어를 업로드할 수 있으며 모든 테넌트에 표시됩니다. 테넌트는 파일을 삭제하거나 수정할 수 없습니다.

ThinLinux 8.6을 ThinOS 9.x로 업그레이드

전제조건

- 사용 가능한 최신 BIOS를 설치하고 ThinOS 8.6_807로 업그레이드해야 합니다. 자세한 BIOS 업그레이드 방법은 *www.dell.com/support*에서 Dell Wyse ThinOS 8.6 문서를 참조하십시오.
- ThinOS 변환 이미지를 ThinOS 펌웨어 리포지토리에 추가해야 합니다. 자세한 내용은 리포지토리에 ThinOS 펌웨어 추가를 참조하십시오.
- Wyse Management Suite에서 그룹 토큰으로 그룹을 생성합니다. 이 그룹 토큰을 사용하여 ThinOS 8.6 디바이스를 등록합니다.
- 씬 클라이언트는 Wyse Management Suite에 등록해야 합니다.
- Wyse Management Suite에서 배경 화면 설정을 구성하지 마십시오.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS**를 클릭합니다.
   ThinOS 구성 모드 선택 창이 표시됩니다.
3. **고급 구성 모드**를 선택합니다.
4. **펌웨어 업그레이드**로 이동하여 **이 항목 구성**을 클릭합니다.
5. 즉시 업그레이드하려면 **라이브 업그레이드 비활성화**를 해제하고 **서명 확인** 확인란의 선택을 취소합니다.
6. **플랫폼 유형** 드롭다운 목록에서 플랫폼을 선택합니다.
7. **자동 배포할 펌웨어** 드롭다운 목록에서 리포지토리에 추가된 펌웨어를 선택합니다.
8. **저장 및 게시**를 클릭합니다.
   펌웨어가 씬 클라이언트에 배포됩니다. 변환 프로세스는 15~20초가 소요되며 씬 클라이언트가 자동으로 재시작됩니다.

Wyse Management Suite를 사용하여 ThinOS 9.x 이상 버전으로 업그레이드

전제조건

- 씬 클라이언트에서 ThinOS 9.0.4024 이상 버전을 실행하고 있는지 확인합니다.
- Wyse Management Suite에서 그룹 토큰으로 그룹을 생성해야 합니다. 이 그룹 토큰을 사용하여 ThinOS 9.x 디바이스를 등록합니다.
- 씬 클라이언트를 Wyse Management Suite에 등록해야 합니다.

단계

1. **그룹 및 구성** 페이지로 이동하여 그룹을 선택합니다.
2. **정책 편집** 드롭다운 메뉴에서 **ThinOS 9.x**를 클릭합니다.
   구성 제어 | ThinOS 창이 표시됩니다.
3. **고급**을 클릭합니다.
4. **펌웨어** 필드에서 **OS 펌웨어 업데이트**를 선택합니다.
5. **탐색**을 클릭하여 펌웨어를 찾아 업로드합니다.
   패키지의 EULA 세부 정보와 공급업체 이름이 표시됩니다.
   노트: ThinOS 9.1.3112에는 두 개의 이미지가 있습니다. 하나는 ThinOS 9.0.4024에서 업그레이드하기 위한 이미지이고 다른 하나는 ThinOS 9.1의 이전 버전에서 업그레이드하기 위한 것입니다. 원하는 이미지를 선택합니다.
6. 공급업체 이름을 클릭하여 각 공급업체의 라이선스 계약을 읽은 다음 **수락**을 클릭하여 패키지를 업로드합니다.
   동일한 공급업체의 EULA 세부 정보를 다시 보지 않으려면 **이 정보를 다시 표시하지 않음**을 선택할 수 있습니다.
   노트: 여러 패키지를 업로드하면 각 패키지의 EULA 세부 정보가 표시됩니다. 패키지의 라이선스 계약에 개별적으로 동의해야 합니다. **거부**를 클릭하면 펌웨어가 업로드되지 않습니다.
7. **배포할 ThinOS 펌웨어 선택** 드롭다운 메뉴에서 업로드된 펌웨어를 선택합니다.
8. **저장 및 게시**를 클릭합니다.
   씬 클라이언트는 펌웨어를 다운로드하고 재시작됩니다. 펌웨어 버전이 업그레이드됩니다.

20

원격 리포지토리

Wyse Management Suite에서 애플리케이션, 운영 체제 이미지 등에 대한 로컬 및 원격 리포지토리를 사용할 수 있습니다. 사용자 계정이 여러 지역에 분산되어 있는 경우 디바이스가 로컬 리포지토리에서 이미지를 다운로드할 수 있도록 각 분산 사용자 계정에 별도의 로컬 리포지토리를 사용하는 것이 효율적일 것입니다. 이러한 유연성은 `WMS_Repo.exe` 소프트웨어로 제공합니다. `WMS_Repo.exe`는 Wyse Management Suite에 등록할 수 있는 분산형 원격 리포지토리를 생성하는 데 도움이 되는 Wyse Management Suite 파일 리포지토리 소프트웨어입니다. `WMS_Repo.exe`는 **Pro** 라이선스 구독자만 사용할 수 있습니다.

전제조건

- Wyse Management Suite를 클라우드 배포와 함께 사용하는 경우**포털 관리** > **콘솔 설정** > **파일 리포지토리**로 이동합니다. **다운로드 버전 x.x**(을)를 클릭하고 `WMS_Repo.exe` 파일을 다운로드합니다.
- Wyse Management Suite 리포지토리 소프트웨어 설치를 위한 서버 요구 사항은 다음과 같습니다.
  - Windows 2012 R2 또는 Windows 2016 Server Standard
  - 4 CPU
  - 8GB RAM
  - 40GB 스토리지 공간

노트: Azure, Amazon Web Services 및 Google Cloud Platform과 같은 클라우드 호스팅 서버에서는 Wyse Management Suite 서버 및 리포지토리 설치가 지원되지 않습니다.

이 작업 정보

WMS-Repo 소프트웨어를 설치하려면 다음을 수행합니다.

단계

1. **관리자**로 로그인하고 `WMS_Repo.exe`를 리포지토리 서버에 설치합니다.
2. **다음**을 클릭하고 화면의 지시사항에 따라 설치를 완료합니다.
3. **실행**을 클릭하여 웹 브라우저에서 **WMS Repository 등록** 화면을 시작합니다.
4. 퍼블릭 클라우드에 등록하는 경우 **퍼블릭 WMS 관리 포털에 등록**을 선택합니다.

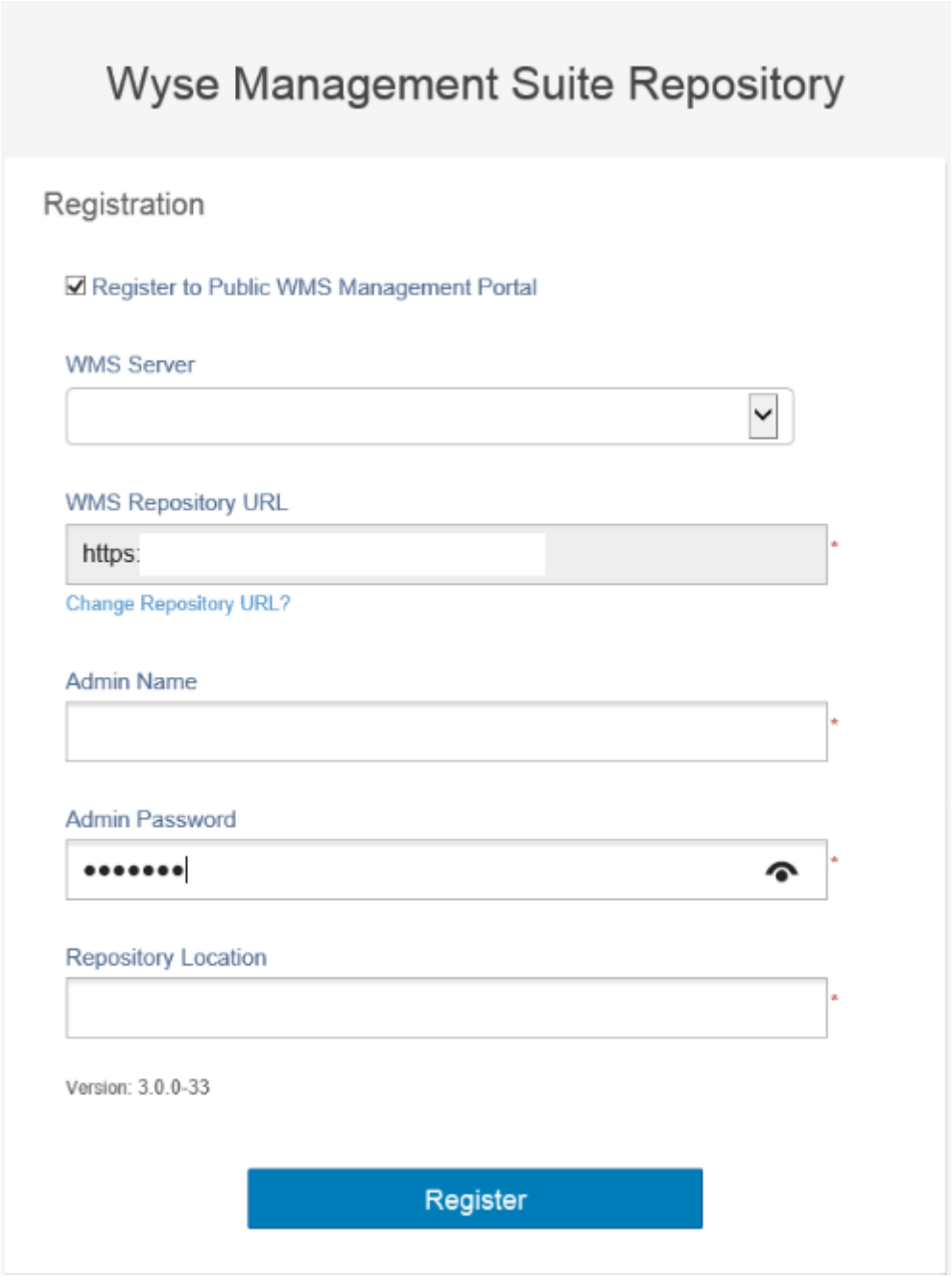


그림 22 . 퍼블릭 클라우드에 등록

5. 다음 세부 사항을 입력합니다.
   a. Wyse Management Suite 서버 URL

      노트: Wyse Management Suite 버전 1.0에 등록하지 않으면 MQTT 서버 URL을 사용할 수 없습니다.

   b. WMS 리포지토리 URL(URL을 도메인 이름으로 업데이트)
   c. Wyse Management Suite 관리자 로그인 사용자 이름 정보
   d. Wyse Management Suite 관리자 로그인 암호 정보
   e. 리포지토리 경로 정보
6. **등록**을 클릭합니다.
7. 등록에 성공하면 **등록** 창이 표시됩니다.

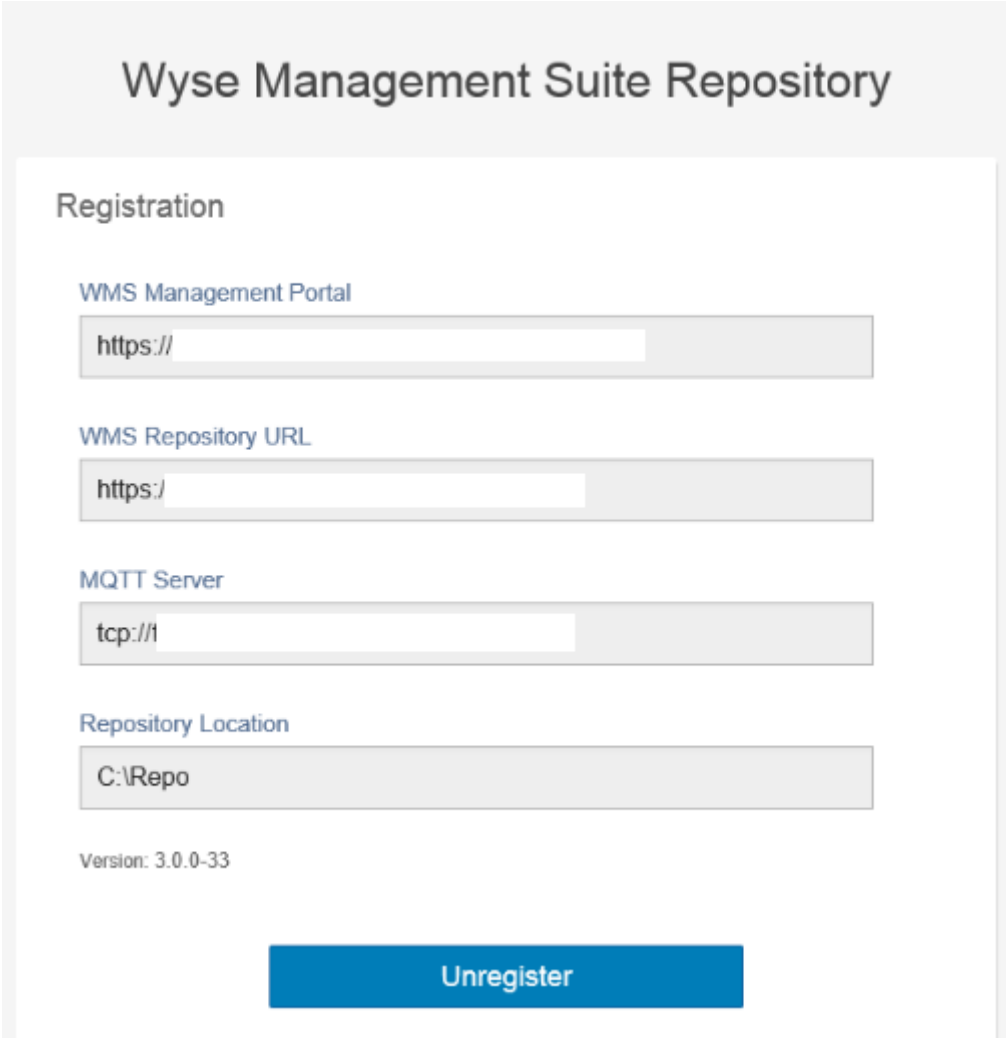


그림 23 . 등록 성공

8. Wyse Management Suite 포털의 다음 화면은 원격 리포지토리 등록에 성공하였다는 것을 나타냅니다.

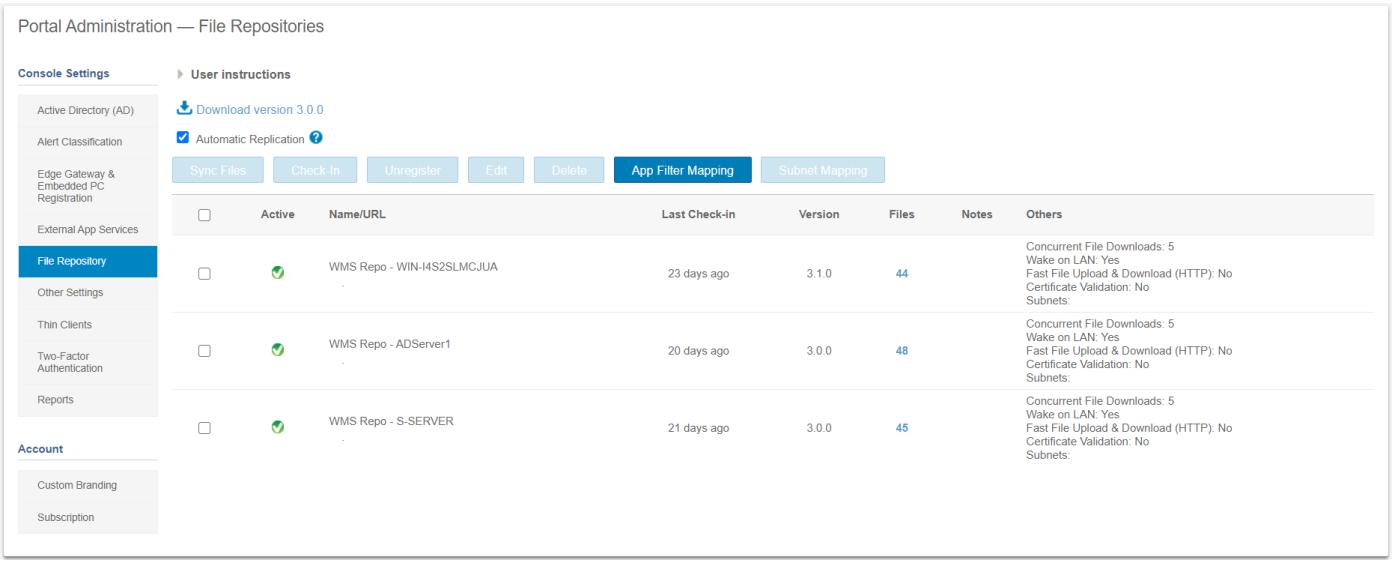


그림 24 . 포털에 등록 성공

9. HTTPS는 기본적으로 `WMS_Repo.exe`에서 활성화되며 자체 서명 인증서와 함께 설치됩니다. 자신의 도메인별 인증서를 설치하려면 등록 페이지를 아래로 스크롤하여 SSL 인증서를 업로드하십시오.

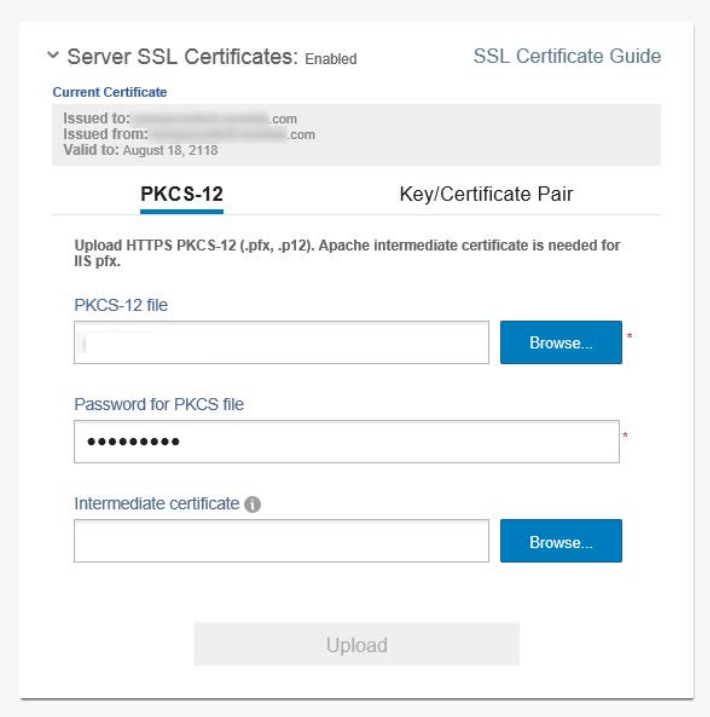


그림 25 . 인증서 업로드

10. 서버가 다시 시작되고 업로드된 인증서가 표시됩니다.

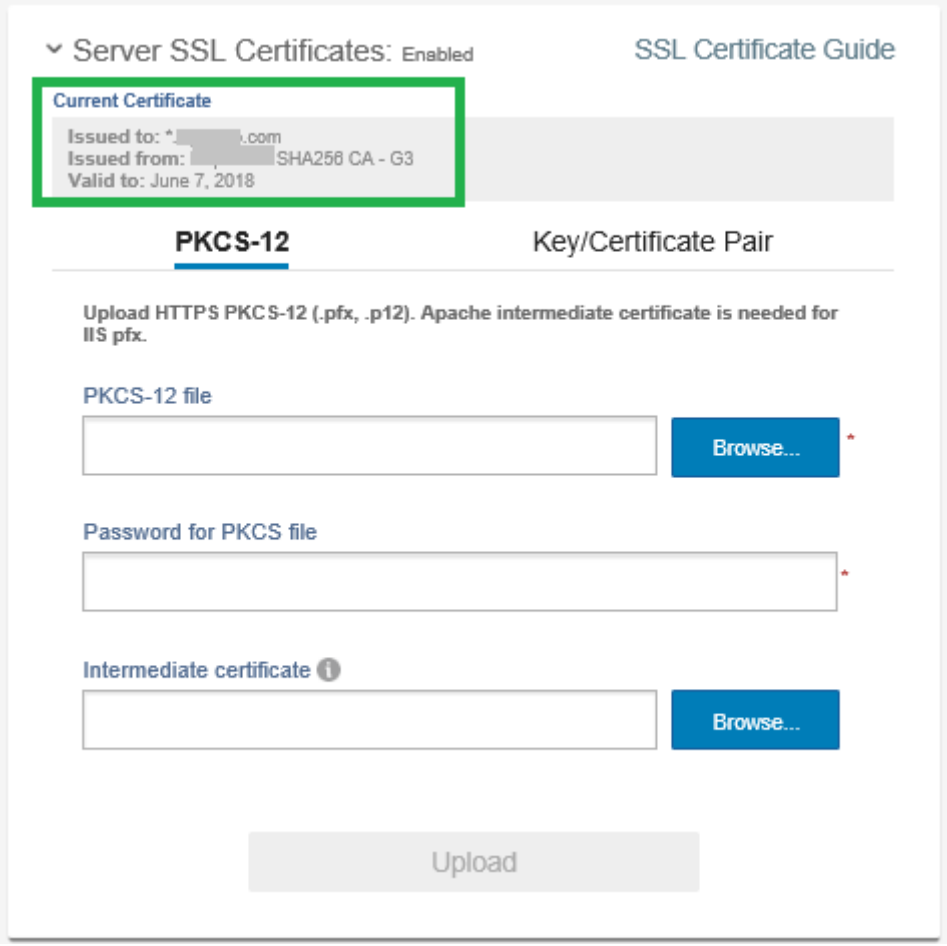


그림 26 . SSL 인증서 활성화

11. Wyse Management Suite가 자체 서명 또는 개인 도메인 인증서로 활성화된 경우 Wyse Management Suite 리포지토리 서버에 인증서를 업로드하여 Wyse Management Suite CA 자격 증명을 확인할 수 있습니다.

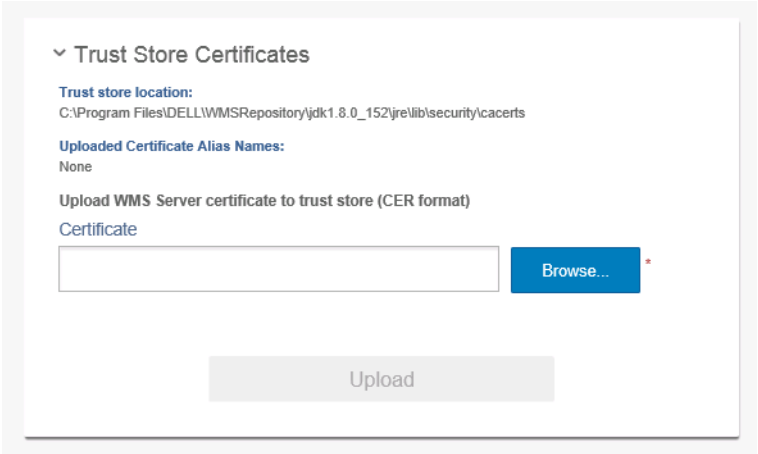


그림 27 . 신뢰 저장소 인증서

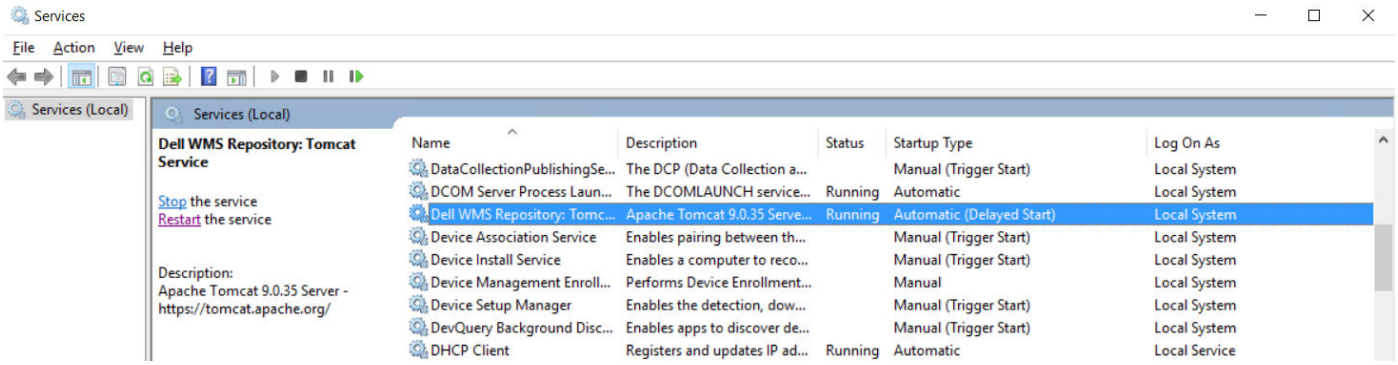
12. 등록 중에 입력한 `C:\wmsrepo` 위치로 이동하면 모든 리포지토리 파일이 저장되고 관리되는 폴더를 볼 수 있습니다.

주제:

- Wyse Management Suite 리포지토리 서비스 관리
- Wyse Management Suite 원격 리포지토리에 대한 프록시 지원

Wyse Management Suite 리포지토리 서비스 관리

Wyse Management Suite 리포지토리는 Windows Local Services 창에서 **Dell WMS Repository: Tomcat Service**로 표시되고 서버가 다시 시작될 때 자동으로 시작하도록 구성됩니다.



Wyse Management Suite 원격 리포지토리에 대한 프록시 지원

Wyse Management Suite 3.2에서 원격 리포지토리는 Wyse Management Suite에 대한 모든 HTTPS 및 MQTT 통신을 위해 HTTPS 및 SOCKS5 프록시를 지원합니다.

원격 리포지토리가 Windows 서비스로 실행되므로 시스템 전체 프록시만 지원됩니다. 또한 AD 인증을 사용하거나 인증이 없는 프록시만 지원됩니다. 어떤 방법으로도 프록시 서버를 구성할 수 있습니다. 다음은 프록시 서버 정보를 구성하는 방법에 대한 몇 가지 예입니다.

- netsh 명령 사용 - 다음 명령을 사용하여 프록시 서버 정보를 구성할 수 있습니다.
  - SOCKS5 프록시

```
netsh winhttp set proxy proxy-server="socks=localhost:9090" bypass-list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="socks=<proxy server
IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

    Proxy Server(s) :  socks=<proxy server IP>
    Bypass List     :  localhost
```

  - HTTPS 프록시

```
netsh winhttp set proxy proxy-server="https=<ProxyServerIP>:<Port number>" bypass-
list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="https=<proxy server
IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

    Proxy Server(s) :  https=<proxy server IP>
    Bypass List     :  localhost
```

- DHCP에서 구성된 WPAD 파일 사용 - Wyse Management Suite 리포지토리 서버는 DHCP IP 주소로 구성되어야 하며 Internet Explorer는 자동 감지 설정으로 구성되어야 합니다. WPAD.pac 파일을 사용하여 DHCP 옵션 태그 252를 구성해야 합니다. 다음은 PAC 파일 콘텐츠 샘플입니다.

```
function FindProxyForURL(url, host)
{
    if (shExpMatch(host, "*wysemanagementsuite.com*")) {
    return "SOCKS <proxy server IP>";
}
```

```
    return "DIRECT";
}
```

그룹 정책을 사용하여 프록시 설정을 구성할 수도 있습니다.

노트: 리포지토리 서비스가 시작되면 프록시 설정을 읽습니다. 나중에 프록시 설정을 변경하는 경우 리포지토리 서비스를 재시작해야 합니다.

노트: SOCKS4 프록시를 사용하는 경우 호스트 이름 확인이 설정되지 않습니다. Wyse Management Suite 리포지토리가 설치된 서버에서 퍼블릭 클라우드 URL/호스트 이름을 확인하려면 `C:\Windows\System32\drivers\etc`에 있는 호스트 파일을 업데이트해야 합니다. SOCKS5 프록시를 사용하는 경우 서버의 네트워크 설정에 구성된 DNS를 사용하는 호스트 이름이 확인됩니다.

21

Windows Embedded Standard WDA 및 Dell Hybrid Client DCA에 대한 프록시 지원

Windows Embedded Standard WDA는 HTTPS 프록시를 지원하며, Dell Hybrid Client DCA는 Wyse Management Suite 공용 서버와의 모든 HTTP 및 보안 MQTT 통신을 위해 HTTP와 SOCKS5 프록시를 지원합니다. WDA 및 DCA가 서비스로 실행되므로 시스템 전체 프록시만 지원됩니다.

AD 인증을 사용하거나 인증이 없는 프록시가 지원됩니다. DHCP 옵션 태그 252를 사용하여 구성된 PAC 스크립트가 지원됩니다. WDA 및 DCA 서비스가 시작되면 프록시 설정을 읽습니다. 프록시 설정이 변경된 경우 WDA 및 DCA 서비스를 재시작해야 합니다.

다음은 프록시 지원의 제한 사항입니다.

- 사용자 수준에서 구성된 프록시는 지원되지 않습니다.
- 사용자가 사용자 이름과 암호를 입력하라는 규정이 없습니다.
- 기본 운영 체제에서 프록시 세부 정보를 읽기 때문에 프록시 URL을 입력할 사용자 인터페이스가 없습니다.
- 1883을 사용한 외부 MQTT는 프록시를 지원하지 않습니다.
- HTTP 프록시는 지원되지 않습니다.
- DNS를 통한 프록시 PAC 파일은 지원되지 않습니다.

주제:

- Windows Embedded Standard WDA용 WININET 프록시를 사용하여 프록시 서버 정보 구성
- Windows Embedded Standard WDA 및 Dell Hybrid Client DCA용 DHCP 옵션 태그를 사용하여 프록시 서버 정보 구성

Windows Embedded Standard WDA용 WININET 프록시를 사용하여 프록시 서버 정보 구성

WININET 프록시 설정을 모든 디바이스에 대한 시스템 수준에서 설정하도록 도메인 정책을 구성해야 합니다.

단계

1. 관리자 권한으로 **명령 프롬프트**를 엽니다.
2. `gpedit.msc` 명령을 실행합니다.
3. 도메인 컨트롤러에서 그룹 정책을 구성하여 컴퓨터당 IE 프록시 구성을 활성화합니다. 정책을 구성하려면 **컴퓨터 구성** > **관리 템플릿** > **Windows 구성 요소** > **Internet Explorer** > **시스템별 프록시 설정**으로 이동하여 옵션을 활성화합니다.
4. 동일한 명령 프롬프트에서 `gpupdate/force`를 실행합니다.
5. 관리자 권한으로 Internet Explorer를 열고 **연결** > **LAN 설정**으로 이동합니다.
6. 프록시를 구성하고 **확인**을 클릭합니다.

Windows Embedded Standard WDA 및 Dell Hybrid Client DCA용 DHCP 옵션 태그를 사용하여 프록시 서버 정보 구성

Windows Embedded Standard 및 Dell Hybrid Client 기반 디바이스는 DHCP IP로 구성해야 합니다. DHCP 구성의 경우 WPAD.pac 파일로 DHCP 옵션 태그 252를 구성해야 합니다.

다음은 샘플 PAC 파일(WPAD.dat) 콘텐츠입니다.

```
function FindProxyForURL(url, host)
{
```

```
        if (shExpMatch(host, "*wysemanagementsuite.com*"))
{
        return "SOCKS 100.xxx.xxx.xxx:1080";
}
        return "DIRECT";
}
```

제한 사항은 다음과 같습니다.

- 보안 MQTT 통신만 프록시를 지원합니다.
- MQTT 포트 1833은 프록시를 지원하지 않습니다.

22

디바이스 문제 해결

디바이스 페이지를 사용하여 문제 해결 정보를 보고 관리할 수 있습니다.

단계

1. **디바이스 세부 정보** 페이지에서 **문제 해결** 탭을 클릭합니다.
2. **스크린샷 요청**을 클릭합니다.
   클라이언트 권한 유무와 상관없이 씬 클라이언트의 스크린샷을 캡처할 수 있습니다. **사용자 동의 필요** 확인란을 선택할 경우 클라이언트에 메시지가 표시됩니다. 이 옵션은 Windows Embedded Standard, Linux 및 ThinLinux 디바이스에만 적용할 수 있습니다.
3. **프로세스 목록 요청**을 클릭하여 씬 클라이언트에서 실행 중인 프로세스 목록을 확인합니다.
4. **서비스 목록 요청**을 클릭하여 씬 클라이언트에서 실행 중인 서비스 목록을 확인합니다.
5. **모니터링 시작**을 클릭하여 성능 메트릭 콘솔에 액세스합니다.
   성능 메트릭 콘솔에 다음과 같은 세부 정보가 표시됩니다.
   - 최근 1분 평균 CPU
   - 최근 1분 평균 메모리 사용량

주제:

- Wyse Management Suite를 사용하여 로그 파일 요청
- Wyse Management Suite를 사용하여 감사 로그 보기
- WinHTTP 프록시가 구성되어 있을 때 디바이스가 Wyse Management Suite에 등록하지 못함
- RemoteFX USB 리디렉션 정책은 USB 대용량 스토리지 디바이스에 적용되지 않음
- Wyse Management Suite에서 구성된 WiFi 설정은 여러 Wyse 5070 씬 클라이언트에서 지속적이지 않음

Wyse Management Suite를 사용하여 로그 파일 요청

전제조건

로그 파일을 가져오려면 디바이스를 활성화해야 합니다.

단계

1. **디바이스** 페이지로 이동하여 특정 디바이스를 클릭합니다.
   디바이스 세부 정보가 표시됩니다.
2. **디바이스 로그** 탭을 클릭합니다.
3. **로그 파일 요청**을 클릭합니다.
4. 로그 파일을 Wyse Management Suite 서버에 업로드한 후에 **여기를 클릭** 링크를 클릭하고 로그를 다운로드합니다.

   노트: ThinOS 디바이스에서는 시스템 로그를 업로드합니다.

Wyse Management Suite를 사용하여 감사 로그 보기

단계

1. **이벤트** > **감사**로 이동합니다.
2. **구성 그룹** 드롭다운 목록에서 감사 로그를 볼 그룹을 선택합니다.
3. **기간 범위** 드롭다운 목록에서 해당 기간 동안 발생한 이벤트를 볼 기간을 선택합니다.
   감사 창은 정보를 일반적인 감사 로그 보기로 정렬합니다. 각 이벤트의 타임스탬프, 이벤트 유형, 소스 및 설명을 시간 순서대로 볼 수 있습니다.

WinHTTP 프록시가 구성되어 있을 때 디바이스가 Wyse Management Suite에 등록하지 못함

WDA는 WinHTTP 클라이언트이며 로컬 시스템에서 WinHTTP 프록시 정보를 가져옵니다.

WinHTTP 프록시를 구성했지만 디바이스가 Wyse Management Suite 서버에 연결되지 않는 경우 다음을 수행하여 시스템 수준에서 사용할 수 있는 프록시 정보를 활성화합니다.

- **케이스 1** - 디바이스가 도메인에 추가되면 도메인의 그룹 정책을 사용하여 각 사용자에 대해 IE-프록시 구성을 활성화합니다. 각 사용자가 아닌 각 클라이언트에 대해 IE-프록시 구성을 활성화하려면 도메인 컨트롤러에서 그룹 정책을 구성해야 합니다.

  `Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Make proxy settings per-machine`로 이동하여 **활성화**를 선택합니다. 또한 Internet Explorer에서 `IE` 설정 > 인터넷 옵션 > 연결 > `LAN` 설정으로 이동하여 **자동 감지 설정**을 활성화합니다.

- **케이스 2** - 디바이스가 도메인에 추가되지 않은 경우 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`로 이동하여 **ProxySettingsPerUser**라고 하는 **32-bit DWORD**를 생성하여 0으로 설정합니다. 또한 Internet Explorer에서 `IE` 설정 > 인터넷 옵션 > 연결 > `LAN` 설정으로 이동하여 **자동 감지 설정**을 활성화합니다.

RemoteFX USB 리디렉션 정책은 USB 대용량 스토리지 디바이스에 적용되지 않음

단계

1. 관리자 권한으로 디바이스에 로그인합니다.
2. 쓰기 필터를 사용 안 함으로 설정합니다.
3. **실행** 명령으로 이동하여 **`Regedit`**를 입력합니다.
4. `HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces`로 갑니다.
5. 문자열 레지스트리 키를 **`100`**으로 추가하고 대용량 스토리지 디바이스에 대한 값을 `{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}`로 설정합니다.

   노트: 중괄호는 필수입니다.

Wyse Management Suite에서 구성된 WiFi 설정은 여러 Wyse 5070 씬 클라이언트에서 지속적이지 않음

Wyse 5070 씬 클라이언트에서 WiFi 연결을 구성할 경우 암호를 요구하지 않고 특정 무선 네트워크(SSID)에 연결됩니다. 동일한 구성이 Wyse Management Suite로 내보내지고 다른 Wyse 5070 Thin Client에 배포되면 구성이 적용되고 동일한 무선 네트워크에 연결할 암호를 입력하라는 메시지가 표시됩니다. WiFi 설정을 영구적으로 설정하려면 다음을 수행합니다.

단계

1. Wyse 5070 씬 클라이언트를 무선 네트워크에 연결합니다.
2. `DWirelessProfileEditor.exe` 파일을 실행합니다.
   무선 프로필 암호 편집기 창이 표시됩니다.
3. 프로필을 xml 파일로 저장할 대상 경로로 이동하여 **저장**을 클릭합니다.
4. **무선 프로필 암호 편집기** 창에서 **WiFi 프로필 내보내기** 버튼을 클릭합니다.
5. **프로필** 드롭다운 목록에서 구성을 배포할 프로필을 선택합니다.
6. **암호** 필드를 지우고 암호를 다시 입력합니다.
7. **암호 변경**을 클릭합니다.

   노트: **WiFi 프로필 내보내기** 버튼을 다시 클릭하지 마십시오.

8. **무선 프로필 암호 편집기** 창을 닫습니다.
9. Wyse Management Suite로 로그인합니다.
10. **앱 및 데이터** > **파일 리포지토리** > **인벤토리**로 이동합니다.
11. **파일 추가**를 클릭합니다.
12. 해당 xml 파일로 이동합니다.
13. **유형** 드롭다운 목록에서 **Windows 무선 프로필**을 선택합니다.
14. 설명을 입력합니다.
15. 현재 구성을 덮어쓰려면 **기존 파일 덮어쓰기** 옵션을 선택합니다.
16. **업로드**를 클릭합니다.
17. **그룹 및 구성** > **프로필 편집** > **WES** > **네트워크**로 이동합니다.
18. **이 항목 구성**을 클릭합니다.
19. **Windows 무선 프로필** 드롭다운 목록에서 업로드된 파일을 선택합니다.
20. **저장 및 게시**를 클릭합니다.

23

FAQ(자주하는 질문)

주제:

- 설정이 충돌하는 경우 Wyse Management Suite와 ThinOS UI 간의 우선 순위는 어떻게 됩니까?
- Wyse Management Suite 파일 리포지토리 사용 방법
- .csv 파일에서 사용자를 가져오는 방법
- Wyse Management Suite의 버전 확인 방법
- DHCP 옵션 태그 생성 및 구성 방법
- DNS SRV 레코드 생성 및 구성 방법
- 호스트 이름을 IP 주소로 변경하는 방법
- 자체 서명된 원격 리포지토리를 사용하여 디바이스를 이미지로 설치하는 방법

설정이 충돌하는 경우 Wyse Management Suite와 ThinOS UI 간의 우선 순위는 어떻게 됩니까?

Wyse Management Suite를 사용하여 구성된 설정이 ThinOS 클라이언트에서 로컬로 구성되었거나 관리 정책 툴을 사용하여 게시된 설정보다 우선합니다.

다음 순서는 ThinOS 구성에 대해 설정된 우선 순위를 정의합니다.

Wyse Management Suite 정책 > **관리 정책 툴** > **로컬 ThinOS UI**

Wyse Management Suite 파일 리포지토리 사용 방법

단계

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. Wyse Management Suite 퍼블릭 클라우드에 리포지토리를 등록하려면 **퍼블릭 WMS 관리 포털에 등록** 옵션을 활성화합니다.
5. **파일 동기화** 옵션을 클릭하여 파일 동기화 명령을 전송합니다.
6. **체크인**을 클릭한 다음 **명령 전송**을 클릭하여 디바이스 정보 명령을 디바이스로 전송합니다.
7. **등록 취소** 옵션을 클릭하여 온프레미스 서비스를 등록 취소합니다.
8. **편집**을 클릭하여 파일을 편집합니다.
   a. **동시 파일 다운로드** 옵션의 드롭다운 목록에서 파일 수를 선택합니다.
   b. **Wake on LAN** 옵션을 활성화 또는 비활성화합니다.
   c. **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.
   d. **인증서 유효성 검사** 확인란을 선택하여 퍼블릭 클라우드에 대한 CA 유효성 검사를 활성화합니다.

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 못함**이라는 하나의 일반 감사 이벤트 메시지를 제공합니다. 앱 및 데이터, 이미지 가져오기/푸시와 같은 모든 작업이 성공적으로 완료되지 않습니다.

- Wyse Management Suite 서버에서 CA 유효성 검사가 비활성화되어 있으면 서버 및 클라이언트의 통신이 인증서 서명 유효성 검사 없이 보안 채널에서 수행됩니다.

e. 제공된 상자에 메모를 추가합니다.
f. **설정 저장**을 클릭합니다.

.csv 파일에서 사용자를 가져오는 방법

단계

1. **사용자**를 클릭합니다.
   사용자 페이지가 표시됩니다.
2. **할당되지 않은 관리자** 옵션을 선택합니다.
3. **대량 가져오기**를 클릭합니다.
   대량 가져오기 창이 표시됩니다.
4. **찾아보기**를 클릭하고 .csv 파일을 선택합니다.
5. **가져오기**를 클릭합니다.

Wyse Management Suite의 버전 확인 방법

단계

1. Wyse Management Suite로 로그인합니다.
2. **포털 관리** > **구독**으로 이동합니다.
   Wyse Management Suite 버전은 **서버 정보** 필드에 표시됩니다.

DHCP 옵션 태그 생성 및 구성 방법

단계

1. 서버 관리자를 엽니다.
2. **툴**로 이동하여 **DHCP 옵션**을 클릭합니다.
3. **FQDN** > **IPv4**로 이동하여 **IPv4**를 마우스 오른쪽 버튼으로 클릭합니다.
4. **미리 정의된 옵션 설정**을 클릭합니다.
   미리 정의된 옵션 및 값 창이 표시됩니다.
5. **옵션 클래스** 드롭다운 목록에서 **DHCP 표준 옵션** 값을 선택합니다.
6. **추가**를 클릭합니다.
   옵션 유형 창이 표시됩니다.
7. 필요한 DHCP 옵션 태그를 구성합니다.
   - 165 Wyse Management Suite 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.
     a. 다음 값을 입력하고 **확인**을 클릭합니다.
        - 이름 – WMS
        - 데이터 유형 - 문자열
        - 코드 - 165
        - 설명 - WMS_서버

     b. 다음 값을 입력한 후 **확인**을 클릭합니다.
        문자열 - `WMS FQDN`
   - 166 MQTT 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.
     a. 다음 값을 입력하고 **확인**을 클릭합니다.
        - 이름 – MQTT
        - 데이터 유형 - 문자열

- 코드 - 166
- 설명 – MQTT 서버

b. 다음 값을 입력하고 **확인**을 클릭합니다.

문자열 - `MQTT FQDN`

예: **`WMSServerName.YourDomain.Com:1883`**

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

a. 다음 값을 입력하고 **확인**을 클릭합니다.
- 이름 - CA 유효성 검사
- 데이터 유형 - 문자열
- 코드 - 167
- 설명 - CA 유효성 검사

b. 다음 값을 입력하고 **확인**을 클릭합니다.

문자열 - TRUE 또는 FALSE

- 199 Wyse Management Suite 그룹 토큰 서버 URL 옵션 태그를 생성하려면 다음을 수행합니다.

a. 다음 값을 입력하고 **확인**을 클릭합니다.
- 이름 - 그룹 토큰
- 데이터 유형 - 문자열
- 코드 - 199
- 설명 - 그룹 토큰

b. 다음 값을 입력하고 **확인**을 클릭합니다.

문자열—defa-격리

노트: 옵션을 DHCP 서버 서버 옵션 또는 DHCP 범위 범위 옵션에 추가해야 합니다.

DNS SRV 레코드 생성 및 구성 방법

단계

1. Server Manager를 엽니다.
2. **툴**로 이동하여 **DNS**를 클릭합니다.
3. **DNS** > **DNS 서버 호스트 이름** > **정방향 조회 영역** > **도메인** > **_tcp**로 이동하고 **_tcp** 옵션을 마우스 오른쪽 버튼으로 클릭합니다.
4. **다른 새 레코드**를 클릭합니다.
   리소스 레코드 유형 창이 표시됩니다.
5. **서비스 위치(SRV)**을 선택하고 **레코드 생성**을 클릭한 후 다음을 수행합니다.

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

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

6. **DNS** > **DNS 서버 호스트 이름** > **정방향 조회 영역** > **도메인**으로 이동하고 도메인을 마우스 오른쪽 버튼으로 클릭합니다.
7. **다른 새 레코드**를 클릭합니다.
8. **텍스트(TXT)**를 선택하고 **레코드 생성**을 클릭한 후 다음을 수행합니다.

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

b. Wyse Management Suite CA 유효성 검사 기록을 생성하려면 다음 값을 입력한 다음 **확인**을 클릭합니다.
   - 기록 이름 - _WMS_CAVALIDATION
   - 텍스트 - TRUE/FALSE

호스트 이름을 IP 주소로 변경하는 방법

이 작업 정보

호스트 이름 확인에 실패할 경우 호스트 이름을 IP 주소로 변경해야 합니다.

단계

1. 관리자 모드에서 DOS 프롬프트를 엽니다.
2. 디렉토리를 **C:\Program Files\DELL\WMS\MongoDB\bin**으로 변경합니다.
3. **mongo localhost -username stratus -p --authenticationDatabase admin** 명령을 입력합니다.
   출력 - MongoDB shell 버전 v4.2.12
4. 암호를 입력합니다.
   출력 -
   - connecting to: mongodb://127.0.0.1:27017/localhost
   - MongoDB 서버 버전: 4.2.12
5. 입력 : use stratus
   출력 - switched to db stratus
6. **> db.bootstrapProperties.updateOne({'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}})** 명령을 입력합니다.
   출력 - { "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. **> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})** 명령을 입력합니다.
   출력 - { "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

자체 서명된 원격 리포지토리를 사용하여 디바이스를 이미지로 설치하는 방법

프라이빗 클라우드의 로컬 리포지토리에서 또는 퍼블릭 클라우드의 원격 리포지토리에서 Windows Embedded Standard 및 ThinLinux 디바이스의 이미징을 수행할 수 있습니다.

전제조건

이미지가 프라이빗 클라우드의 로컬 리포지토리에서 또는 퍼블릭 클라우드의 원격 리포지토리에서 자체 서명된 인증서를 사용하여 배포된 경우 관리자는 자체 서명된 인증서를 씬 클라이언트로 푸시하여 CA 유효성 검사가 수행될 때 이미징을 수행해야 합니다.

단계

1. Internet Explorer 또는 MMC에서 자체 서명된 인증서를 내보냅니다.
2. Wyse Management Suite에 인증서를 업로드합니다. 이미지 정책을 참조하십시오.
3. 보안 정책을 사용하여 인증서를 타겟 클라이언트 또는 클라이언트 그룹으로 푸시합니다.
   구성 정책 작업이 완료될 때까지 기다립니다.
4. 프라이빗 클라우드의 로컬 리포지토리에서 또는 퍼블릭 클라우드의 원격 리포지토리에서 CA 유효성 검사를 활성화합니다.
5. 이미지 정책을 생성하고 이를 그룹으로 예약합니다.